

YubiEnroll with Microsoft Entra ID

Quick Start Guide

Document Updated: Jul 7, 2025

Contents

	2
Introduction	3
Step 1. Install and Launch YubiEnroll	3
Step 2. Configure YubiEnroll in Microsoft Entra ID	4
2a. Enable MFA for YubiKeys	4
2b. Register the YubiEnroll app	4
2c. Configure Permissions	5
Step 3. Add Provider and Profile in YubiEnroll	6
Step 4. Enroll Your First End User	7

Introduction

YubiEnroll enables organizations of all sizes to easily enroll YubiKeys on behalf of end users supporting the move to a passwordless and phishing-resistant enterprise. This quick start guide outlines the high level requirements and steps to quickly get started enrolling end users with YubiEnroll for Microsoft Entra ID. For a full description of YubiEnroll features, see the [YubiEnroll User Guide](#).

Follow these steps to get up and running with YubiEnroll:

1. [Install and launch](#) the YubiEnroll app.
2. [Configure YubiEnroll](#) in Microsoft Entra ID.
3. [Add the provider configuration](#) with an enrollment profile in YubiEnroll.
4. [Enroll your first end user](#) in YubiEnroll.

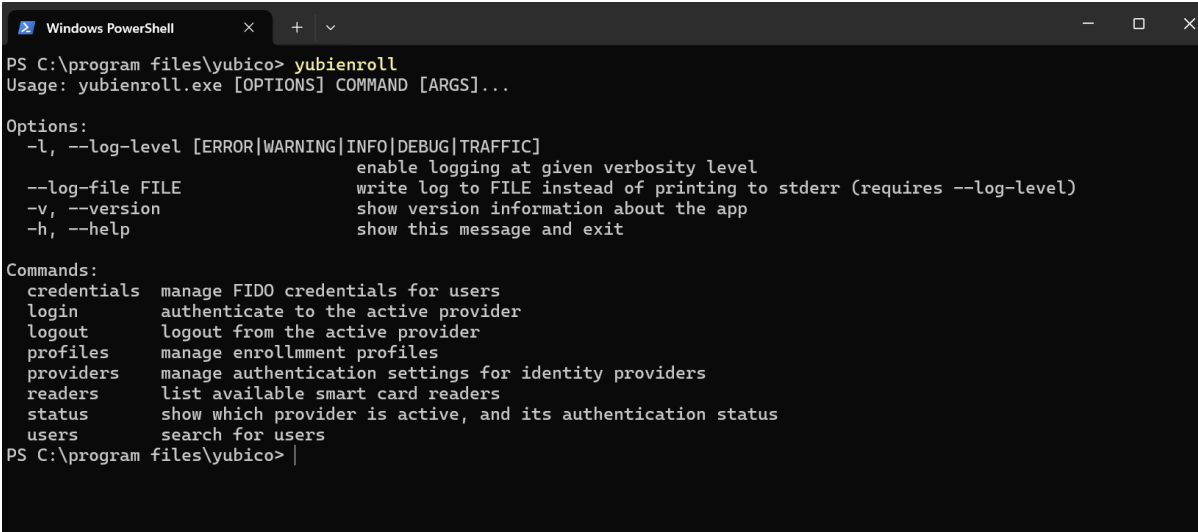
Step 1. Install and Launch YubiEnroll

Ensure you have the following in place before starting the implementation:

- Windows 11 with administrator privileges.
- Microsoft Entra ID.
- Permissions to manage users and credentials in the target tenant.

To install YubiEnroll for Windows, do the following:

1. Download the YubiEnroll installer from [Yubico Downloads](#).
2. Open a File Explorer, browse to the Downloads folder and double-click the installer.
3. Follow the instructions to complete the YubiEnroll setup steps.
4. Open a terminal, locate YubiEnroll (default path is “C:\Program Files\Yubico\YubiEnroll\”), and run `yubienroll` to launch the app.



```
Windows PowerShell
PS C:\program files\yubico> yubienroll
Usage: yubienroll.exe [OPTIONS] COMMAND [ARGS]...

Options:
  -l, --log-level [ERROR|WARNING|INFO|DEBUG|TRAFFIC]
                                enable logging at given verbosity level
  --log-file FILE                write log to FILE instead of printing to stderr (requires --log-level)
  -v, --version                  show version information about the app
  -h, --help                     show this message and exit

Commands:
  credentials  manage FIDO credentials for users
  login        authenticate to the active provider
  logout       logout from the active provider
  profiles     manage enrollment profiles
  providers    manage authentication settings for identity providers
  readers      list available smart card readers
  status       show which provider is active, and its authentication status
  users        search for users
PS C:\program files\yubico> |
```

Step 2. Configure YubiEnroll in Microsoft Entra ID

In this step you will enable MFA for YubiKeys, register the YubiEnroll application in the Microsoft Entra ID tenant, and configure the required user permissions.

2a. Enable MFA for YubiKeys

Ensure that Microsoft Entra ID Multi-Factor authentication (MFA) for Passkey (FIDO2) is enabled and that the target user accounts for YubiEnroll enrollment are in the scope.

To enable MFA for target user accounts, log in to the [Microsoft Entra admin center](#) and go to **Identity > Protection > Authentication methods > Policies > Passkey (FIDO2)**.

Enable the feature and either select all users, or select groups to be in the scope for YubiEnroll enrollment. For more information on configuring FIDO authentication with YubiKeys in Microsoft Entra ID see [Enable passkeys \(FIDO2\) for your organization \(Microsoft documentation\)](#).

2b. Register the YubiEnroll app

When configuring the Microsoft Entra ID provider in YubiEnroll, the following parameter values are needed:

- `client_id`
- `tenant_id`
- `redirect_uri`

These parameter values are created when registering the YubiEnroll (OAuth) application in Microsoft Entra ID. To register the YubiEnroll app, open the [Microsoft Entra admin center](#), go to **Application > App registrations** and select **New registration**.

- Ensure to select **Public client/native (mobile & desktop)** as the platform type.
- The **Redirect URI** must start with “http://localhost”, for example “http://localhost/yubienroll-redirect”. You do not need to specify the port as Microsoft Entra ID supports ephemeral ports.

Microsoft Entra admin center Search resources, services, and docs (G+/)

Home > App registrations > Register an application ...

Name
The user-facing display name for this application (this can be changed later).
YubiEnroll-App ✓

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (yubicosi only - Single tenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Public client/native (mobile ...) http://localhost/yubienroll-redirect ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

For more details on how to register the YubiEnroll app, see [Register an application with the Microsoft identity platform \(Microsoft documentation\)](#).

To find the values for **Application (client) ID**, **Directory (tenant) ID**, and **Redirect URI** needed when adding the provider in YubiEnroll, open the YubiEnroll app in Microsoft Entra ID. The values are displayed in the **Overview** section under **Essentials**. Copy and save the values for later use.

2c. Configure Permissions

The YubiEnroll app requires the following two permissions in Microsoft Entra ID to be added as Microsoft Graph Delegated permissions:

- *User.ReadBasic.All*
- *UserAuthenticationMethod.ReadWrite.All*

To add these, open the YubiEnroll app in Microsoft Entra ID, select **API permissions** in the left menu, and click **Add a permission**.

Home > App registrations > YubiEnroