YubiOn FIDO Logon Standalone

Administrator Manual

SOFTGIKEN Co., Ltd.

August 2026 Edition

Contents

Chapter 1. Introduction

1.1 Purpose of This Manual

This manual is written for administrators who install and configure **YubiOn FIDO Logon Standalone** (hereafter "this product") on Windows computers. It covers everything from checking the system requirements through installation, initial configuration, and day-to-day operation.

For instructions on how end users actually sign in with an authenticator, see the separate **End User Guide**.

1.2 Intended Readers

This manual is intended for:

- **IT administrators and information systems staff** who deploy this product to Windows computers in an organization
- Operations staff who manage this product's licenses and authenticators (FIDO2 devices)

Basic knowledge of Windows administrator privileges, Group Policy, and the registry is assumed.

1.3 Product Overview

This product is a standalone Credential Provider that adds authentication with a **FIDO2 authenticator (such as a YubiKey)** to Windows sign-in, making it more secure than password-only sign-in.

Its main characteristics are as follows.

- **It never communicates with a server.** FIDO2 verification, credential storage, and the password cache are all handled locally on the computer, so it works on its own even in a closed network with no Internet connection.
- Credentials (public key, credential ID, and so on) are encrypted with a key unique to the computer using **DPAPI (LOCAL_MACHINE)** and stored locally. They cannot be decrypted on another computer.
- **Local accounts, Active Directory domain accounts, Entra ID (Azure AD) accounts, and Microsoft accounts** are all supported. One PC can have multiple users, and each user can register multiple authenticators.
- Authenticators can be registered either by **pre-registration by an administrator** or by **self-registration by the user at first sign-in**.

> **Note** A valid license is required for this product to work. For how to register a license, see "Registering the License".

1.4 How This Manual Is Organized

Chapter	Contents
Chapter 1 Introduction	Purpose of this manual and product overview
Chapter 2 System Requirements and Operating Environment	Requirements to check before deployment
Chapter 3 Installation	Deployment with the MSI installer
Chapter 4 Overview of the Settings Tool	Starting the settings tool and its screen layout
Chapter 5 Registering the License	License registration and the machine code
Chapter 6 Launch Authentication for the Settings Tool (Optional)	FIDO authentication at settings tool launch, and administrator authenticators
Chapter 7 Basic Settings	Authenticator logon, secure mode, and other settings
Chapter 8 Registering and Managing User Authenticators	Managing users' FIDO authenticators
Chapter 9 Managing Master Keys	Administrator authenticators for signing in on a user's behalf
Chapter 10 Managing Recovery Codes	Issuing codes for emergency sign-in
Chapter 11 Transferring Settings and Credentials	Export and import
Chapter 12 Operation and Maintenance	Collecting support information and checking logs
Chapter 13 Troubleshooting	Common problems and what to do
Appendix A Glossary	Definitions of terms
Appendix B List of Settings	Reference for the settings
Appendix C List of Event Log Entries	List of audit events

1.5 Related Manuals

Manual	Intended readers	Contents
Administrator Manual (this manual)	IT administrators	Deployment, configuration, operation
Quick Start Guide for Administrators	IT administrators	Shortest single path from installation to initial setup and verification
End User Guide	General users	Signing in with an authenticator

Chapter 2. System Requirements and Operating Environment

Before deploying this product, check that the target computer meets the following requirements.

2.1 Supported Operating Systems

Category	Supported versions
Client OS	Windows 10 (20H2 or later) / Windows 11
Server OS	Windows Server 2022 or later

> **Note** The above is based on configurations that can also support sign-in over RDP (WebAuthn redirection). **Windows Server 2019 and versions of Windows 10 earlier than 20H2 do not support WebAuthn redirection and are therefore out of scope for support** (for details, see "Requirements for Signing In over Remote Desktop (RDP)" in this chapter).

> **Important** This product ships separate installers for server and for regular (client) editions. A license is also tied to the OS type of the computer (server / client), so use the installer and license that match the OS type. If the type does not match, the license is rejected as an "OS edition mismatch".

2.2 Runtime Environment

Item	Requirement
CPU	**A 64-bit processor of 1 GHz or faster** (this product is provided in a 64-bit edition only)
Memory	**4 GB or more**
Storage	**200 MB or more of free space** (about 40 MB for the program, plus space for logs, settings, and credentials)
Software	**.NET Framework 4.7.2** or later
USB	A **USB port** for connecting a FIDO2 authenticator (when used over RDP, the port is needed on the client PC)

> **Note** The CPU and memory figures above match what the supported operating systems themselves (Windows 11, Windows Server 2022, and so on) require. The additional resources this product needs are small; the resident service uses on the order of a few tens of MB of memory. In practice, any configuration that satisfies the requirements of the OS and your other business applications is fine.

> **Note (about log space)** Operation logs are written to `%ProgramData%\YubiOn\FidoStandalone\logs`, and **the file rolls over daily**. **Logs older than 90 days are deleted automatically by the service**, so logs do not grow without limit (Chapter 12 "Checking the Logs").

2.3 FIDO2 Authenticator Requirements

- Any **FIDO2-capable authenticator** can be registered, not only a YubiKey.
- The authenticator must support **UV (user verification: PIN or biometrics)**. If no PIN has been set, the user is prompted to set one (4 characters minimum) at first registration.
- **U2F (CTAP1) only keys cannot be registered or used for signing in by default.** They can be used only if the setting **Allow non-UV keys (U2F)** is turned on, but in that case the hmac-secret extension is unavailable, so no password cache is created and **the Windows password must be entered at every sign-in**.

2.4 Requirements for Signing In over Remote Desktop (RDP)

To use FIDO logon over RDP, all of the following requirements must be met. **Environments that do not meet all of them are out of scope for support** (there is no automatic fallback to password logon).

- **Both the client PC (RDP client) and the host** must be one of the following, which support WebAuthn redirection.

OS	Required update
Windows 11	2022-10 cumulative update (KB5018418) or later
Windows 10 (20H2 or later)	2022-10 cumulative update (KB5018410) or later
Windows Server 2022 or later	2022-10 cumulative update (KB5018421) or later

> **Important** **Windows Server 2019 does not support WebAuthn redirection** (the protocol for this feature itself was added in 2022). Even if the Group Policy item exists, it does not work, so FIDO logon over RDP cannot be used on Server 2019. The same applies to versions of Windows 10 earlier than 20H2.

- The Group Policy for **WebAuthn request redirection** must be enabled (set **Do not allow WebAuthn redirection** to **Disabled** or **Not Configured**)
- The FIDO authenticator must be **connected to the RDP client PC** (it is not recognized if inserted on the host)

- **Enable authenticator logon** must be turned on for the target computer (Chapter 7 "Enabling Authenticator Logon")

> **Note** **Secure mode is not required** for FIDO logon over RDP. When secure mode is off, conventional password logon remains available over RDP as well. If you want FIDO authentication to be mandatory for RDP connections too, turn secure mode on (Chapter 7 "Secure Mode").

> **Additional note** When the RDP host is Windows 10, the way the password cache is created differs somewhat because of how WebAuthn redirection is specified, but sign-in itself works.

2.5 Additional Notes on Behavior

- The **RP ID** (the FIDO2 relying party identifier) is fixed to `standalone.yubion.local` and cannot be changed.
- The **FIDO authentication timeout** is fixed at 120 seconds (2 minutes).
- Credentials and other data are stored under `%ProgramData%\YubiOn\FidoStandalone`.

2.6 Components That Are Installed

Running the installer deploys the following components.

Component	Role
Credential Provider	Adds the FIDO logon method to the Windows sign-in screen
Windows service (`YubiOnFidoStandaloneService`)	Handles FIDO2 verification and the storage and decryption of credentials (runs as LocalSystem)
Settings tool (administrator GUI)	Manages the license, authenticators, and all settings

Chapter 3. Installation

3.1 Before You Install

- The target computer meets the requirements in "System Requirements and Operating Environment"
- You have the **installer that matches the OS type of the computer (server / client)**
- The user performing the installation has **administrator privileges**
- You have the issued **license file** (required for this product to work)

3.2 Installation Steps

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.

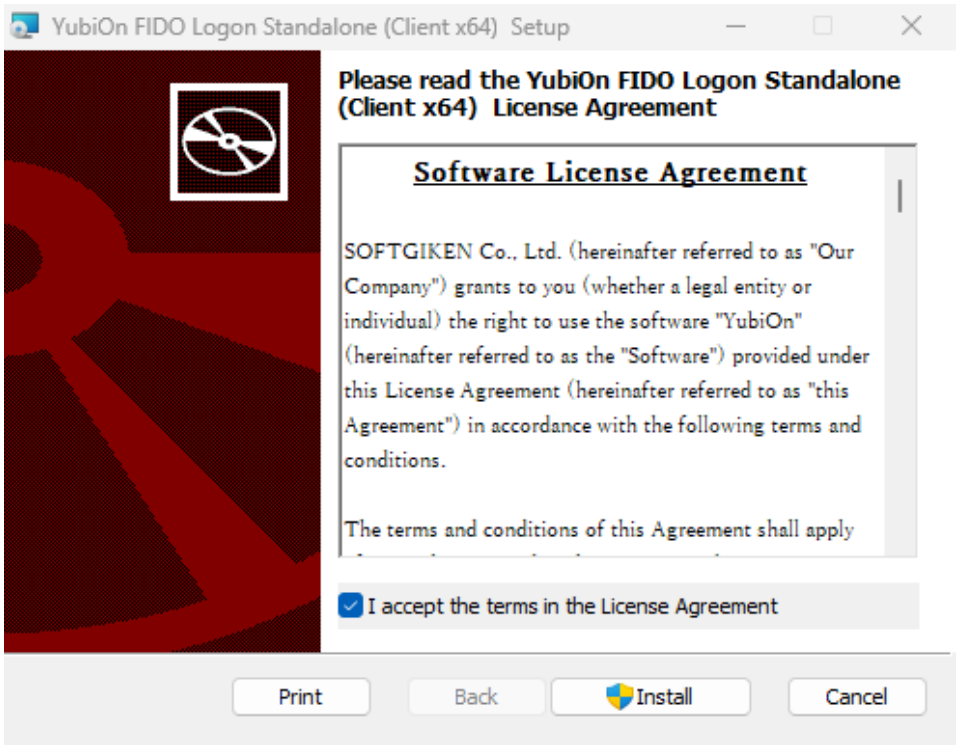

Figure: The MSI installer wizard

Note: If Microsoft Defender SmartScreen appears

When you run the installer, a blue screen saying "Windows protected your PC" may appear. This is the standard Windows confirmation screen for executables obtained from the Internet; you can continue the installation as follows.

1. Select **More info**.
2. Select **Run anyway**, which then appears.

During installation, the data folder `%ProgramData%\YubiOn\FidoStandalone` is created and its access permissions (ACL) are set to a protected state.

3.3 After Installation

Right after installation, FIDO logon is not yet enabled. The following work is required next.

1. **Registering the license** (Chapter 5)
2. **Registering authenticators** (Chapter 8)
3. **Enabling authenticator logon and other settings** (Chapter 7)

3.4 Uninstalling

This product can be uninstalled from **Apps & features** in Windows.

> **Caution** If the **Uninstall protection** setting is on, the product does not appear in the app list. Turn the setting off in the settings tool before uninstalling.

Chapter 4. Overview of the Settings Tool

This product is managed from the **settings tool**, an administrator GUI.

4.1 Starting the Tool

1. Open the Start menu and select **All apps** to show the list of applications.
2. In the list, click **YubiOn FIDO Logon Standalone Settings Tool**.
3. A User Account Control (UAC) prompt appears; select **Yes**.

The settings tool runs with administrator privileges (UAC elevation), so the prompt in step 3 appears every time. Users without administrator privileges cannot start it.

> **Additional note** The shortcut name starts with "Y", so it is near the end of the application list, under "Y". Depending on the Windows version, it may appear inside a **YubiOn** folder.

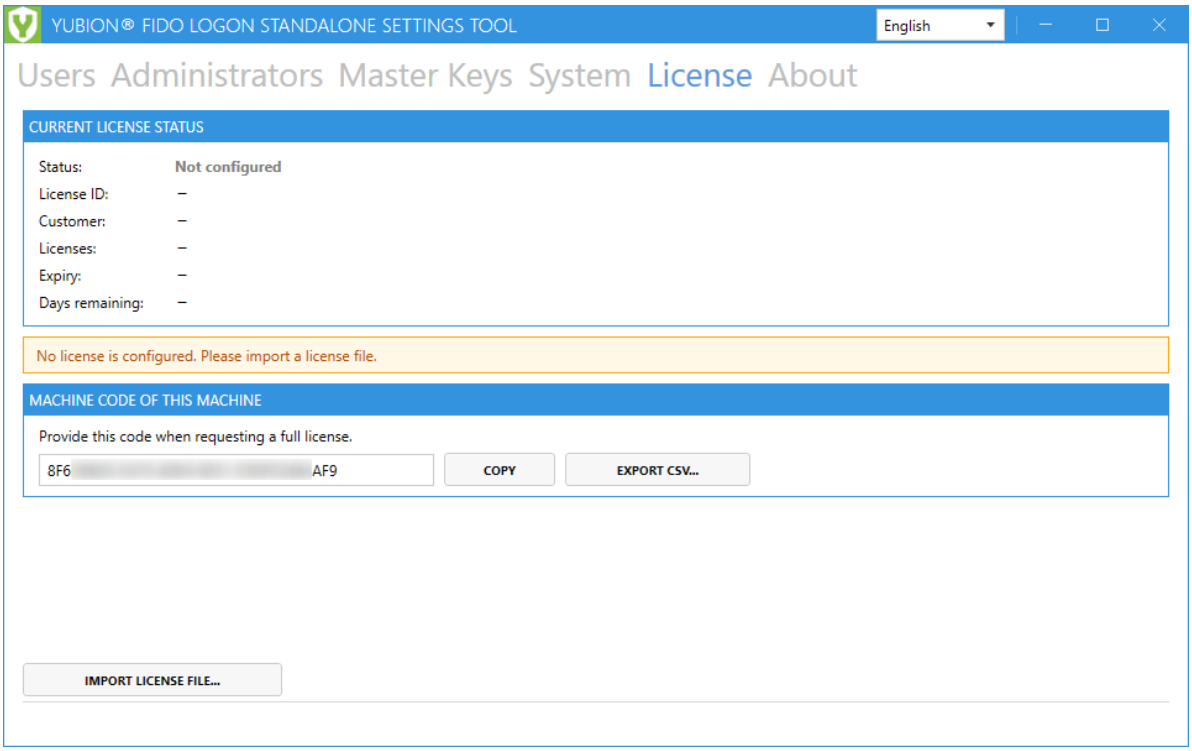

Figure: The main window of the settings tool

4.2 Screen (Tab) Layout

The settings tool consists of the following tabs (in the order they appear).

Tab	Main functions	Chapter in this manual
Users	Registering and deleting authenticators, managing recovery codes	Chapter 8, Chapter 10

Tab	Main functions	Chapter in this manual
Administrators	Switching launch authentication on and off, managing administrator credentials	Chapter 6
Master Keys	Registering, deleting, and renaming master keys	Chapter 9
System	Behavior settings, transferring settings	Chapter 7, Chapter 11
License	Showing and registering the license, showing the machine code	Chapter 5
About	Checking the version, collecting support information	Chapter 12

Reference The License tab and the About tab can always be used, even when the license is not valid (so that you can check the machine code, register a license, and collect support information).

Chapter 5. Registering the License

A valid license is required to use this product's FIDO logon feature. The license is managed on the **License** tab of the settings tool.

5.1 License Types

Type	Description
Full license	Works only on the computer it was registered for. It is tied to the identifying information of the computer (the machine code).
Temporary license	Works for a limited period without being tied to a computer. Used for trials and transition periods.

5.2 Checking the Machine Code

Issuing a full license requires the **machine code** of the target computer. The machine code is the computer's **BIOS (SMBIOS) system UUID**, normalized to the following form.

- **Uppercase, with hyphens, 36 characters** (the `8-4-4-4-12` form)
- Example: `4C4C4544-0042-3010-8051-B7C04F503233`

5.2.1 When the Machine Code Changes and When It Does Not

The BIOS system UUID behind the machine code is **a value recorded in the firmware of the motherboard (system board)**. The OS only reads it, so **it does not change when you reinstall the OS**.

Operation on the computer	Machine code	License
Reinstalling, resetting, or upgrading the OS	**Unchanged**	**Can be used as is** (no re-issue needed)
Replacing or adding a disk (HDD / SSD)	Unchanged	Can be used as is
Adding or replacing memory or peripherals	Unchanged	Can be used as is
Changing or updating BIOS / UEFI settings	Normally unchanged	Normally can be used as is
Replacing the motherboard (including board repair)	**Changes**	**Re-issue required**
Replacing the PC itself (moving to a new computer)	**Changes** (it is a different computer)	**Re-issue required**

Important (a license must be re-issued when you replace the PC or the motherboard)
A full license works only on the computer with the registered machine code. **If you move to a new PC, or replace the motherboard, that computer's machine code differs from before, so the existing license will not work** (the license status in the settings tool shows **Invalid (machine mismatch)**). Obtain the new computer's machine code as described in this section and **ask the issuer to re-issue the license**.

- If you need to start using the replacement immediately, you can register a **temporary license** (see "License Types" in this chapter), which is not tied to a computer, and run on it while you wait for the full license to be re-issued.
- Exclude the machine code of any **computer you have stopped using** from your next re-issue request (for contract seat management).
- On the other hand, **reinstalling or resetting the OS does not change the machine code, so no re-issue is needed**. Simply register your backed-up license file again and it will keep working.

Note For a virtual machine (VM), the UUID comes from the configuration on the virtualization platform. Cloning or recreating a VM can change the value, in which case a re-issue is also required.

5.2.2 Checking It in the Settings Tool

On a computer where this product is already installed, you can check it from the settings tool.

1. Open the **License** tab of the settings tool.

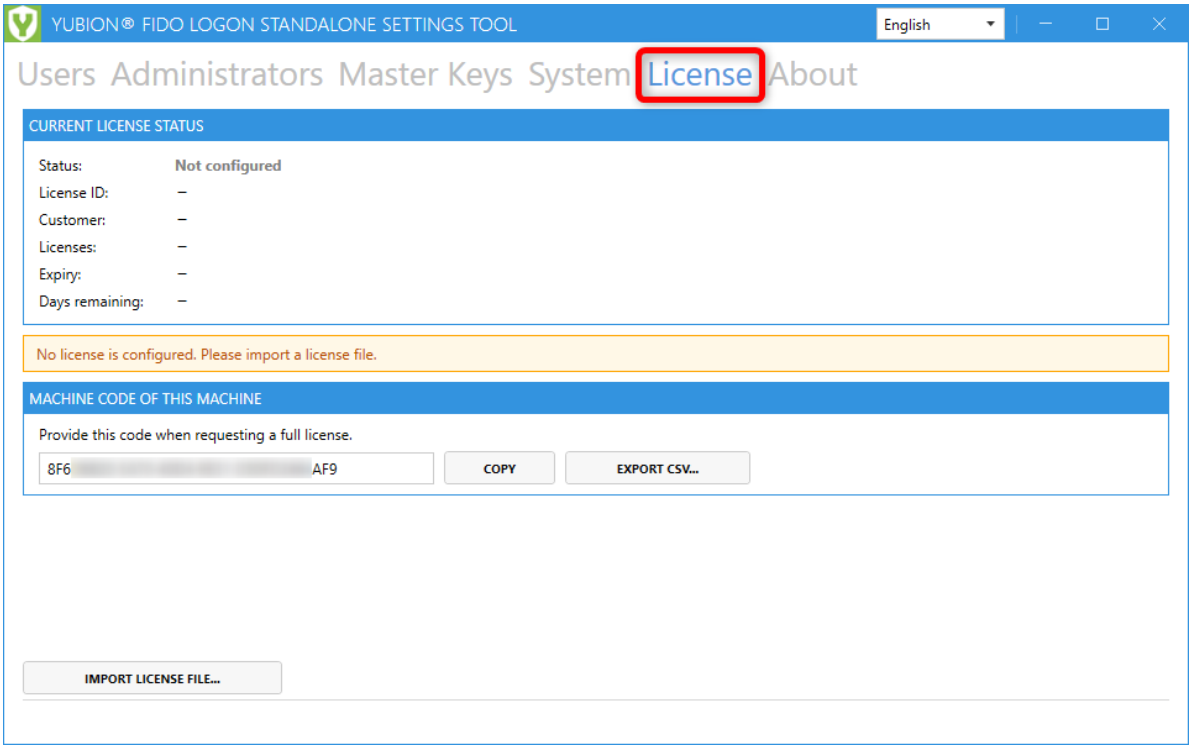

Figure: The License tab

2. Check the value shown in the **Machine Code of This Machine** box.

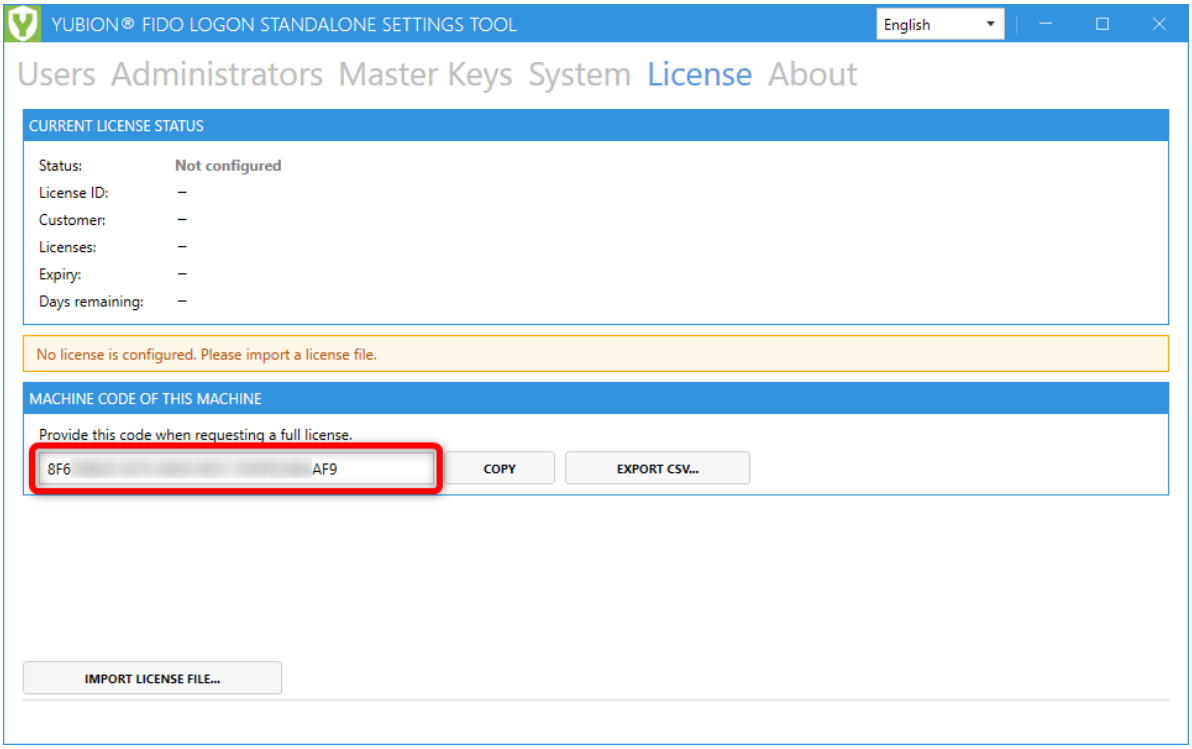

Figure: The machine code shown on the License tab

3. Obtain the value with **Copy** or **Export CSV...** and submit it to the license issuer.

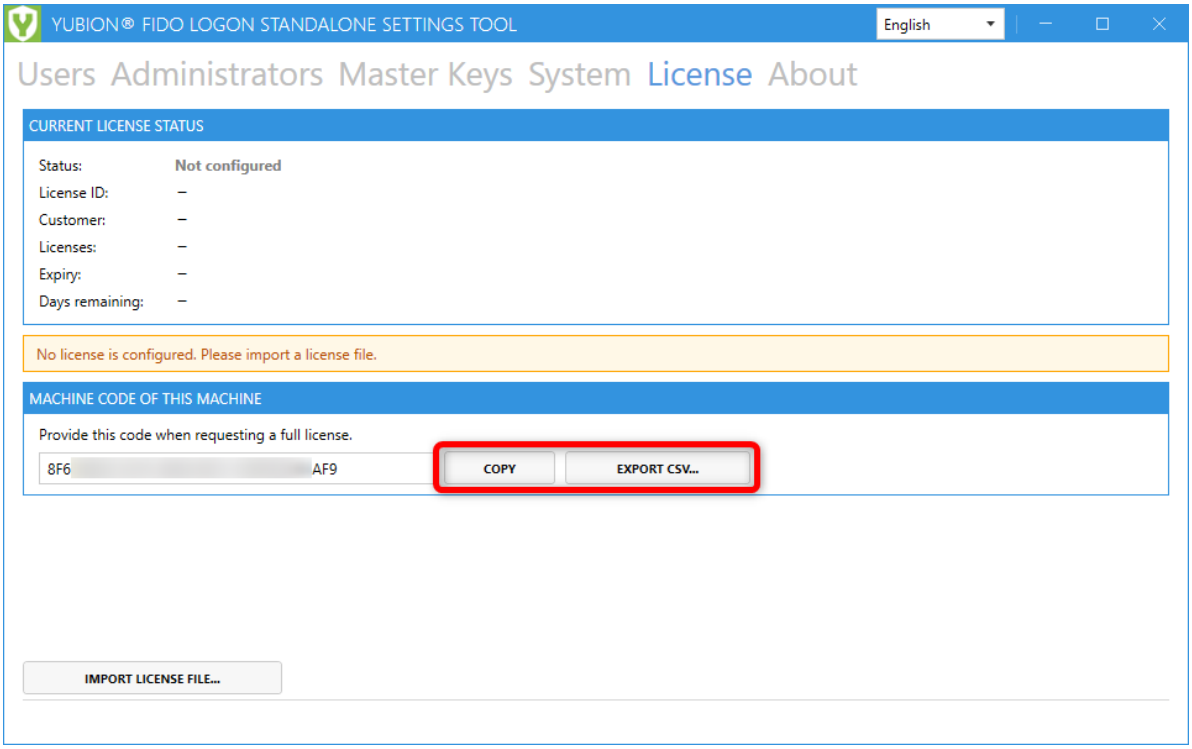

Figure: The button for copying the machine code

To have licenses issued for several computers at once, export the machine code as CSV on each computer and submit them together to the issuer.

5.2.3 Obtaining It Without Installing This Product

Even before deploying this product, the BIOS system UUID behind the machine code can be obtained with standard OS features or with asset management products. Use this when you want to request licenses for many computers at once before deployment.

Method 1: PowerShell (recommended)

Run the following command in PowerShell.

```
Get-CimInstance Win32_ComputerSystemProduct | Select-Object -ExpandProperty UUID
```

Method 2: Command Prompt (for older operating systems)

```
wmic csproduct get uuid
```

> **Caution** The `wmic` command is removed by default in Windows 11 24H2 and later. Use method 1 (PowerShell) on newer operating systems.

Method 3: Use an asset management product

Microsoft Configuration Manager (SCCM), Microsoft Intune, and other inventory or asset

management products can also collect a computer's SMBIOS UUID. The field name differs by product and may appear as **UUID**, **SMBIOS UUID**, **System UUID**, or **BIOS GUID**.

> **Important (check before submitting)** This product normalizes the machine code to **uppercase with hyphens** before comparing it. If a value obtained elsewhere is lowercase, **convert it to uppercase** before submitting. In addition, the following invalid values (defaults set on some computers) cannot be used as a machine code. If you encounter one, check the settings on the computer.
>
> - `00000000-0000-0000-0000-000000000000` (all zeros)
> - `FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF` (all Fs)
> - `03000200-0400-0500-0006-000700080009` (a default on some motherboards)

5.2.4 Format of the File to Submit

When submitting several computers at once, a text file in the same format as the settings tool's CSV export can be used as is.

- **Character encoding:** UTF-8 (without BOM)
- **Delimiter:** comma (`,`)
- **Header row:** none
- **One line per computer**, with the columns in this order

Column	Contents	Example
1	Machine name (computer name)	`PC-001`
2	Machine code (UUID)	`4C4C4544-0042-3010-8051-B7C04F503233`
3	OS type (`client` or `server`)	`client`

Example:

```
PC-001,4C4C4544-0042-3010-8051-B7C04F503233,client
PC-002,9A8B7C6D-5E4F-3A2B-1C0D-EF1122334455,client
SRV-01,1122AABB-CCDD-EEFF-0011-223344556677,server
```

> **About the OS type** A full license is also tied to the OS type of the computer (server / client). In PowerShell you can determine it with the following command (`1` means client; anything else means server).
>
> ```
> (Get-CimInstance Win32_OperatingSystem).ProductType
> ```
>
> To output the whole line above (machine name, UUID, OS type) at once, run:
>
> ```
> $uuid = (Get-CimInstance Win32_ComputerSystemProduct).UUID.ToUpper()
> $os = if ((Get-CimInstance Win32_OperatingSystem).ProductType -eq 1) { 'client' } else { 'server' }
> "$env:COMPUTERNAME,$uuid,$os"
> ```

5.3 Registering the License File

1. Place the issued **license file** on the computer.
2. Select **Import License File...** at the bottom of the License tab and specify the license file.

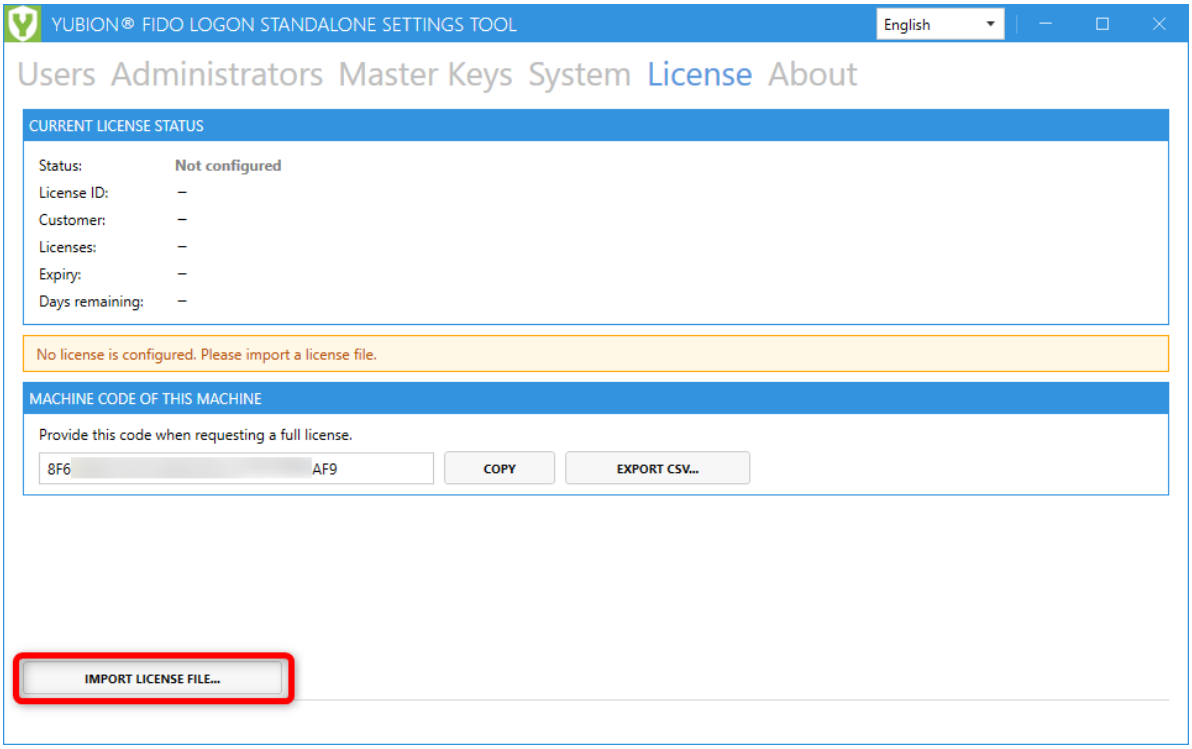

Figure: The Import License File button

3. Confirm that the license status becomes "Valid".

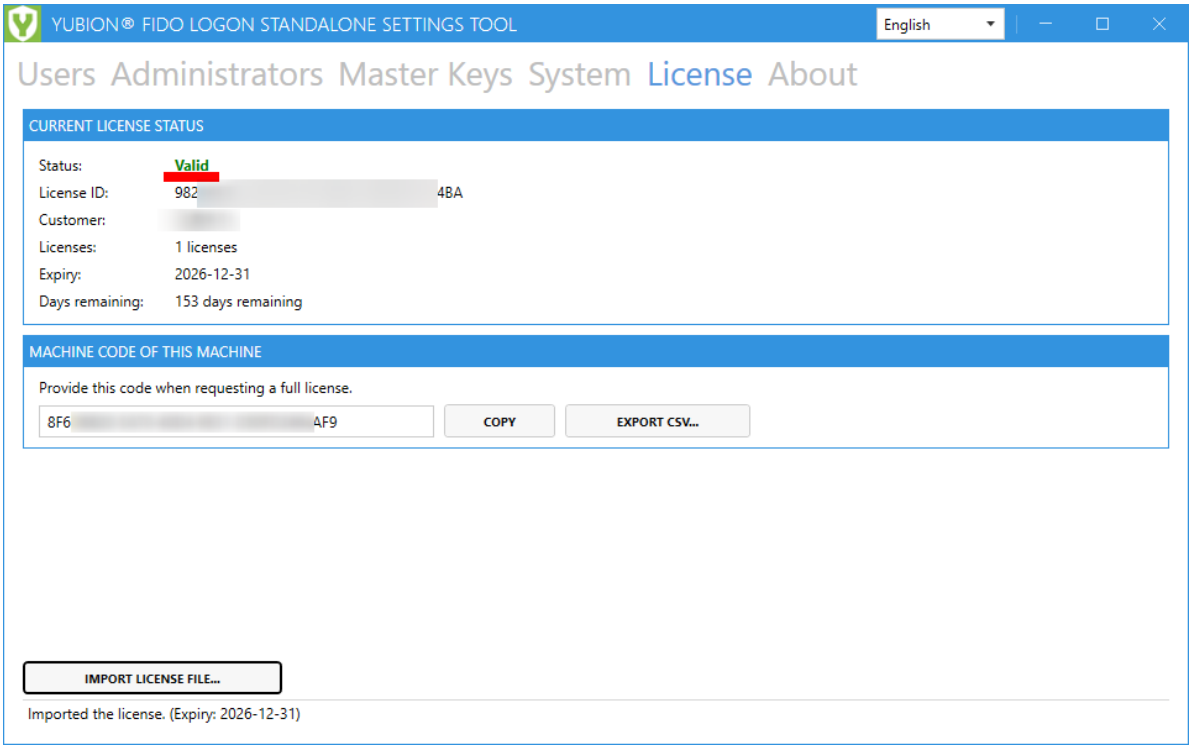

Figure: The license activated

5.4 Renewing the License

When a license file is re-issued to extend the expiry date, switch from a temporary license to a full license, or add contract seats, you can renew **simply by importing the new license file**. There is no need to delete the old license or reinstall the product.

5.4.1 Renewal Steps

1. Receive the new license file from the issuer.
2. Open the **License** tab of the settings tool, select **Import License File...**, and specify the new file (the same operation as "Registering the License File" in this chapter).
3. Confirm that "Imported the license. (Expiry: yyyy-mm-dd)" is shown and that the status and expiry date have been updated.

The existing license file is overwritten automatically. Renewal is done per computer and does not affect authenticators, master keys, recovery codes, or any settings.

> **Note** The license status is evaluated at every sign-in, so there is no need to restart the service or the computer after renewing. The new license takes effect from the next sign-in.

5.4.2 When to Renew

- **You can renew before the license expires.** When a full license is within 30 days of its expiry date, its status changes to **Valid (n days until expiry)**, and the License tab shows the remaining days along with a warning that prompts you to renew. Consider renewing when you see this. After renewal, the status returns to **Valid**.
- **You can also renew after it has expired, using the same steps.** While the license is expired, some tabs of the settings tool cannot be used, but **the License tab remains usable**, so renewal is possible. After renewal, the tabs become usable again immediately, and FIDO logon comes back automatically from the next sign-in (see "Behavior When the License Expires" in this chapter).
- Renewing a full license **does not change the computer's machine code**. You only need to submit a machine code again if you have replaced the PC itself or the motherboard (see "When the Machine Code Changes and When It Does Not" in this chapter).

5.4.3 When Renewal Is Rejected

An import is validated before being saved, and a file matching any of the following is refused. In that case **the current license file is not replaced and the state before renewal is kept** (event ID 3701 is recorded).

Message shown	Main cause and what to do
File not found.	There is no file at the specified path. Check the location of the file.

Message shown	Main cause and what to do
The license file is invalid (signature verification failed or XML format error).	The file is corrupted or its contents have been altered. Obtain it again from the issuer.
The license file has already expired and cannot be imported.	You selected an old license file. Specify a file with a newer expiry date.
This license does not include this machine's machine code and cannot be imported.	The file is for a different computer. Request a re-issue using the machine code obtained in "Checking the Machine Code" in this chapter.
This license is registered for a different OS edition (server/client) than this machine and cannot be imported.	You mixed up the server and client editions. Request a re-issue for the OS type of this computer.

5.4.4 Renewing Many Computers at Once

You can also renew without the settings tool, by directly replacing each computer's license file with the new one. This can be used for bulk renewal with a distribution script or Group Policy.

- The destination is `%ProgramData%\YubiOn\FidoStandalone\license.slcx`. Access to this folder is restricted, so you must **write to it with administrator privileges**.
- The service detects the replacement and, if the license is valid, records event ID **2910**. There is no need to restart the service or the computer.
- If you accidentally replace it with an invalid file (corrupted, for another computer, or expired), the service **automatically restores** the backup of the last valid license (event ID **2911**). If there is no backup to restore from, nothing is restored and event ID **2912** is recorded.

> **Caution** If the license file is deleted, it is not restored (deletion cannot be distinguished from intentional removal). The status becomes "Not configured" and FIDO logon stops working.

5.5 List of License States

State	Meaning	Behavior
Valid	Normal	Works
Valid (n days until expiry) / ExpiringSoon	Within 30 days of the expiry date	Works
Temporary license / TemporaryValid	Valid on a temporary license	Works
Not configured / NotConfigured	No license registered	Does not work
Invalid	The file is not legitimate	Does not work

State	Meaning	Behavior
Invalid (machine mismatch) / MachineMismatch	A license for another computer	Does not work
Invalid (OS edition mismatch) / OsTypeMismatch	Server / client mismatch	Does not work
Expired	Past the expiry date	Does not work

> **No lockout occurs** Even when the license is not valid, users are never locked out by having FIDO logon forced on them. In that state, ordinary password sign-in is available, and FIDO logon comes back automatically once you register a license again.

5.5.1 Behavior When the License Expires

A license is valid **through the end of the date written in the license file (23:59:59)**. From the following day it becomes **Expired**, and behavior is as follows.

Sign-in screen

- This product's **FIDO tile is no longer shown**. Signing in with an authenticator is not possible.
- **Even when secure mode is on, other sign-in methods are no longer suppressed once the license expires.** Users with a registered authenticator can sign in with a password as usual, and the same applies to unlocking the screen. Note that expiry does not rewrite the secure mode setting. When you renew the license, suppression comes back from the next sign-in without changing any setting.
- This product does not intervene in RDP connections either.

> **Reference** The license status is evaluated at every sign-in. Even if the license expires, a session you are already signed in to is not interrupted. The behavior above starts from the next sign-in or unlock.

Settings tool

- The status on the License tab changes to a red **Expired (yyyy-mm-dd)**, and the remaining-days field becomes **Expired (n days over)**. A warning is also shown: "The license expired on yyyy-mm-dd. Please import a new license."
- When you start the settings tool, it opens with **the License tab selected**.
- The four tabs **Users, Administrators, Master Keys, and System** become unusable (the **License** and **About** tabs remain usable).

- If **Require FIDO authentication to launch the settings tool** is on, **administrator authentication is still required at launch even while the license is expired**. Be careful: if you have lost your administrator authenticator, you will not be able to change settings even after renewing the license.

Because those four tabs are unusable, the following operations cannot be performed while the license is expired.

Operation	Tab
Assigning (registering), deleting, and renaming authenticators; issuing recovery codes	Users
Registering and deleting administrator authenticators; switching launch authentication	Administrators
Registering, deleting, and renaming master keys	Master Keys
Changing system settings; exporting and importing settings and credentials	System

Registered information

- Registered authenticators, administrator authenticators, master keys, recovery codes, and all settings are **not deleted** when the license expires.
- When you import a valid license, the tabs of the settings tool become usable again immediately, and FIDO logon comes back automatically from the next sign-in. **You do not have to redo any registration or configuration.**

> **Caution** An expired license file **cannot be imported** ("The license file has already expired and cannot be imported." is shown). Obtain a license file with a newer expiry date from the issuer.

Preventing expiry

- When a full license is within 30 days of its expiry date, the status changes to **Valid (n days until expiry)**, and the License tab shows the remaining days along with a warning that prompts you to renew. Check the License tab periodically.
- **A temporary license never shows the "expiring soon" state.** Instead, the message "Running on a temporary license. Please import a full license by yyyy-mm-dd." is shown at all times.
- The license status is recorded in the event log entry written when the service starts (event ID **2900**). On an expired computer it prints `License: Expired (yyyy-mm-dd)`, so you can check the state of many computers from the event log.

Chapter 6. Launch Authentication for the Settings Tool (Optional)

For extra security, you can require FIDO authentication to launch the settings tool itself (**Require FIDO authentication to launch the settings tool** on the **Administrators** tab; off by default).

> **Note** Do the steps in this chapter after you have registered a license (Chapter 5 "Registering the License File").

- When it is on, an "Administrator Authentication" dialog appears at launch and asks for FIDO authentication with an **administrator authenticator (administrator credential)**. Select **Authenticate** and touch your authenticator.

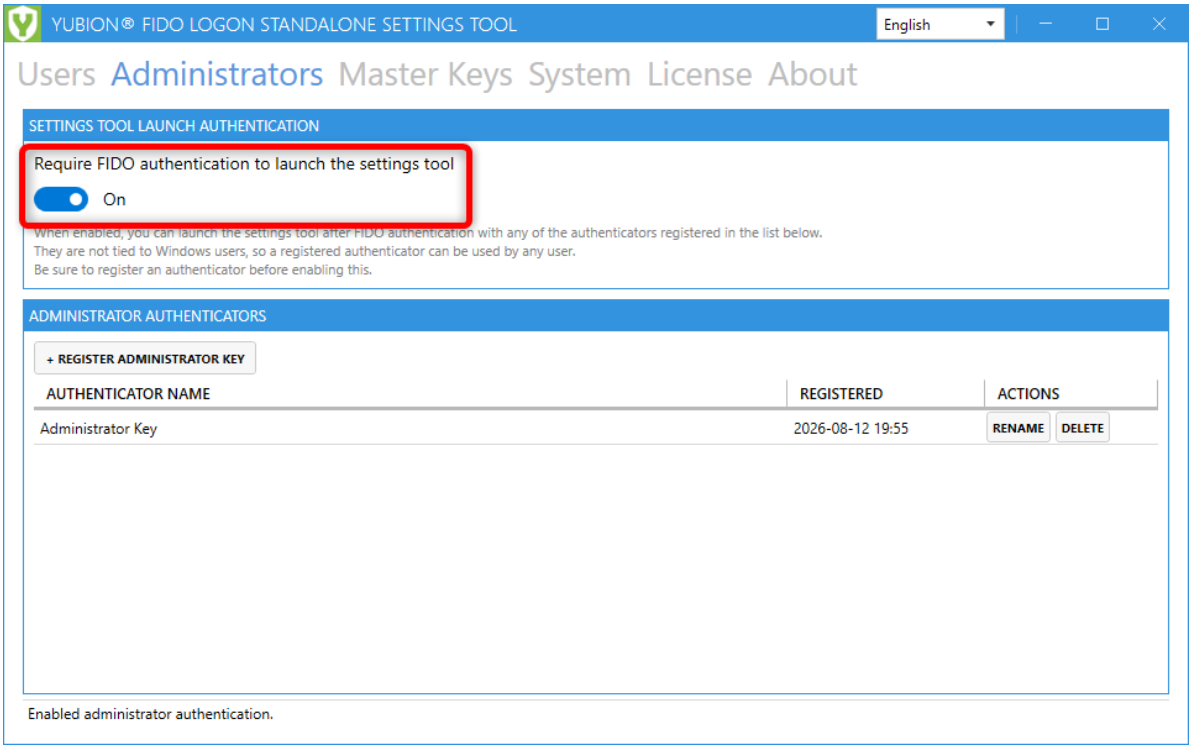

Figure: The FIDO authentication dialog at settings tool launch

- Administrator authenticators are **not tied to Windows users**. Once registered, an authenticator can be used no matter which user is signed in.
- Before turning this on, you must register **at least one** administrator authenticator (it cannot be turned on while none is registered).
- If you delete all registered administrator authenticators, this setting automatically turns itself off again (to prevent lockout).

6.1 Registering an Administrator Authenticator

1. Open the **Administrators** tab.

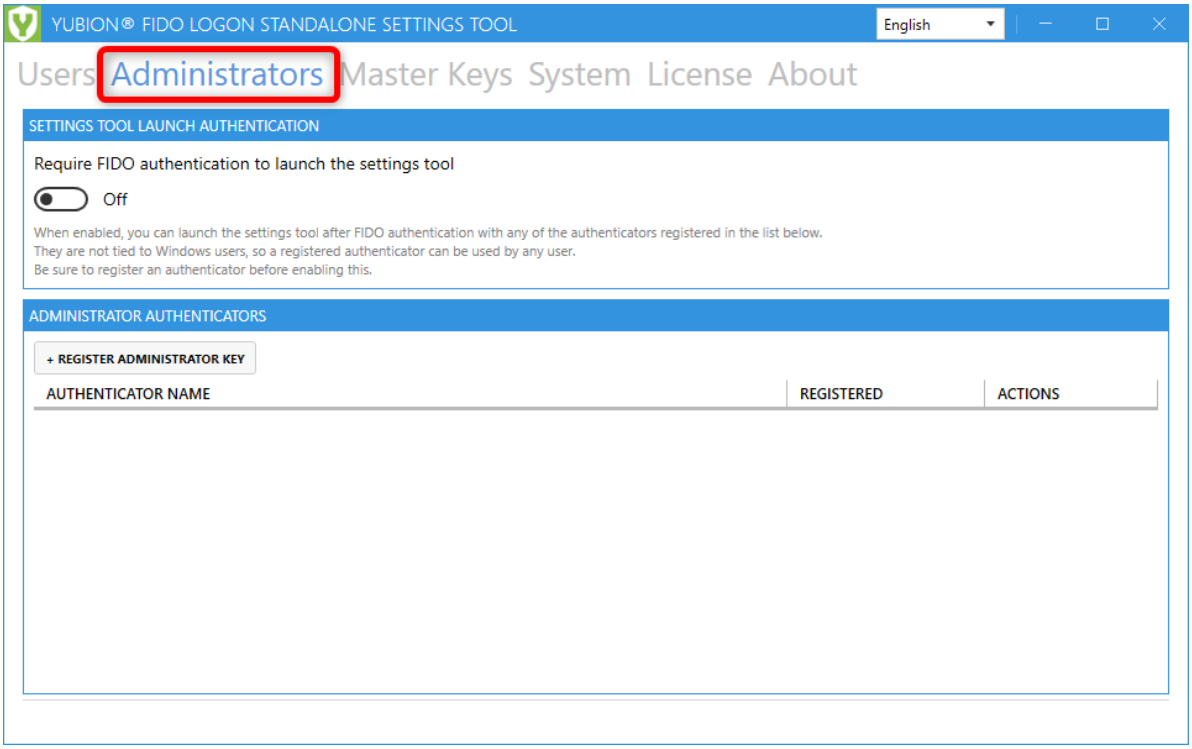

Figure: The Administrators tab

2. Select **+ Register Administrator Key**.

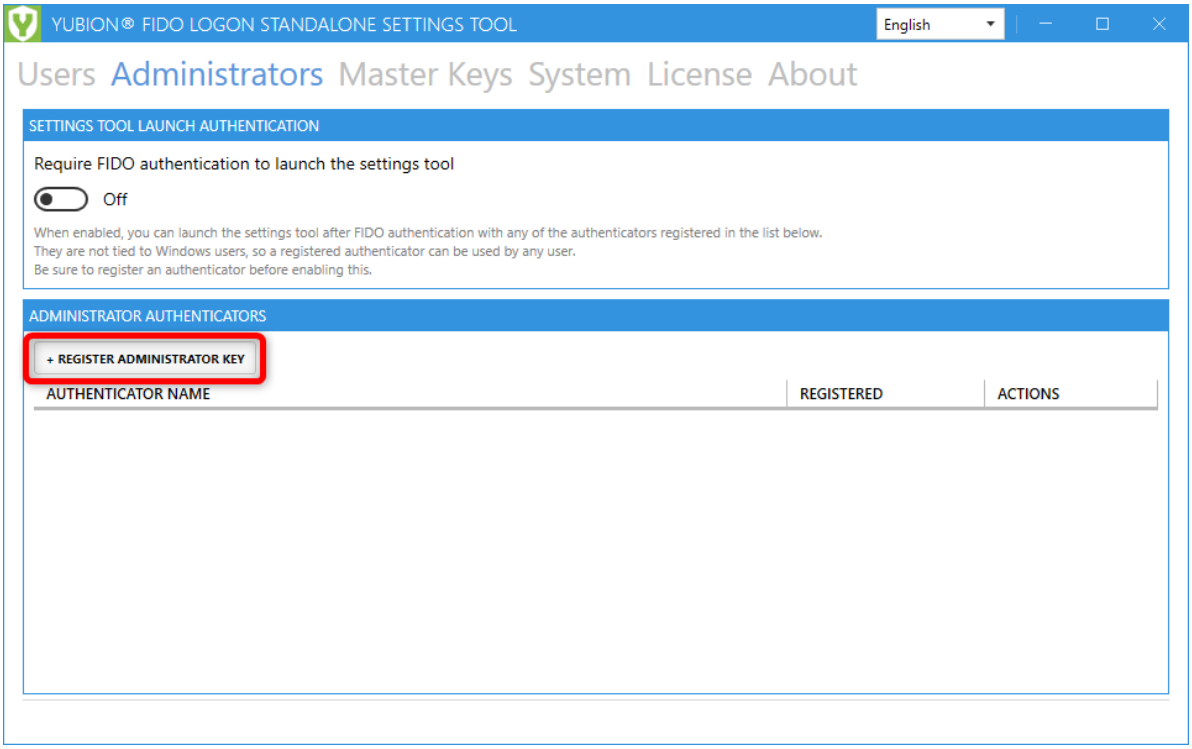

Figure: Selecting the "+ Register Administrator Key" button

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

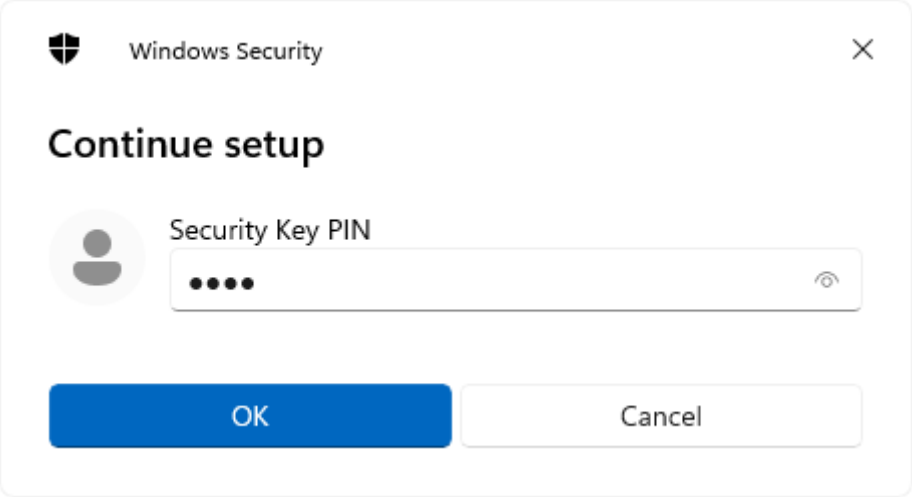

Figure: The PIN entry dialog

4. When registration finishes, the **Set Authenticator Name** dialog appears. Enter a name (if you cancel, the default name is kept and you can change it later with **Rename**).

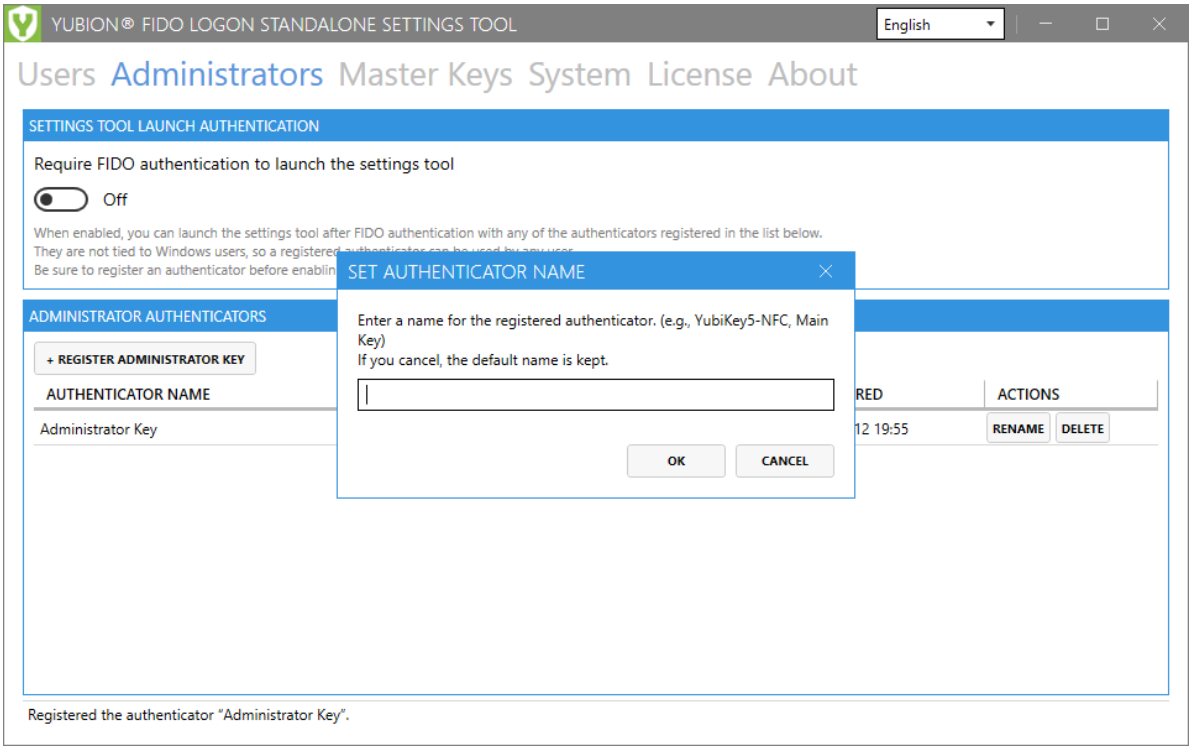

Figure: The Set Authenticator Name dialog

5. Confirm that it has been added to the **Administrator Authenticators** list.

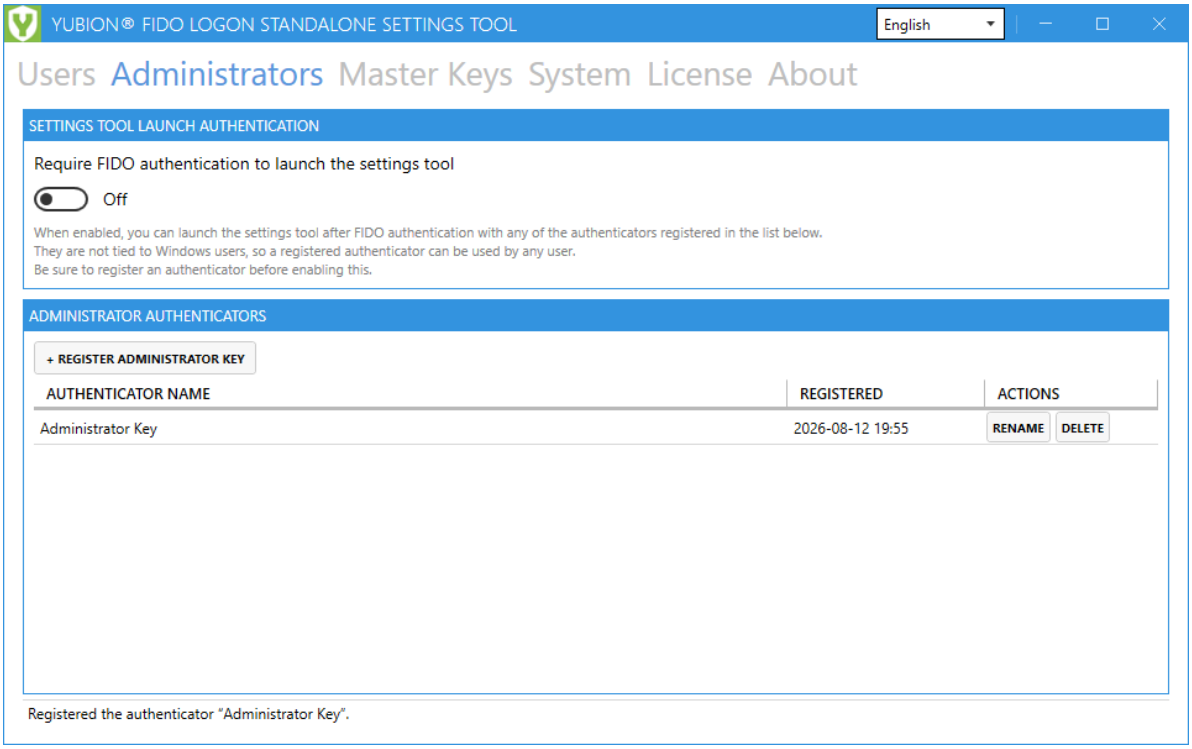

Figure: The administrator authenticator added to the list

Registered authenticators are managed with **Rename** and **Delete** in the **Actions** column of the list.

Chapter 7. Basic Settings

Enable FIDO logon and adjust its behavior to match your operational policy. Most settings are on the **System** tab.

> **Prerequisite** Before turning these settings on, you must register **at least one** authenticator that can be used for signing in (a user authenticator or a master key) (Chapter 8, Chapter 9).

7.1 Enabling Authenticator Logon

When you turn on **Enable authenticator logon (add this product's CP to sign-in options)** on the System tab, this product's Credential Provider is registered with Windows and the FIDO logon tile appears on the sign-in screen.

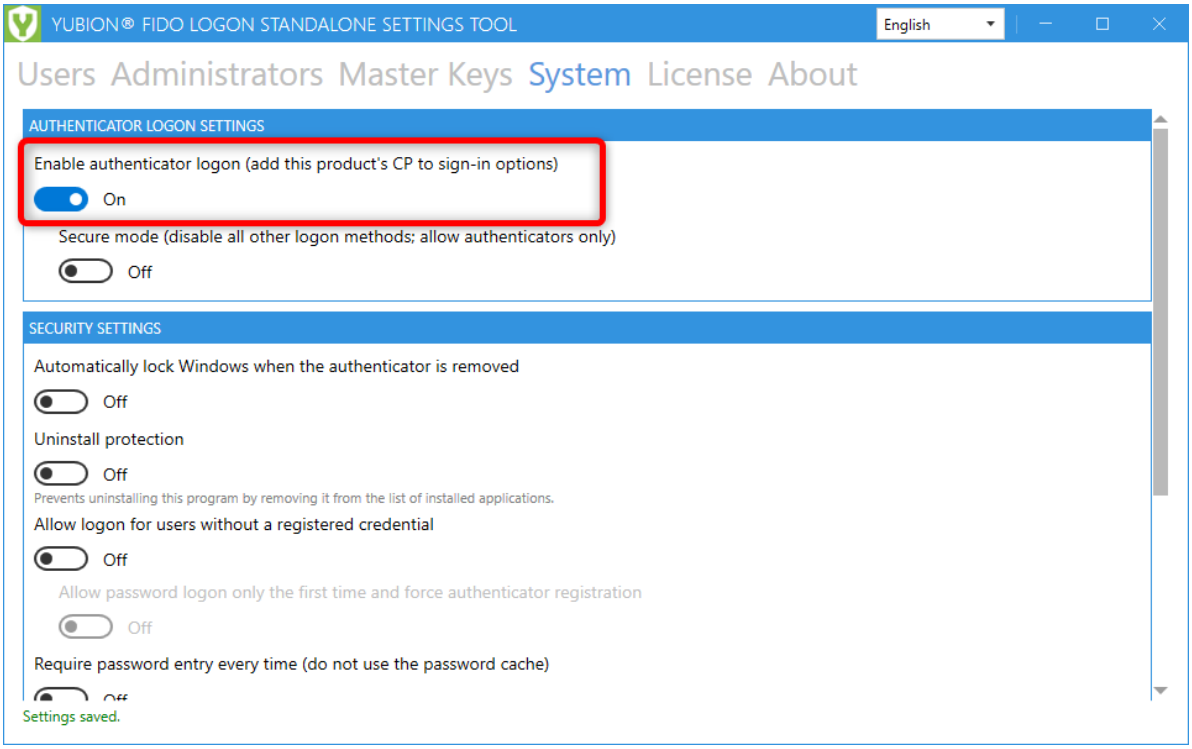

Figure: The Enable authenticator logon setting

- It cannot be turned on while there is not a single authenticator that can be used for signing in.
- If the number of user authenticators and master keys both reach zero, it automatically turns itself off again.

7.2 Secure Mode

Turning on **Secure mode (disable all other logon methods; allow authenticators only)** disables the other Credential Providers and restricts sign-in to this product's FIDO logon. This makes signing in with an authenticator mandatory.

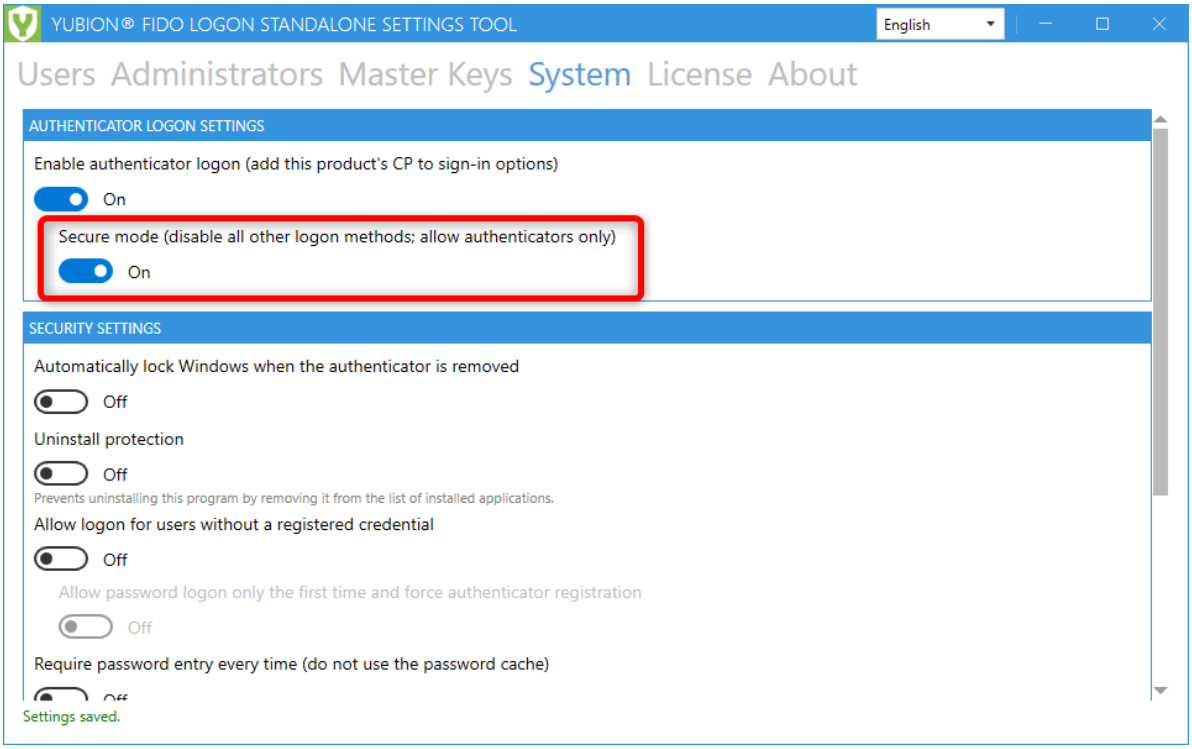

Figure: The Secure mode setting

- **Enable authenticator logon** is a prerequisite for turning it 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.

> **Caution** Once secure mode is on, users without a registered authenticator can no longer sign in with a password. Turn it on only after every target user has registered an authenticator. For emergencies, we recommend preparing a **master key** (Chapter 9) and **recovery codes** (Chapter 10).

7.3 Other Behavior Settings

The System tab also offers the following behavior settings. The setting names are the ones shown in the settings tool.

Setting	Default	Description
Automatically lock Windows when the authenticator is removed	Off	Locks Windows automatically when the authenticator is unplugged
Uninstall protection	Off	Hides the product from the app list to prevent accidental uninstallation

Setting	Default	Description
Require password entry every time (do not use the password cache)	Off	When on, the Windows password is required at every sign-in even after successful authentication with an authenticator, without using the cache
Allow non-UV keys (U2F)	Off	When on, U2F (CTAP1) keys may be registered and used for signing in (no password cache; password required every time)

7.3.1 Handling Users Without a Registered Authenticator

How users without a registered authenticator are treated is controlled by the following two settings.

- **Allow logon for users without a registered credential:** when on, users who have not registered an authenticator can still sign in with a password.
- **Allow password logon only the first time and force authenticator registration:** when on, an unregistered user can sign in with a password the first time only, and is prompted to register an authenticator at that point.

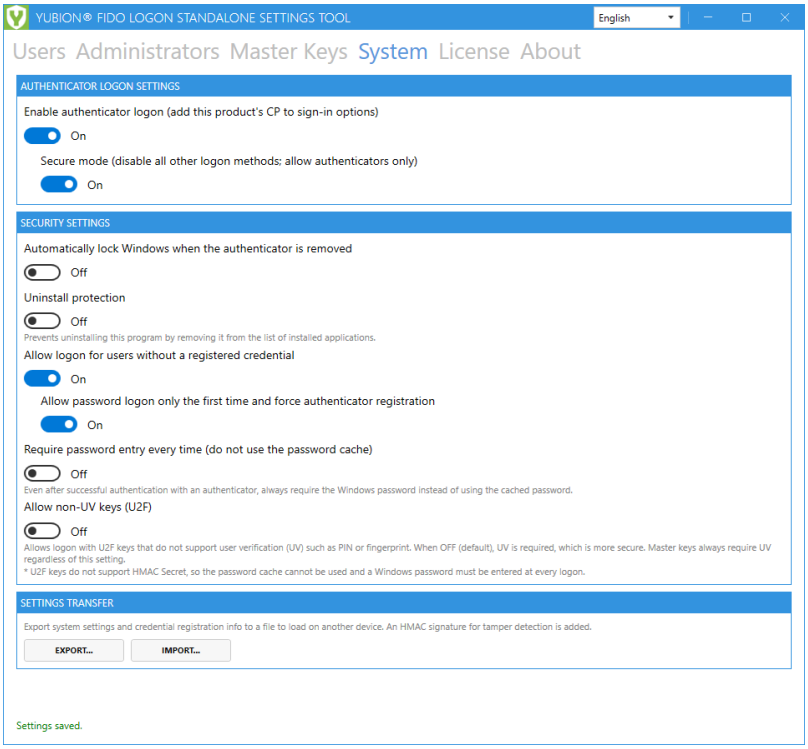

Figure: The System tab

Chapter 8. Registering and Managing User Authenticators

The authenticators users employ for FIDO logon are managed on the **Users** tab of the settings tool.

8.1 Registration Methods

There are two ways to register an authenticator. Choose the one that fits your operation.

1. **Pre-registration by the administrator:** the administrator registers the target user's authenticator from the settings tool (see "Registering an Authenticator (Pre-Registration by the Administrator)" in this chapter).
2. **Self-registration by the user:** the user registers their own authenticator at first sign-in (see "Letting Users Register Their Own Authenticator (Self-Registration)" in this chapter). This suits situations with many users, where pre-registering computer by computer is impractical.

8.2 Registering an Authenticator (Pre-Registration by the Administrator)

1. Open the **Users** tab.

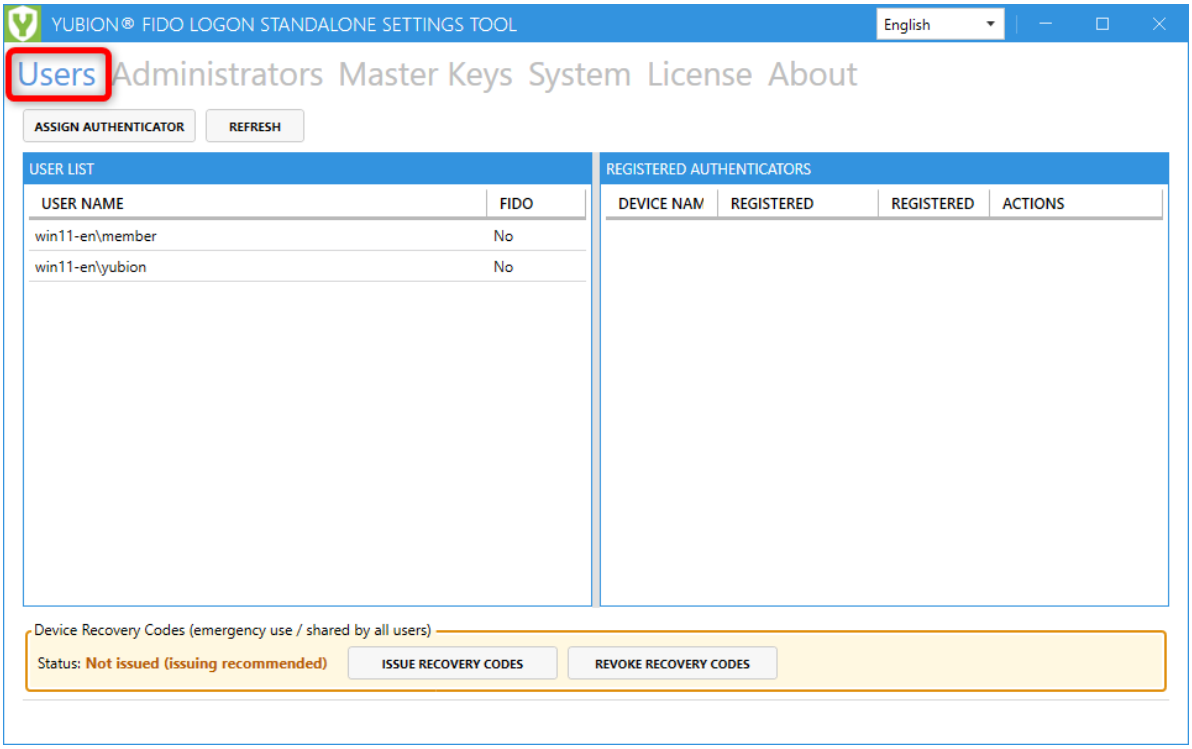

Figure: The Users tab

2. Select the target Windows account.

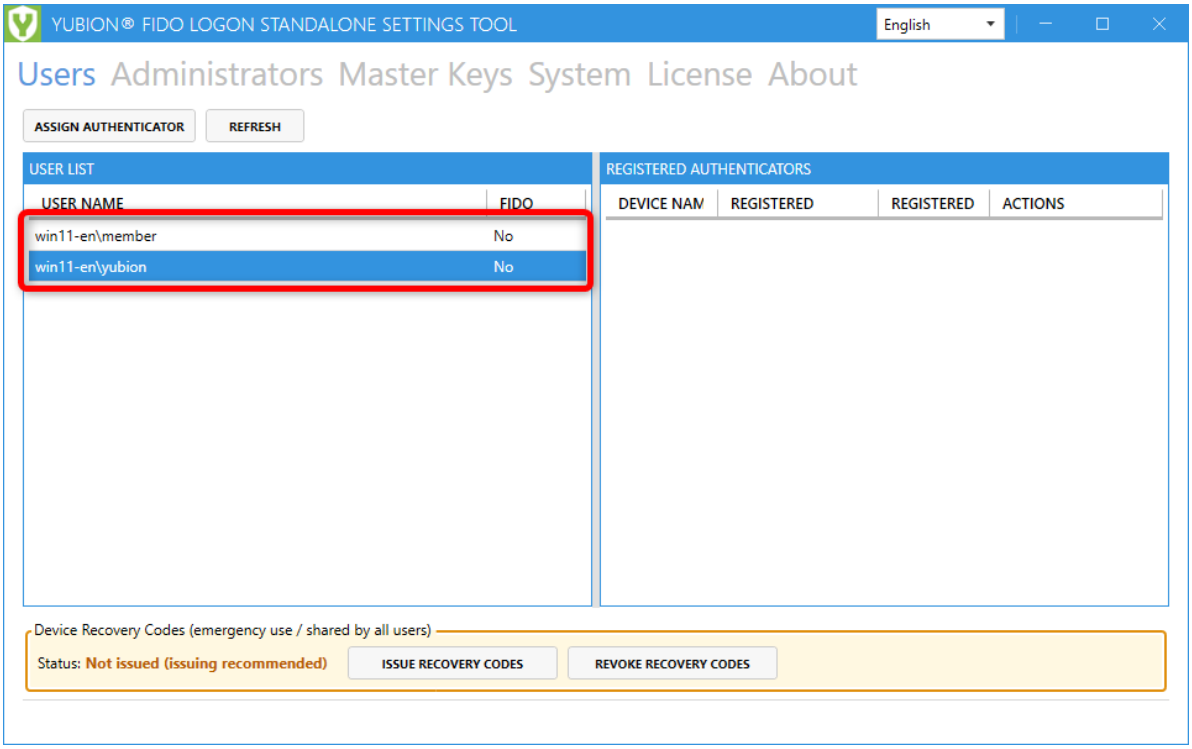

Figure: Selecting the target Windows account

3. Select **Assign Authenticator**.

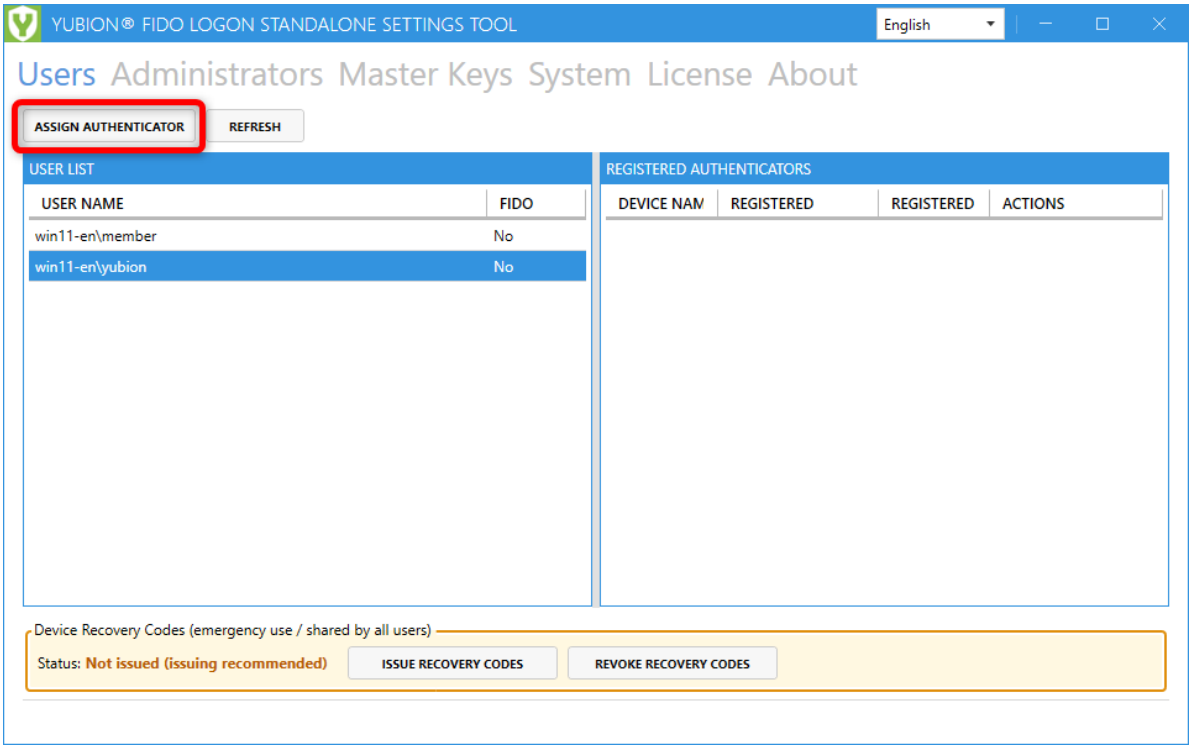

Figure: Selecting the "Assign Authenticator" button

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

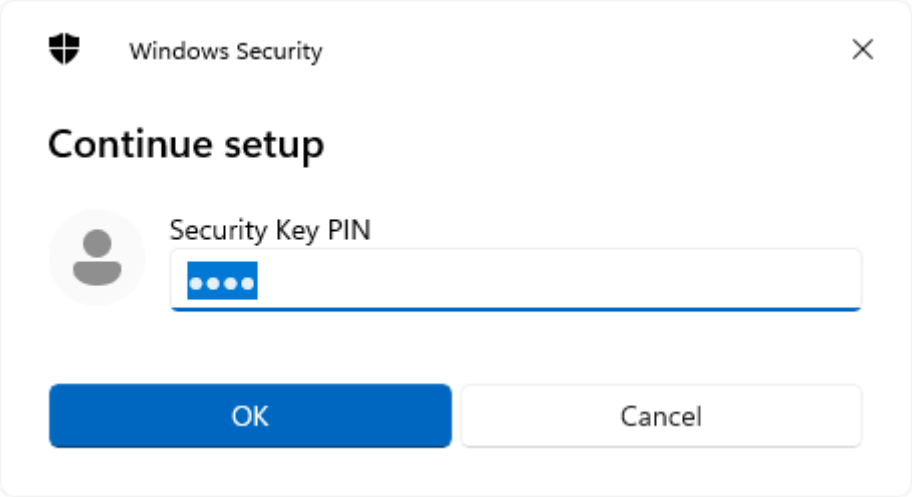

Figure: The PIN entry dialog

5. When registration finishes, the **Set Authenticator Name** dialog appears. Enter a name (for example, YubiKey5-NFC or Main Key). If you cancel, the default name is kept and you can change it later with **Rename**.

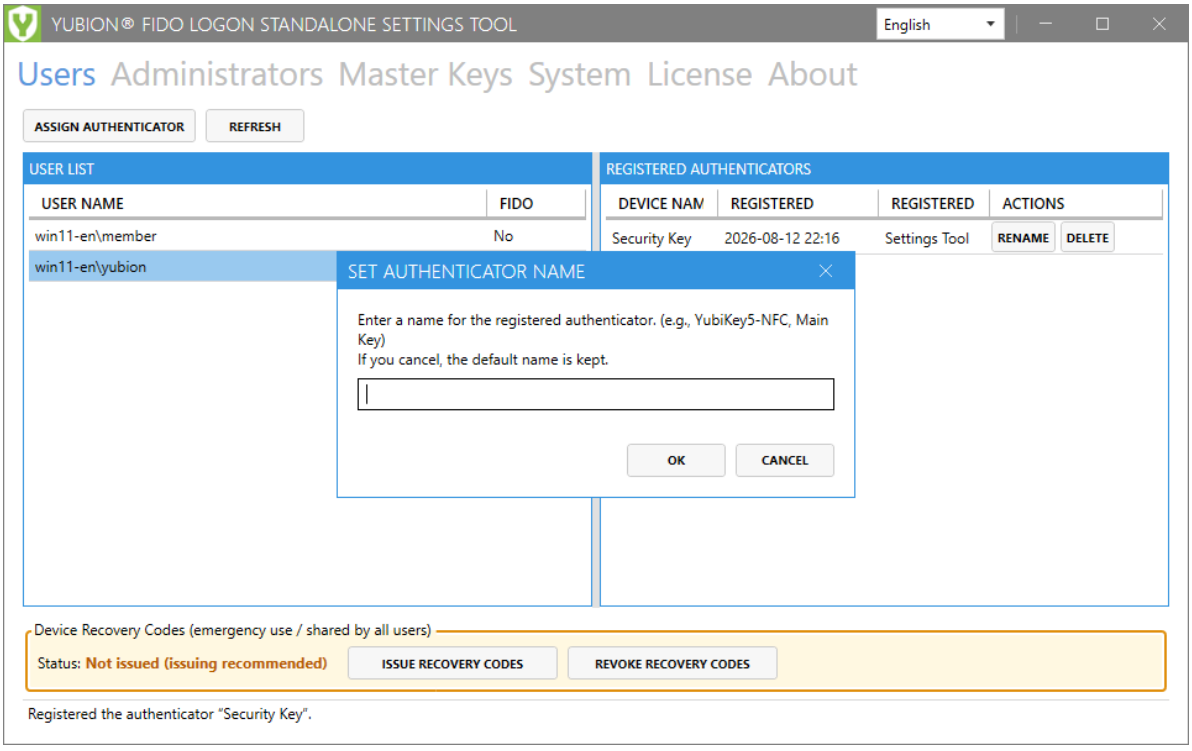

Figure: The Set Authenticator Name dialog

6. Confirm that the authenticator has been added to the **Registered Authenticators** list.

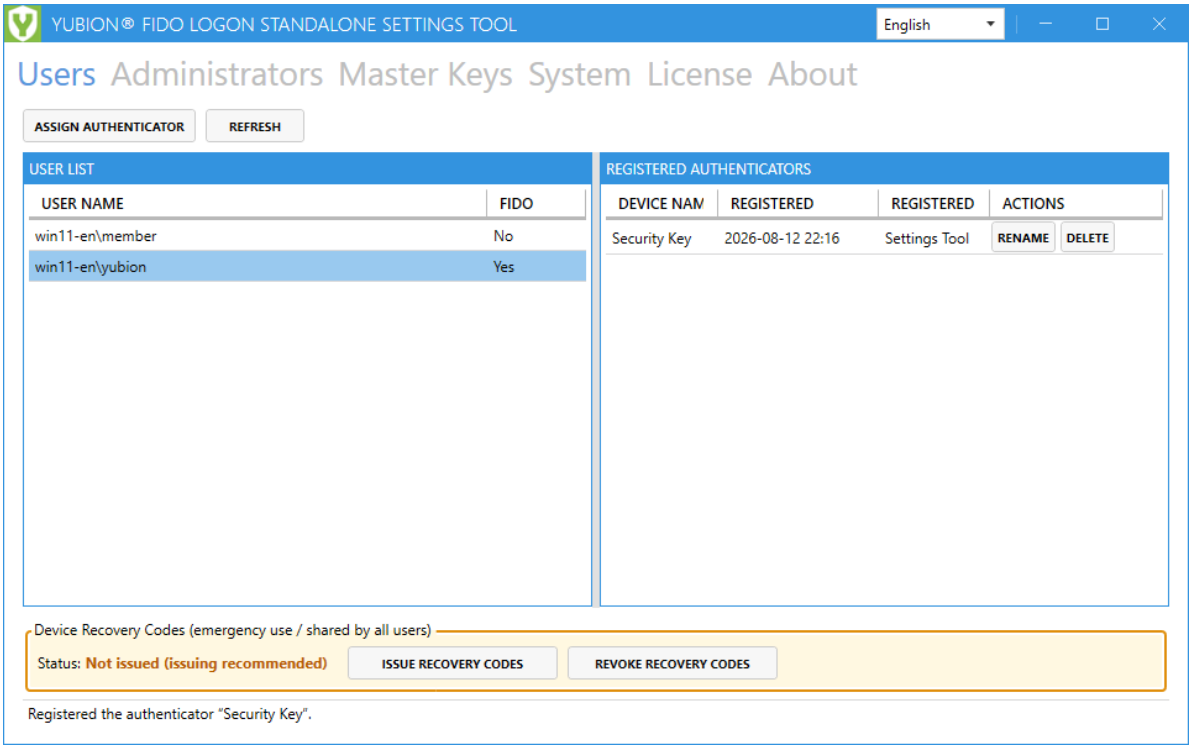

Figure: The authenticator added to the Registered Authenticators list

Note Account names in the user list are shown 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`

Important The user list in the settings tool shows only **accounts that already have a user profile** on that computer (that is, accounts that have signed in to it at least once). A user who has never signed in does not appear in the list and cannot be assigned an authenticator. To pre-register for such a user, have them sign in to that computer once first so that a profile is created.

Important (the Windows "Passkey access" setting) If **Passkey access** under **Settings → Privacy & security → Passkeys** in Windows is **off**, **an authenticator cannot be assigned (registered)**. This product's settings tool uses the Windows WebAuthn feature to register authenticators, so it is blocked by this setting. Turn **Passkey access on** before registering.

This setting is per computer (per signed-in user). While it is off, all of the following operations in the settings tool fail.

- Registering an authenticator (this section)
- Registering a master key (Chapter 9)
- Registering an administrator credential and launch authentication (Chapter 6 "Launch Authentication for the Settings Tool (Optional)")

Note that this setting item exists only in relatively recent versions of Windows 11. If you do not see a "Passkeys" item in Settings, this restriction does not apply.

8.3 Letting Users Register Their Own Authenticator (Self-Registration)

If, instead of pre-registering, you want **each user to register their own authenticator at first sign-in**, configure the following. Users without a registered authenticator can then sign in with a password the first time only, and are prompted to register an authenticator at that point.

8.3.1 Required Settings

Configure the **System** tab as follows (for details of each setting, see Chapter 7).

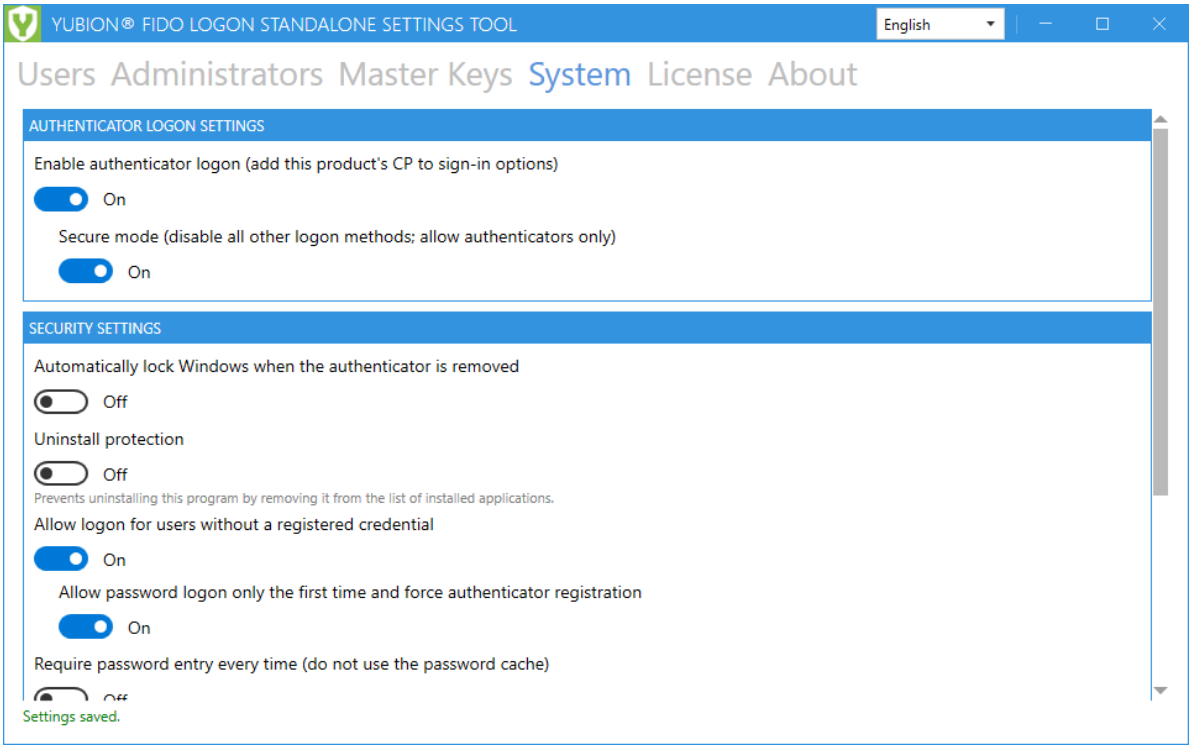

Figure: The system settings required for self-registration

Step	Setting	Value
1	Enable authenticator logon	ON
2	Allow logon for users without a registered credential	ON
3	Allow password logon only the first time and force authenticator registration	ON
4 (recommended)	Secure mode	ON

- Step 3 can be configured only while step 2 (allow) is ON.
- **Why step 4 (secure mode) is recommended:** if secure mode stays off, the standard Windows password tile is also shown on the sign-in screen, and users can sign in without registering an authenticator. Turning secure mode on hides the other sign-in methods and reliably steers users into self-registration.

> **Prerequisite for initial deployment** Step 1 (Enable authenticator logon) cannot be turned on while there is not a single authenticator usable for signing in. In an initial deployment where nobody has registered an authenticator yet, registering one **master key** (Chapter 9) as the administrator satisfies this condition.

8.3.2 Setting Combinations and Behavior

The behavior for users without a registered authenticator depends on the combination of "allow" and "force".

Allow logon for users without a registered credential	Allow password logon only the first time...	Behavior for unregistered users
OFF	–	Cannot sign in with a password (with secure mode ON, only an informational tile is shown)
ON	OFF	Can sign in with a password only (**no authenticator registration is requested**)
ON	ON	Signs in with a password the first time and **is asked to self-register an authenticator** at that point

> **Caution** If you turn only "allow" ON and leave "force" OFF, users can sign in with a password alone and are never prompted to register an authenticator. There is no screen for registering at an arbitrary time after signing in, so **if you want self-registration, turn both "allow" and "force" ON**.

8.3.3 What the User Does

With self-registration enabled, the first sign-in of a user without a registered authenticator proceeds as follows.

1. The user enters their password and signs in.

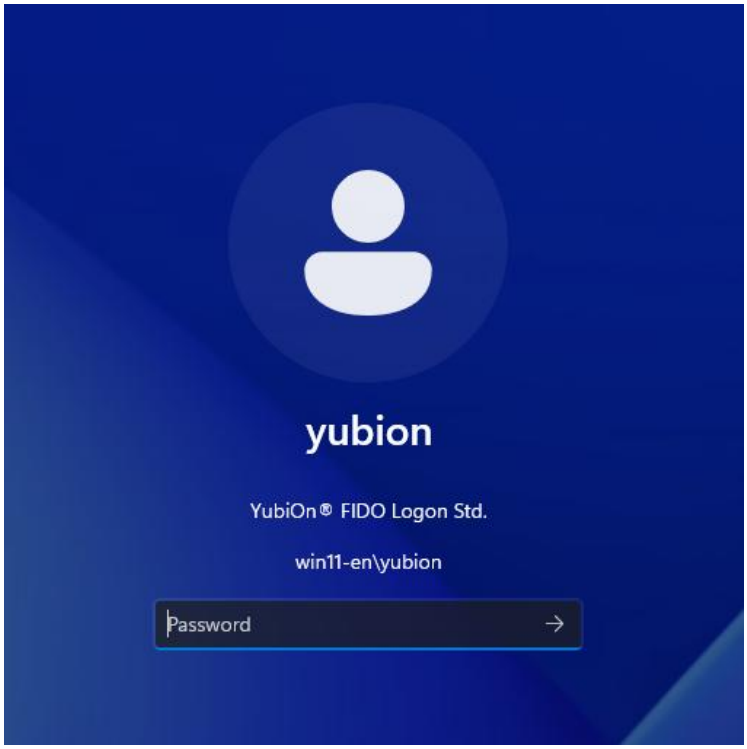

Figure: The password entry screen

2. The user is asked to register an authenticator, and connects one.

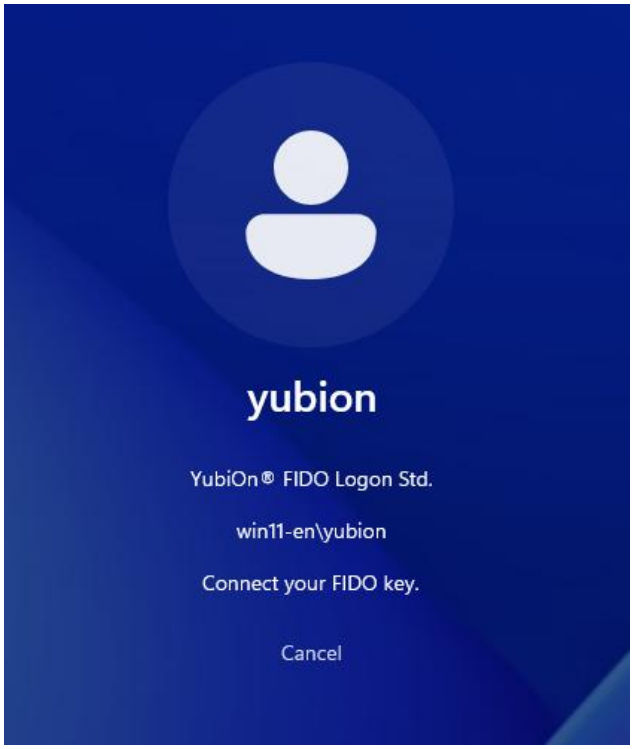

Figure: The screen asking the user to connect an authenticator

3. If no PIN is set, the user sets one.

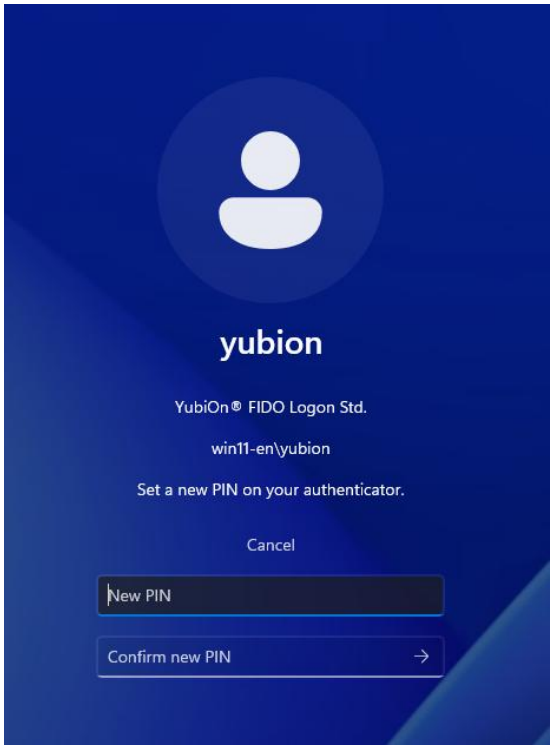

Figure: The PIN setup screen

4. The user touches the authenticator to complete registration.

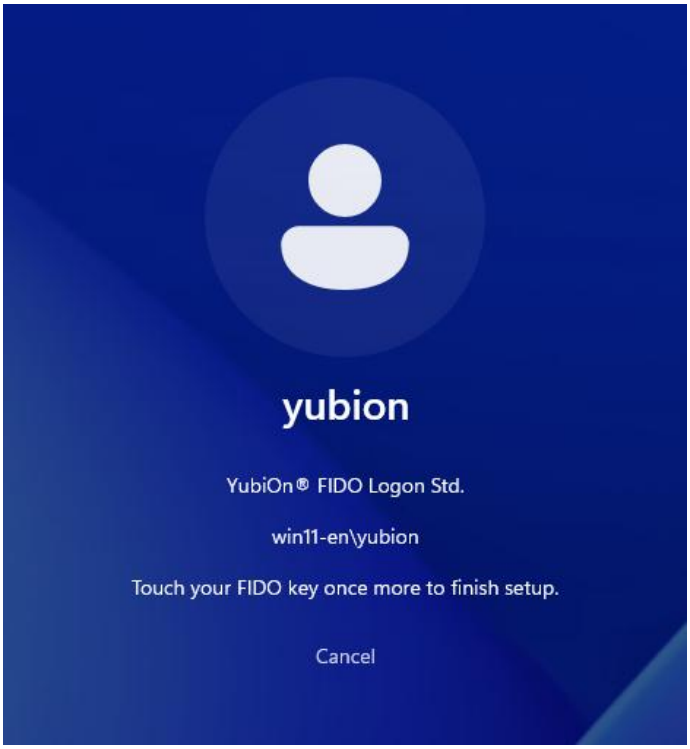

Figure: The screen asking the user to touch the authenticator

5. The sign-in then completes. From the second time on, it is an ordinary FIDO sign-in.

For the exact screen-by-screen steps, see "Registering Your Authenticator" in the separate **End User Guide**.

8.3.4 Points to Note

- **Domain and Entra ID accounts:** these accounts are normally not shown as tiles on the sign-in screen, so users self-register by typing their account name under **Other user**.
- **Relationship with master keys:** master key sign-in on a user's behalf is not offered for unregistered users who are subject to self-registration (priority is given to having the user register).

8.4 Deleting and Renaming Authenticators

- Use **Delete** in the **Actions** column of the **Registered Authenticators** list on the **Users** tab to remove an authenticator assignment.
- Use **Rename** in the same **Actions** column to give an authenticator an easily identifiable name.

> **Caution** If the number of user authenticators and master keys both reach zero, **Enable authenticator logon** and **Secure mode** are turned off automatically.

8.5 Preparing for Authenticator Lockout Caused by Wrong PIN Entry

A FIDO2 authenticator **locks when the PIN is entered incorrectly several times in a row, and**

eventually becomes unusable until it is reset (initialized). This is a characteristic of the authenticator itself, and **this product cannot unlock it**. Resetting also erases all credentials inside the authenticator, so **it must be registered with this product again**.

The lock proceeds in two stages.

Stage	State	Message on the sign-in screen	How to recover
Temporary block	The PIN was entered incorrectly several times in a row (typically 3 times)	"PIN authentication is blocked. Remove the security key and insert it again."	Remove the authenticator and insert it again, and the PIN can be entered once more
Permanent block	Wrong entries continued until no attempts remained (typically 8 in total)	"The PIN is blocked. Please reset the security key."	**The authenticator must be reset.** The credentials are lost and re-registration is required

> **Caution** The maximum number of attempts depends on the authenticator's specifications. In addition, **the number of remaining attempts is not shown on the sign-in screen**. Users cannot tell how many attempts they have left, so they may reach a permanent block without noticing.

For this reason, **avoid relying on a single authenticator and prepare the following in advance.**

Preparation	Summary	Reference
Register a spare authenticator	The same user can have two or more authenticators registered (there is no upper limit). If one locks, they can sign in as usual with the other. This is **the most reliable preparation** and does not inconvenience the user.	"Registering an Authenticator (Pre-Registration by the Administrator)" in this chapter
Register a master key	Lets an administrator sign in on behalf of any account. This is your means of recovery when a user's authenticator locks.	Chapter 9
Issue recovery codes	Allow emergency sign-in **without using an authenticator at all**. They are unaffected by an authenticator lock.	Chapter 10

Important A master key is also a FIDO2 authenticator with a PIN and can lock in the same way. Do not rely on a single master key; **issue recovery codes as well**. Recovery codes, which allow signing in without an authenticator, are the most effective last resort against an authenticator lock.

Warning This product **cannot detect that an authenticator has been PIN-locked**. The automatic turning off of "authenticator logon" and "secure mode" (see the caution in the previous section) happens when **the number of registrations reaches zero**, for example through deletion in the settings tool; an authenticator that is still registered but locked is still counted as "one registered". Therefore, **if secure mode is on and every registered authenticator and master key becomes PIN-locked while no recovery codes have been issued, you will no longer be able to sign in to that computer (lockout).** This state cannot be recovered by changing settings in this product, so **be sure to prepare as described above.**

Chapter 9. Managing Master Keys

A **master key** is an **administrator FIDO authenticator that can sign in to any account**, regardless of assignment to a Windows account. It is managed on the **Master Keys** tab of the settings tool.

9.1 What It Is For

- Temporary access to accounts such as those of departed employees
- Signing in on a user's behalf when their authenticator has failed, been lost, or **become unusable through a PIN lock**
- Signing in for administrative work

9.2 Characteristics and Limits

- Up to **3 keys** can be registered per computer.
- Registration is possible **only through the settings tool** (users cannot self-register a master key).
- **UV (PIN or biometrics) is always required**, both at registration and at authentication (regardless of the settings).

9.3 Registration Steps

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

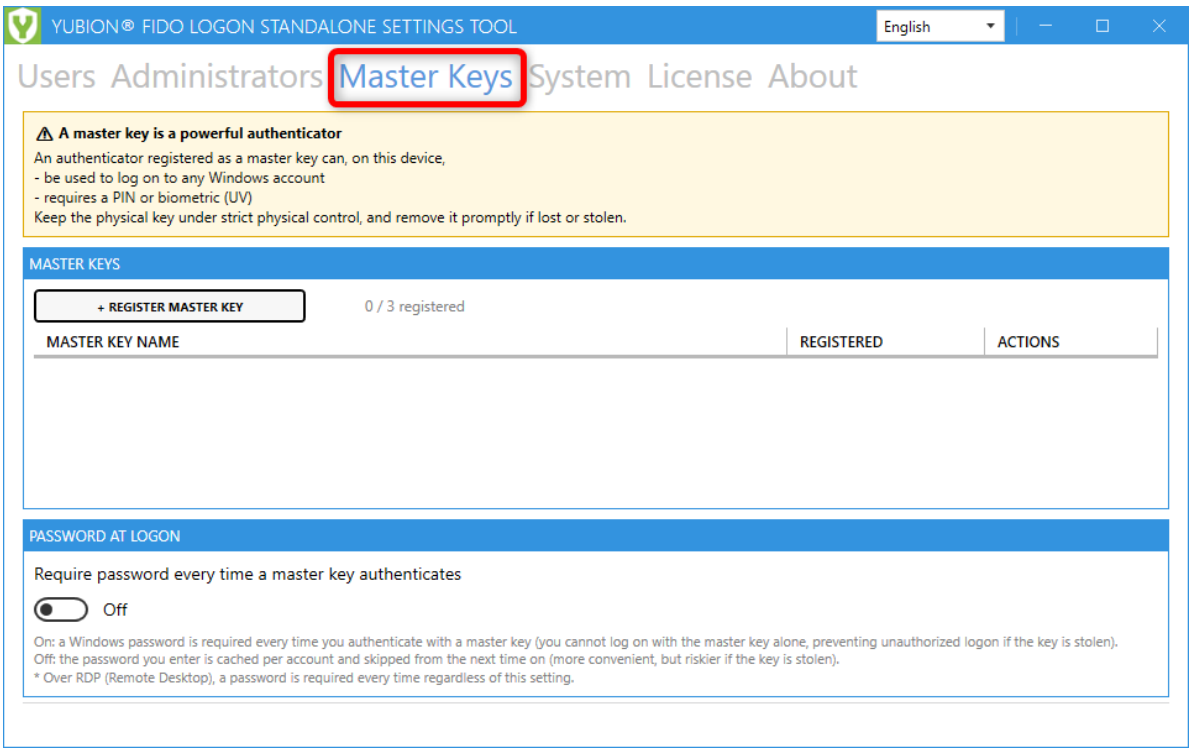

Figure: The Master Keys tab

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

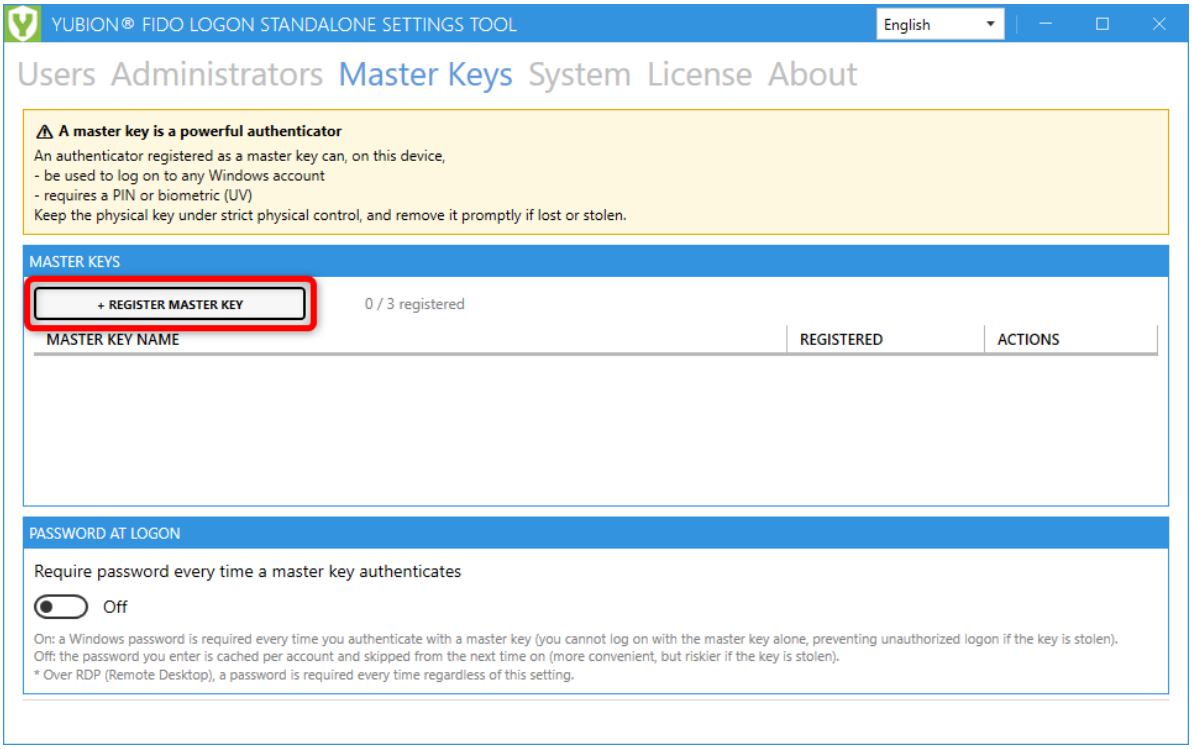

Figure: Selecting the "+ Register Master Key" button

3. A confirmation dialog appears stating that the key can sign in to any Windows account. Read it and select **Yes**.

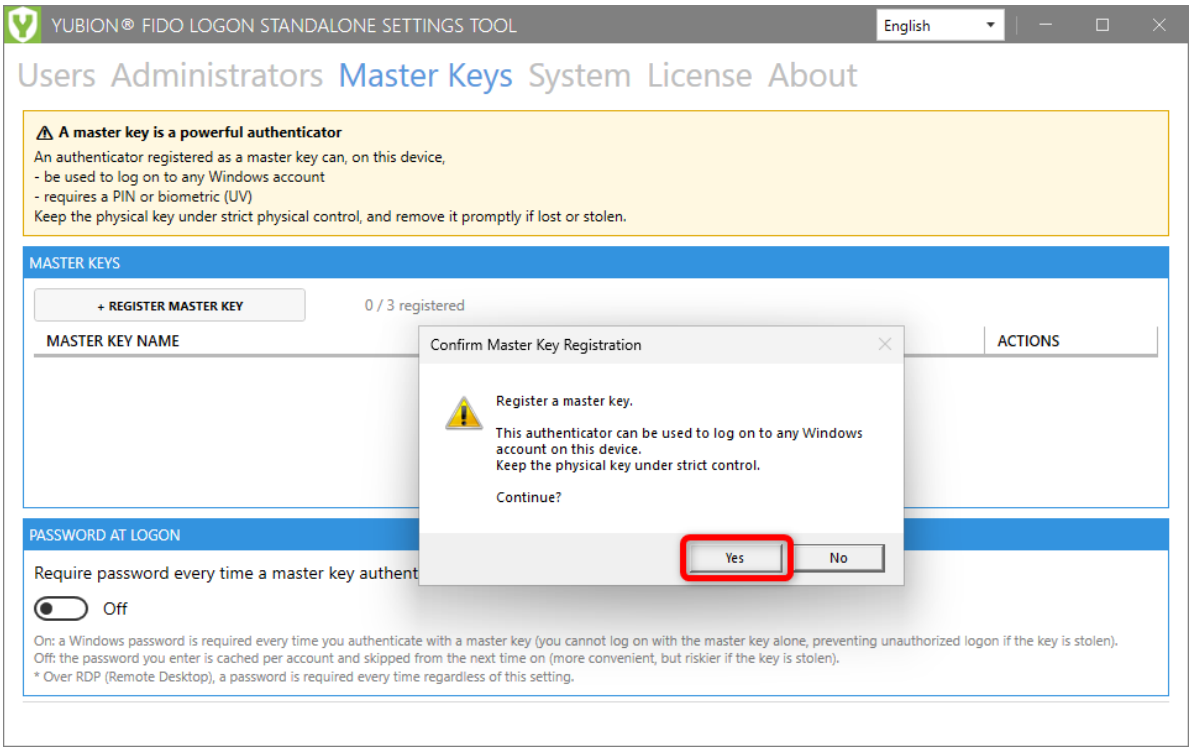

Figure: The master key registration confirmation dialog

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

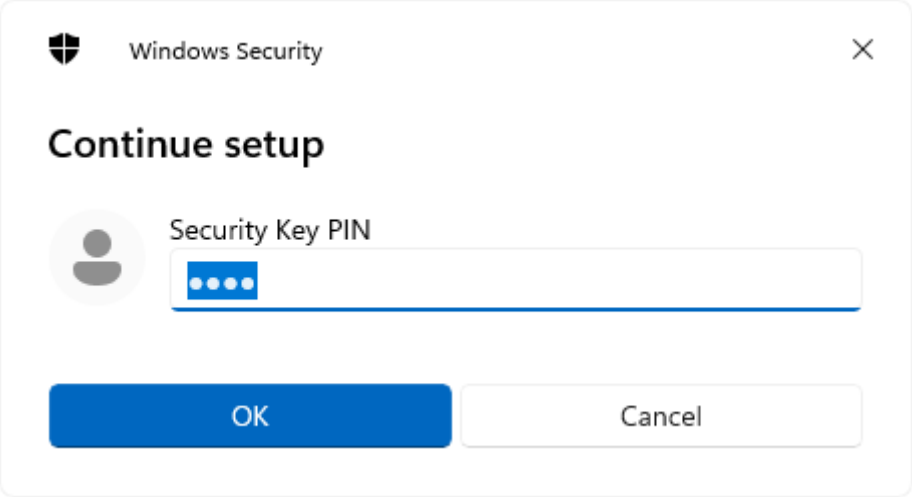

Figure: The PIN entry dialog

5. When registration finishes, the **Set Master Key Name** dialog appears. Enter a name (for example, Admin YubiKey or Backup Key). If you cancel, the default name is kept and you can change it later with **Rename**.

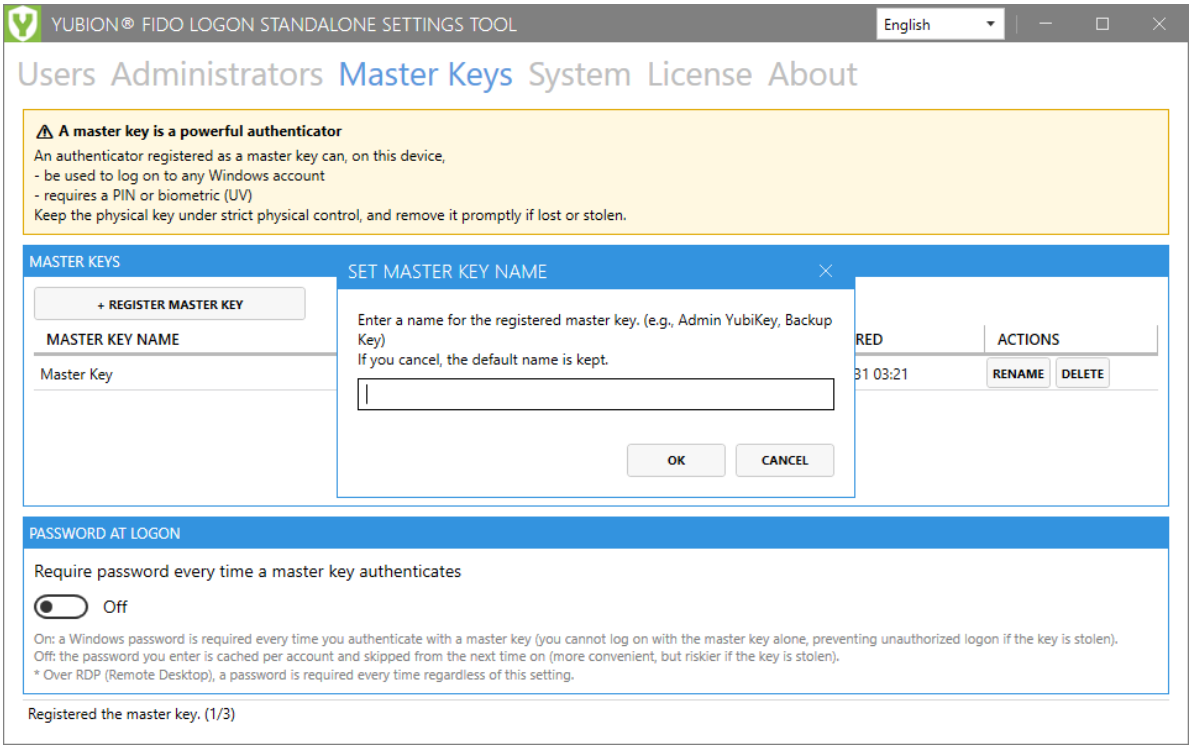

Figure: The Set Master Key Name dialog

6. Confirm that it has been added to the master key list.

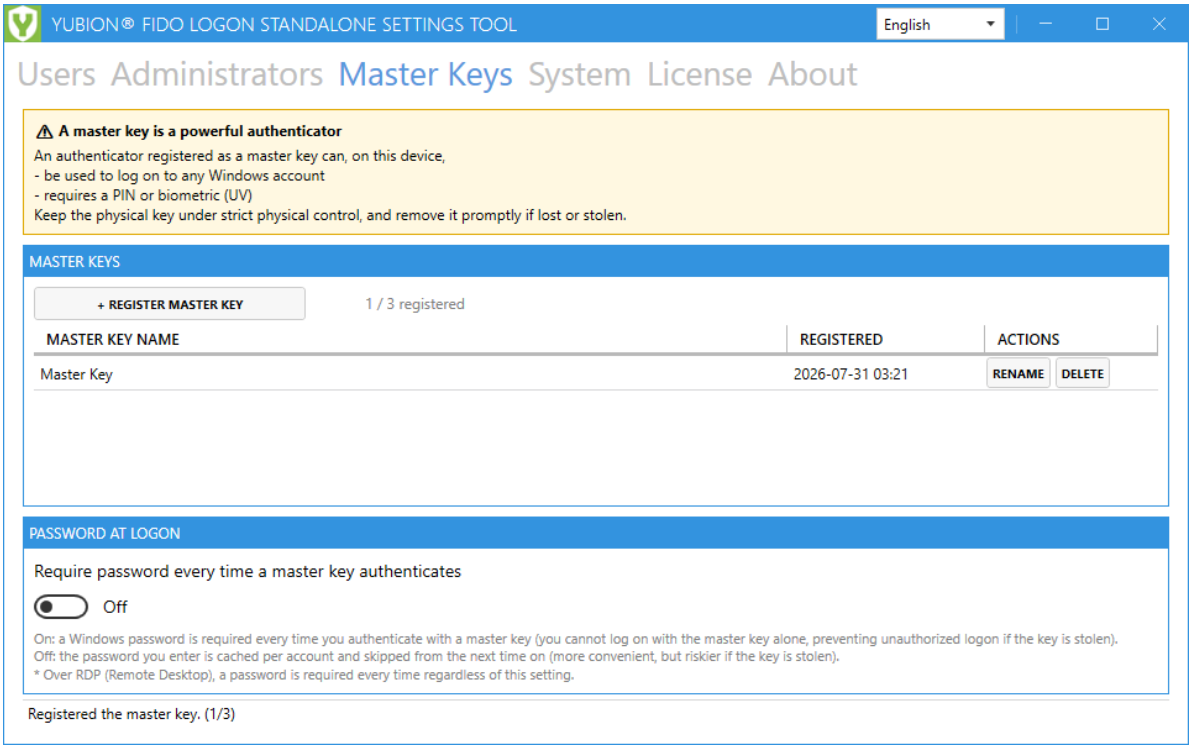

Figure: The master key added to the list

Caution A master key cannot be registered while **Passkey access** under **Settings** → **Privacy & security** → **Passkeys** in Windows is off (see the caution in Chapter 8 "Registering an Authenticator (Pre-Registration by the Administrator)").

9.4 Operational Cautions

- A master key should be **kept under personal physical control and not shared**.
- **If a master key is lost, delete it from the settings tool promptly.** Until it is deleted, that key can sign in to any account. If one is lost, also consider changing the passwords of all users.
- Whether a password is required every time a master key authenticates is controlled by **Require password every time a master key authenticates**, in the **Password at Logon** group at the bottom of the **Master Keys** tab (off by default, meaning the cache is used).

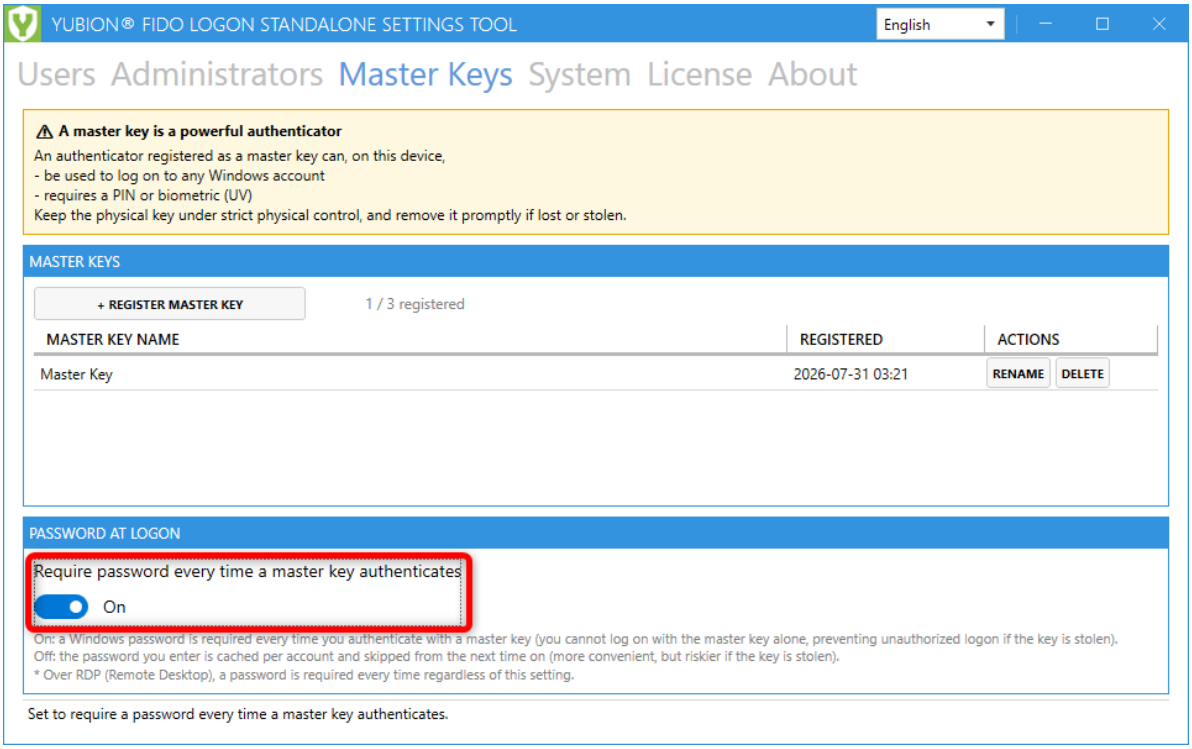

Figure: The "Require password every time a master key authenticates" setting

Chapter 10. Managing Recovery Codes

Recovery codes are single-use codes for emergency sign-in when an authenticator cannot be used. They are managed in the **Device Recovery Codes (emergency use / shared by all users)** group at the bottom of the **Users** tab of the settings tool.

> **Important (issue them on every computer as a rule)** Recovery codes are the only way to sign in **without using an authenticator at all**. An authenticator locks after repeated wrong PIN entries and becomes unusable until it is reset, but **this product cannot detect that lock, so the automatic turning off of "authenticator logon" does not happen either**. If every registered authenticator and master key locks and no recovery codes have been issued, **a computer with secure mode on can no longer be signed in to, and no settings change in this product can restore access**. Even when you prepare spare authenticators or master keys, those can lock in the same way, so **treat issuing recovery codes as a mandatory step when deploying a computer** (for details, see Chapter 8 "Preparing for Authenticator Lockout Caused by Wrong PIN Entry").

10.1 Characteristics

- They are issued **per computer (shared by all users)**. Any user on the computer can use them.
- They are issued **10 at a time, always**.
- Each code can be used **only once**.
- A code is 16 alphanumeric characters (hyphenated every 4 characters) and has ample strength (about 78 bits).
- A recovery code alone is not enough to sign in; **the Windows password is always required as well**.

10.2 Issuing Recovery Codes

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

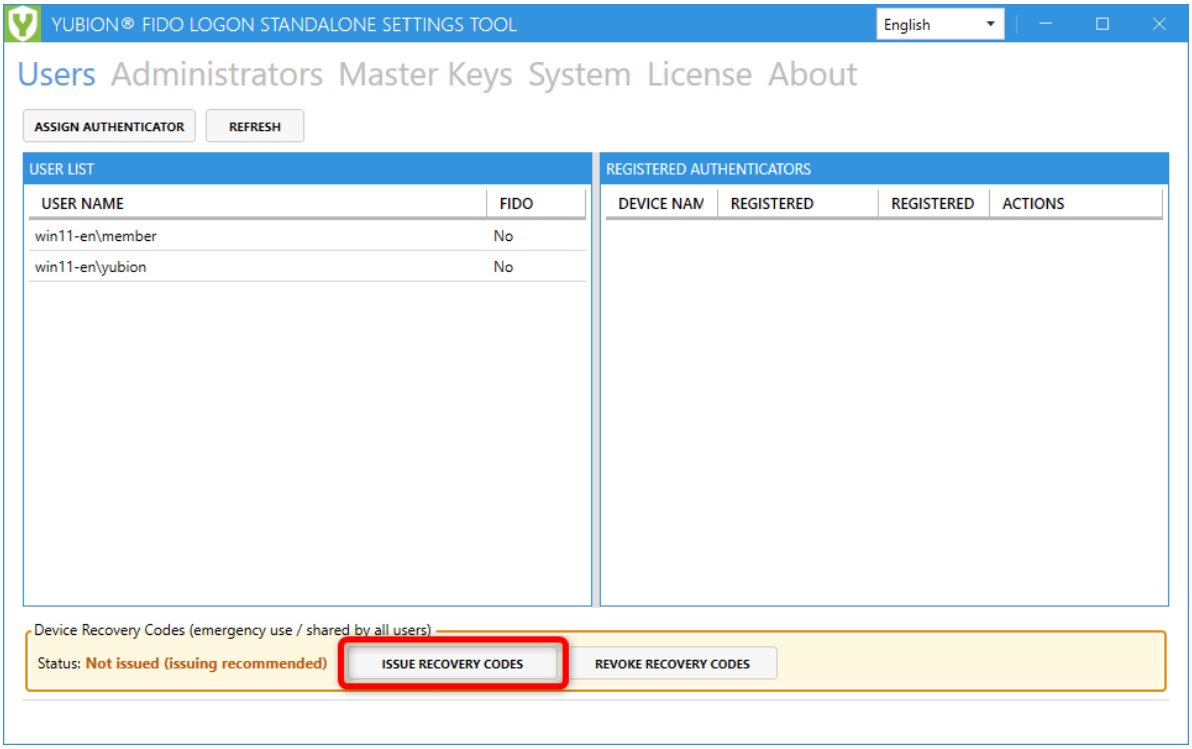

Figure: The Issue Recovery Codes button

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

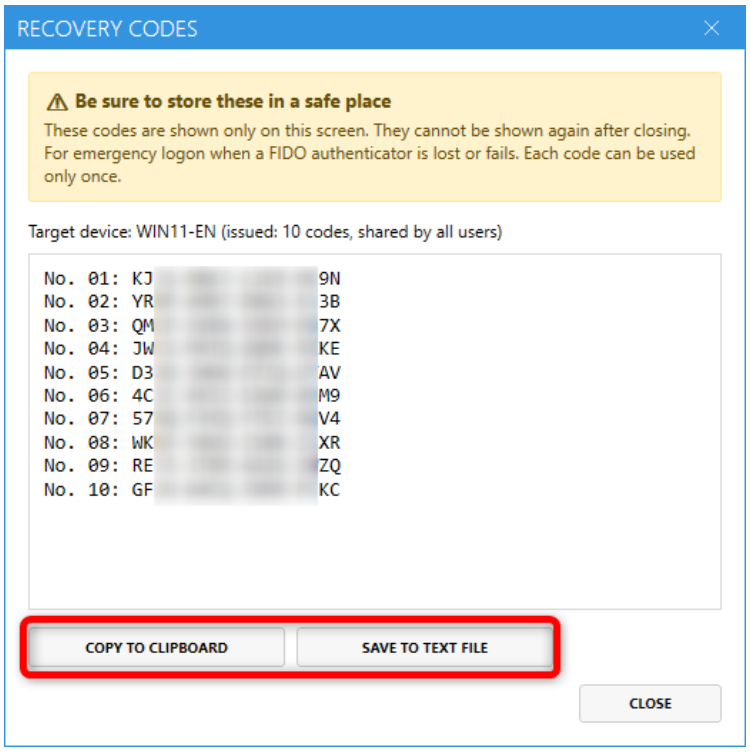

Figure: The recovery code dialog

Important The codes are **shown only once, right after they are issued**. They cannot be shown again after you close the screen. Be sure to store them at this point. Only verification hashes are stored on the computer, not the codes themselves.

10.3 Reissuing and Revoking

- **Reissue:** selecting **Issue Recovery Codes** while codes have already been issued shows a reissue confirmation dialog. Continuing invalidates all existing codes and then issues 10 new ones.

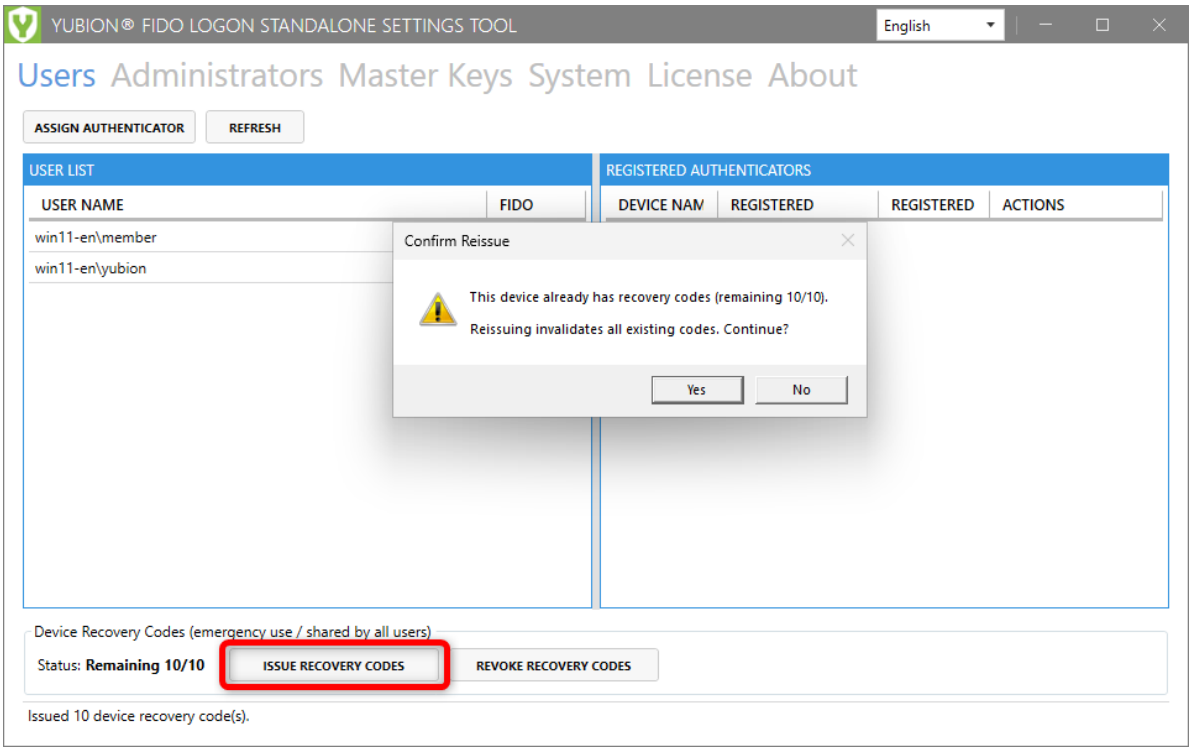

Figure: The reissue confirmation dialog

- **Revoke:** selecting **Revoke Recovery Codes** invalidates all issued codes.

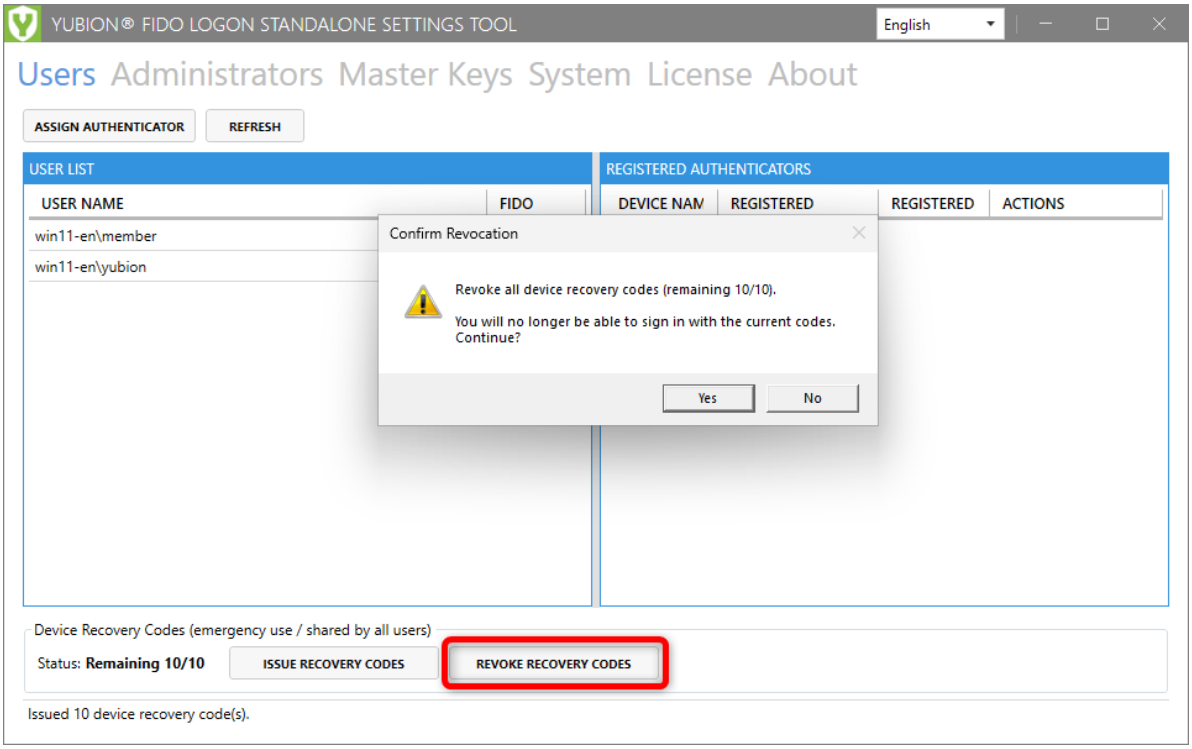

Figure: The revoke confirmation dialog

10.4 Status Display

The recovery code status is shown to the right of **Status:**. When none have been issued, **Not issued (issuing recommended)** is shown and the whole group is highlighted in a warning color. When codes have been issued, it shows something like **Remaining 10/10**.

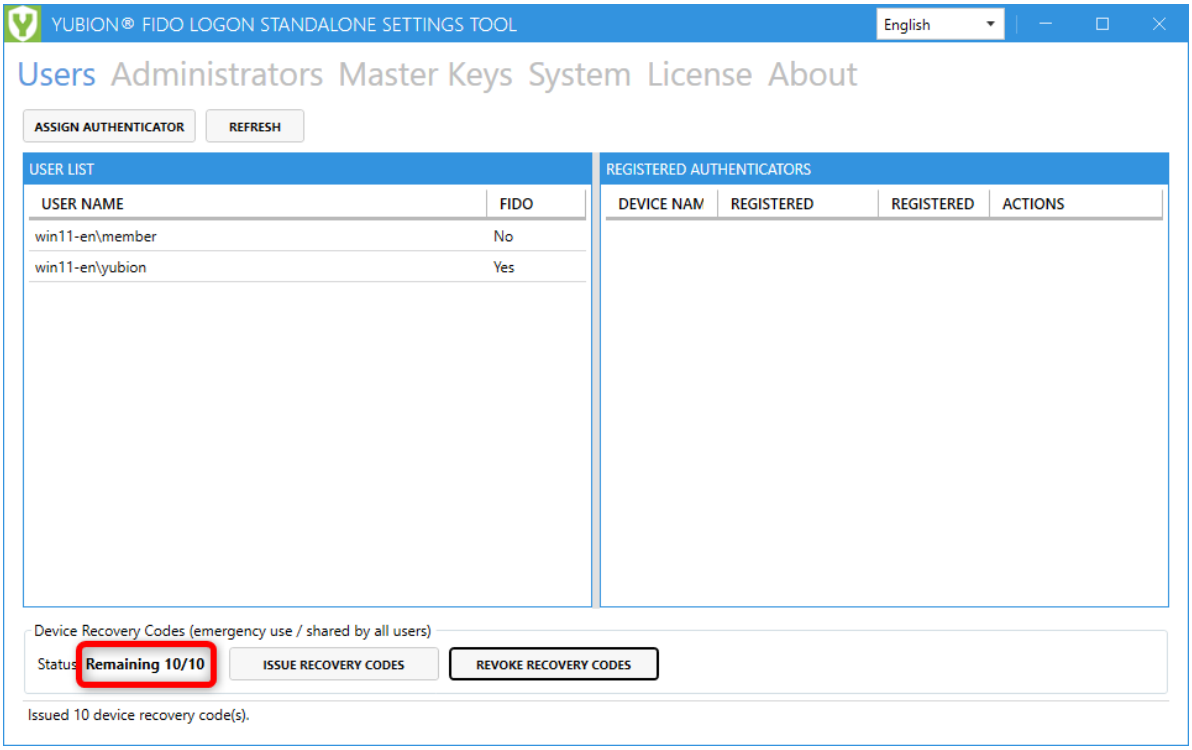

Figure: The recovery code status display

Chapter 11. Transferring Settings and Credentials (Export and Import)

Export and import let you move settings and credentials to another computer, or back them up. The operation is at the bottom of the **System** tab.

11.1 What Is Transferred and What Is Not

Transferred:

- All system settings
- User credentials
- Administrator credentials
- Master keys

Not transferred:

- The license file and the machine code
- Recovery codes
- The password cache
- Logs

> **Important (issue recovery codes on the destination computer)** Because recovery codes are not transferred, they remain **not issued** on the computer you import to. Recovery codes are the only way to sign in without using an authenticator at all, and they are your last line of defense against a lockout caused by an authenticator PIN lock. Be sure to issue recovery codes on the destination computer after importing (Chapter 10 "Issuing Recovery Codes").

11.2 Export

1. In the **Settings Transfer** group at the bottom of the **System** tab, select **Export...**.

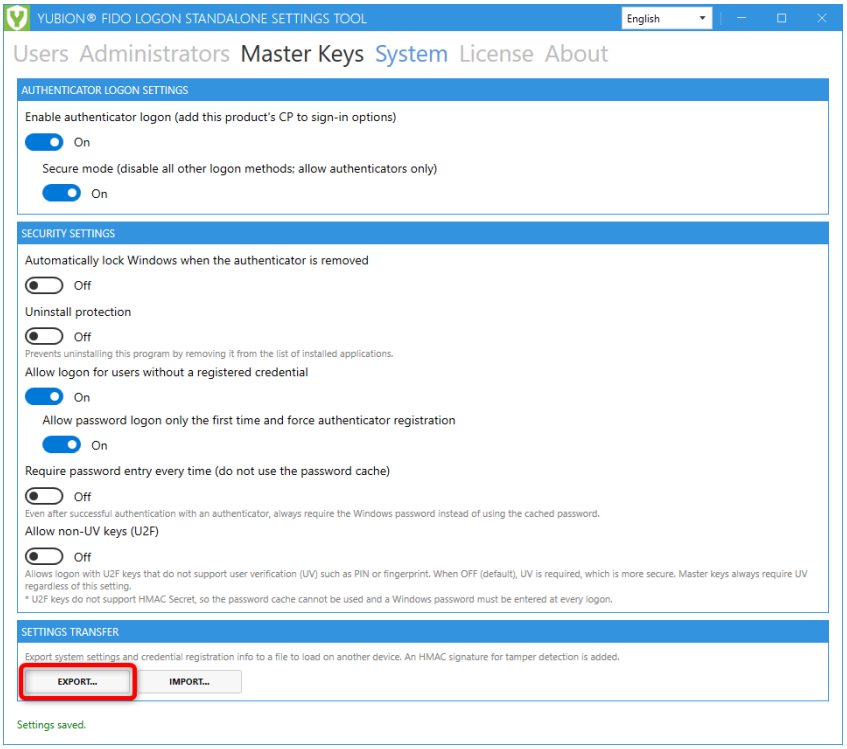

Figure: The Export button

2. Specify a destination and save the export file (extension `.fidocfg.json`).

> **Security** The export file contains credentials. Credentials are decrypted on the source computer and re-encrypted on the destination computer. The integrity of the file is protected, but handle it with care and transport it over a secure channel.

11.3 Import

1. In the settings tool on the destination computer, select **Import...** in the **Settings Transfer** group at the bottom of the **System** tab, and specify the export file.

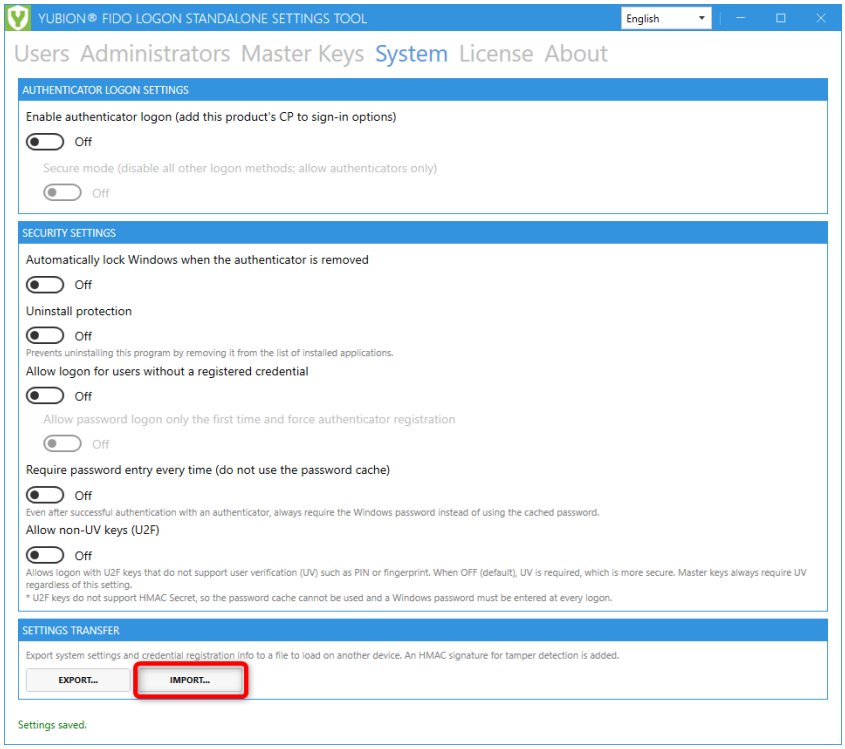

Figure: The Import button

2. On the **import confirmation screen**, review the list of accounts to be imported.
3. Confirm the contents and apply.

Figure: The import confirmation dialog

> **Lockout prevention** If the import would result in zero authenticators usable for signing in, "authenticator logon" and "secure mode" are turned off automatically.

Chapter 12. Operation and Maintenance

12.1 Collecting Support Information

For fault investigation, you can collect the computer's settings, logs, and related data in one package.

1. Open the **About** tab.

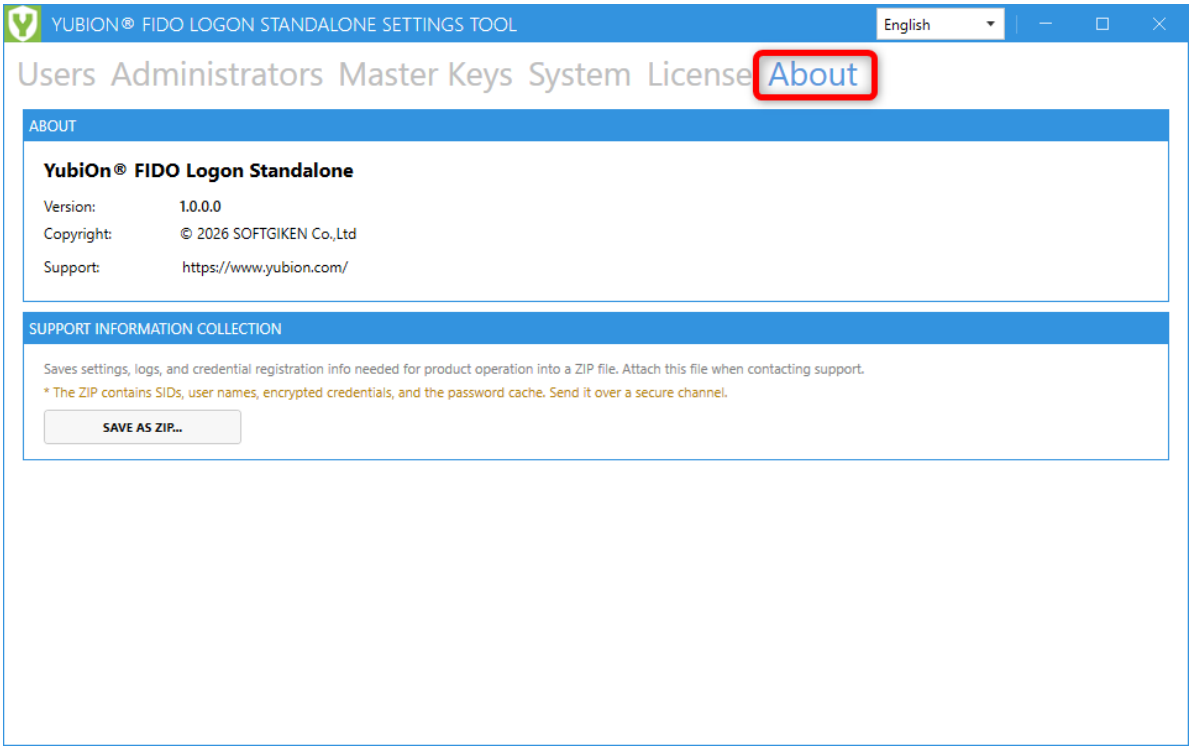

Figure: The About tab

2. Select **Save as ZIP...** in the **Support Information Collection** group.

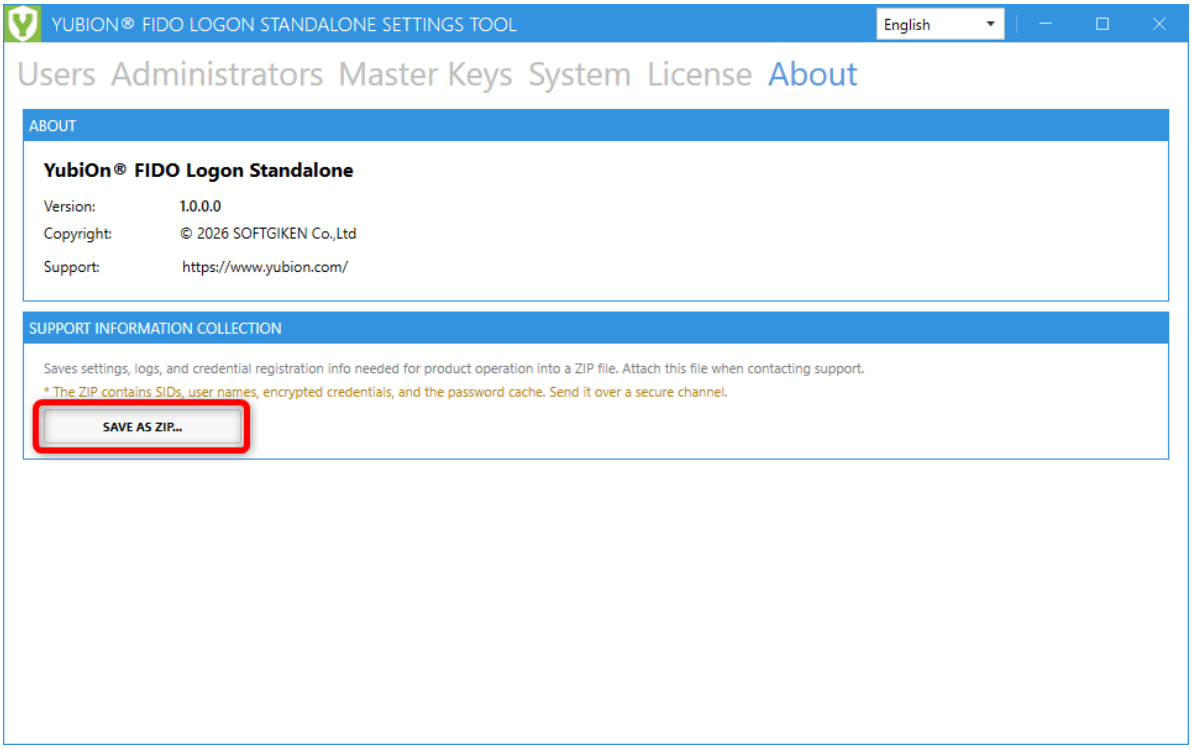

Figure: The Save as ZIP button

3. In the save dialog, specify the destination and the file name (the initial destination is the desktop).
4. Send the generated ZIP file to the support desk over a secure channel.

> **Security** The ZIP contains credential files in encrypted form. They cannot be decrypted on another computer, but metadata such as account names and public keys can be read. Send it over a secure channel.

12.2 Checking the Logs

This product's operation logs are written to the **Windows Event Viewer** (event source name `YubiOnFidoLogonStandalone`). There is no log viewer inside the settings tool.

- Sign-in successes and failures, authenticator registration, deletion, and renaming, license-related events, service start, and more are recorded.
- For a complete list of the events that are written (event ID, level, contents), see "Appendix C List of Event Log Entries".

12.2.1 Detailed Operation Logs (Files)

Separately from the event log, detailed logs for fault investigation are written to files. You do not need to look at them in normal operation (they are what the support desk may ask for, and what is collected in the previous section, "Collecting Support Information").

Item	Contents
Location	Under `%ProgramData%\YubiOn\FidoStandalone\logs` (the `Service`, `CredentialProvider`, `AdministrateTool`, and `CliTool` folders)
Rotation	**Daily** (for example, `Svc_Trace.log.20260427`)
Retention	**90 days.** Files older than that are **deleted automatically by the service**

> **Note** Automatic deletion runs once a day while the service is running. On a computer where the service has been stopped for a long time, old logs are deleted together after the next start. Log files currently being written are never deleted.

12.3 Behavior in Safe Mode

So that using secure mode together with safe mode does not cause a lockout, the service is registered to start during a safe boot as well.

> **Note** Whether WebAuthn can enumerate authenticators in safe mode (Minimal) depends on the environment. Verify this on real hardware before going into production.

Chapter 13. Troubleshooting

13.1 Cannot Sign In, or the FIDO Tile Does Not Appear

- Check that the license is "Valid" (Chapter 5). When the license is not valid, the FIDO tile is not shown and password sign-in becomes available.
- Check that an authenticator is registered for the target user.
- Check that **Enable authenticator logon** is on.

13.2 Cannot Sign In over RDP

- Check the OS versions of the client and the host, the Group Policy for WebAuthn request redirection, and where the authenticator is connected (the client side) (Chapter 2).
- Check that **Enable authenticator logon** is on for the target computer (whether secure mode is ON or OFF has no bearing on whether you can sign in over RDP).

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

- Check whether you have registered a license for another computer, or one for a different OS type (server / client).
- Check the machine code again and obtain a license for the correct computer.
- **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 (Chapter 5 "When the Machine Code Changes and When It Does Not"). Note that **reinstalling the OS does not change the machine code**, so it is not a cause of this problem.
- A computer whose machine code cannot be obtained (for example, one with an invalid default UUID) also shows "machine mismatch". Check on the License tab of the settings tool whether a machine code is displayed (Chapter 5).

13.4 An Authenticator Was Lost, or the PIN Was Forgotten

- Direct the user to sign in for an emergency with a **recovery code** (Chapter 10).
- The administrator can sign in on the user's behalf with a **master key** (Chapter 9).
- Delete the lost authenticator from the settings tool.

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

Check the following in order.

1. **Is the Windows "Passkey access" setting turned off?**
   If **Passkey access** under **Settings** → **Privacy & security** → **Passkeys** is **off**, authenticators cannot be registered. The settings tool uses the Windows WebAuthn feature to register them, so it is blocked by this setting. Turn it **on** and register again. Registering a master key,

registering an administrator credential, and launch authentication fail for the same reason. On Windows versions with no "Passkeys" item in Settings, this restriction does not apply.

2. **Is the target user shown in the list?** Only accounts that already have a user profile on that computer (that have signed in at least once) are shown (Chapter 8).
3. **Does the authenticator support FIDO2?** U2F (CTAP1) only keys cannot be registered by default (Chapter 2 "FIDO2 Authenticator Requirements").
4. **Is the PIN blocked?** If it is, see "The Authenticator Is Locked After Repeated Wrong PIN Entries" below.

13.6 The Authenticator Is Locked After Repeated Wrong PIN Entries

Determine the state from the message on the sign-in screen.

- **"PIN authentication is blocked. Remove the security key and insert it again."** (temporary block)
  Remove the authenticator and insert it again, and the PIN can be entered once more. If the correct PIN is known, simply retry.
- **"The PIN is blocked. Please reset the security key."** (permanent block)
  That authenticator **cannot be used until it is reset (initialized)**. Follow the manufacturer's instructions for the reset procedure. **Resetting erases all credentials in the authenticator, so delete that authenticator in the settings tool and register it again.**

The ways to get the user signed in are as follows.

1. If the user has a **spare authenticator** registered, they can sign in with it.
2. They can sign in for an emergency with a **recovery code** (Chapter 10) (the Windows password is required as well).
3. The administrator can sign in on their behalf with a **master key** (Chapter 9).

> **Warning** If none of the above is available (every registered authenticator and master key is PIN-locked and no recovery codes have been issued), a computer with secure mode on can no longer be signed in to. Because this product cannot detect a PIN lock, the automatic turning off of "authenticator logon" does not happen either. This state cannot be recovered by changing settings in this product, so be sure to prepare in advance as described below.

For preparations, see Chapter 8 "Preparing for Authenticator Lockout Caused by Wrong PIN Entry".

13.7 Notes for Offline Environments (AD Domain)

- Even when an AD-joined computer cannot reach a domain controller, users who have previously signed in to that computer can use FIDO logon.
- A user who has never signed in cannot be signed in by typing their name (the same restriction as the OS cached logon).

Appendix A Glossary

Term	Description
FIDO2	A passwordless authentication standard based on public key cryptography.
Authenticator (credential / FIDO2 authenticator)	A FIDO2 device such as a YubiKey. The private key stays inside the device; this product stores only the public key and the credential ID.
Credential Provider (CP)	A plug-in sign-in method built into the Windows sign-in screen.
Secure mode	A mode that disables the other CPs and restricts sign-in to this product's FIDO logon.
Authenticator logon	The setting that registers this product's CP with Windows and makes FIDO logon available.
hmac-secret	A FIDO2 authenticator extension. Used to encrypt the password cache, which therefore cannot be decrypted without the authenticator connected.
Master key	An administrator FIDO authenticator that can sign in to any Windows account (up to 3 per computer; UV always required).
Administrator credential (administrator authenticator)	An authenticator used for launch authentication of the settings tool ("Require FIDO authentication to launch the settings tool"). It is not tied to a Windows user, and it is a separate concept from a master key.
Recovery code	A single-use code for emergency sign-in when an authenticator cannot be used (10 codes; the Windows password is required as well).
DPAPI (LOCAL_MACHINE)	The Windows Data Protection API. Encrypts with a key unique to the computer; the data cannot be decrypted on another computer.
RP ID	The FIDO2 relying party identifier. Fixed to `standalone.yubion.local` in this product.
UV (user verification)	Verification of the person by PIN or biometrics.

Term	Description
Machine code	The normalized BIOS UUID used to tie a license to a computer.

Appendix B List of Settings

Throughout this manual, settings are referred to by the **setting name shown in the settings tool**. The following is the list of items that can be configured in the settings tool.

Setting (as shown in the settings tool)	Default	Summary
Enable authenticator logon	Off	Registers / unregisters this product's CP
Secure mode	Off	Disables the other CPs and forces FIDO logon
Automatically lock Windows when the authenticator is removed	Off	Locks automatically when the authenticator is unplugged
Uninstall protection	Off	Hides the product from the app list
Allow logon for users without a registered credential	Off	Allows password logon for unregistered users
Allow password logon only the first time and force authenticator registration	Off	Forces unregistered users to register at first sign-in
Require password entry every time	Off	Does not use the cache; requires entry every time
Allow non-UV keys (U2F)	Off	Allows U2F keys (no password cache)
Require FIDO authentication to launch the settings tool	Off	Requires FIDO authentication when the settings tool starts
Require password every time a master key authenticates	Off	Requires a password at every master key authentication

Internal Specifications Not Shown in the Settings Tool

The following are fixed behaviors and are not shown in the settings tool (they cannot be changed).

Item	Value
RP ID (relying party identifier)	`standalone.yubion.local` (fixed)
Cache validity period	Unlimited

Appendix C List of Event Log Entries

This product writes audit information such as sign-ins and administrative operations to the **Windows event log**. Use it for auditing and fault investigation.

Destination and Source Information

Item	Value
Destination log	Application log
Event source name	`YubiOnFidoLogonStandalone`
Category	Not used (default)

> **How to check** Open **Event Viewer** → **Windows Logs** → **Application** in Windows and look at the events whose source is `YubiOnFidoLogonStandalone`.

Event ID Numbering Scheme

Range	Purpose	Main source
1100–1199	Result of FIDO authentication	Credential Provider
1200–1211	Result of sign-in (FIDO / password)	Credential Provider
1300–1301	Authenticator registration through self-registration (via the CP)	Credential Provider
1400–1401	Sign-in with a recovery code	Service
1500–1521	Authentication and sign-in with a master key	Credential Provider
1600–1601	Entry-point errors for sign-in with a typed account ID	Credential Provider
2100–2103	Session (sign-in / sign-out / lock)	Service
2200	Automatic lock on authenticator removal	Service
2900–2912	Service state and license file monitoring	Service
3100–3201	Exporting and importing settings	Settings tool

Range	Purpose	Main source
3300–3302	Managing recovery codes	Settings tool
3400–3401	Collecting support information	Settings tool
3500–3502	Managing master keys	Settings tool
3600–3602	Managing user authenticators (credentials)	Settings tool
3700–3701	Importing a license	Settings tool

> **Main fields in the message body** `User` (user name), `SID`, `Session ID`, `Client` (where the connection came from: local or the RDP client name), `Authenticator` (authenticator name), `Device ID`, `NTSTATUS` (sign-in result code), and so on. Entra ID accounts are recorded in the `AzureAD\{UPN}` form.

Sign-In and Authentication (Credential Provider)

Result of FIDO Authentication (1100–1199)

ID	Level	Contents	When it occurs
1100	Information	FIDO authentication succeeded	The assertion from the authenticator was verified successfully
1110	Warning	FIDO authentication failed: wrong PIN / PIN blocked	A wrong PIN was entered, or the PIN was blocked
1111	Information	FIDO authentication failed: canceled	The user canceled the authentication
1112	Warning	FIDO authentication failed: timed out	The authentication timed out
1113	Warning	FIDO authentication failed: unregistered authenticator	An unregistered authenticator was used, or verification was rejected
1114	Error	FIDO authentication failed: service not running / cannot communicate	The challenge request to, or the verification exchange with, the service failed

ID	Level	Contents	When it occurs
1199	Error	FIDO authentication failed: other	Any other exception (CTAP error, device removal, no PIN set, and so on)

Result of Sign-In (1200–1211)

ID	Level	Contents	When it occurs
1200	Information	Sign-in succeeded (via FIDO)	Windows sign-in from the FIDO tile succeeded
1201	Warning	Sign-in failed (via FIDO)	Windows sign-in failed after successful FIDO authentication (wrong password, and so on)
1210	Information	Password sign-in succeeded	Sign-in from the password-only tile succeeded
1211	Warning	Password sign-in failed	Sign-in from the password-only tile failed

Authenticator Registration Through Self-Registration (1300–1301)

ID	Level	Contents	When it occurs
1300	Information	Authenticator registration through self-registration succeeded	The authenticator was registered successfully in the CP self-registration flow
1301	Warning	Authenticator registration through self-registration failed	Registration failed in the same flow (cancellation, PIN-related problem, communication failure, and so on)

Sign-In with a Recovery Code (1400–1401)

ID	Level	Contents	When it occurs
1400	Warning	Recovery code sign-in succeeded	Sign-in completed after a recovery code was verified (the remaining count is also recorded)
1401	Warning	Recovery code sign-in failed	The code did not match, was already used, or none had been issued

> Because recovery codes are used only in emergencies such as a lost or failed authenticator, even success is recorded at the "Warning" level so that it stands out in an audit.

Authentication and Sign-In with a Master Key (1500–1521)

ID	Level	Contents	When it occurs
1500	Warning	Master key authentication succeeded	Authentication with a master key succeeded (the target account and key name are recorded)
1520	Warning	Sign-in via a master key succeeded	Windows sign-in after master key authentication succeeded
1521	Warning	Sign-in via a master key failed	Windows sign-in failed after successful master key authentication

> **Note** Because a master key is a powerful privilege that can sign in to any account, even success is recorded at the "Warning" level.
> **Failures** of master key authentication (wrong PIN, cancellation, timeout, and so on) are recorded as ordinary FIDO authentication failures (**1110–1199**), not as dedicated events.

Entry-Point Errors for Sign-In with a Typed Account ID (1600–1601)

ID	Level	Contents	When it occurs
1600	Warning	The typed account was not found	The ID typed under "Other user" could not be resolved
1601	Information	The typed account has no registered authenticator	The account was resolved but has no authenticator registered (the subsequent behavior is also recorded)

Service

Session Notifications (2100–2103)

ID	Level	Contents	When it occurs
2100	Information	Sign-in (session start)	A session sign-in was detected
2101	Information	Sign-out	A session sign-out was detected
2102	Information	Computer locked	A screen lock was detected
2103	Information	Computer unlocked	An unlock was detected

Automatic Lock (2200)

ID	Level	Contents	When it occurs
2200	Warning	Automatic lock on authenticator removal	An automatic lock was performed because the authenticator was removed

Service State and License Monitoring (2900–2912)

ID	Level	Contents	When it occurs
2900	Information	Service started	When the service starts (the secure mode state and license information are recorded)
2901	Information	Service stopped	When the service stops
2910	Information	License file updated	An update of a valid license file was detected
2911	Warning	Invalid license detected and automatically restored	An invalid license file was detected and restored from the backup
2912	Warning	Invalid license detected (restore not possible)	An invalid file was detected but could not be restored from a backup

Administrative Operations in the Settings Tool

> These events record the operator (`Operator` / "... by").

Exporting and Importing Settings (3100–3201)

ID	Level	Contents	When it occurs
3100	Information	Settings export succeeded	When the export of settings and credentials completes
3101	Warning	Settings export failed	When an export fails
3200	Information	Settings import succeeded	When the import of settings and credentials completes
3201	Warning	Settings import failed	When an import fails

Managing Recovery Codes (3300–3302)

ID	Level	Contents	When it occurs
3300	Information	Recovery codes issued	When recovery codes are issued for the first time
3301	Warning	Recovery codes reissued	When existing codes are discarded and new ones issued
3302	Warning	Recovery codes revoked	When recovery codes are revoked

Collecting Support Information (3400–3401)

ID	Level	Contents	When it occurs
3400	Information	Support information collected	When the support information (ZIP) has been generated
3401	Warning	Support information collection failed	When collection fails

Managing Master Keys (3500–3502)

ID	Level	Contents	When it occurs
3500	Information	Master key registered	When a master key is registered
3501	Warning	Master key deleted	When a master key is deleted
3502	Information	Master key renamed	When a master key is renamed

Managing User Authenticators (Credentials) (3600–3602)

ID	Level	Contents	When it occurs
3600	Information	Authenticator registered	When a user's authenticator is registered from the settings tool
3601	Warning	Authenticator deleted	When a user's authenticator is deleted
3602	Information	Authenticator renamed	When an authenticator is renamed

Importing a License (3700–3701)

ID	Level	Contents	When it occurs
3700	Information	License import succeeded	When a license import completes (the license information is recorded)
3701	Warning	License import failed	When validation at import rejects the file

Contact

For inquiries about installing, configuring, or operating this product, contact the **reseller** you purchased it from, or the **YubiOn Support Desk** below.

Support Desk

Item	Contents
Name	YubiOn Support Desk (SOFTGIKEN Co., Ltd.)
Hours	Weekdays 9:00–17:00 (excluding weekends, public holidays, and our company holidays)
Email	support@yubion.com
Product information	https://www.yubion.com/

Attaching the ZIP file obtained in Chapter 12 "Collecting Support Information" helps us investigate more quickly.

Manufacturer

Item	Contents
Manufacturer	SOFTGIKEN Co., Ltd.
Website	https://sgk.co.jp/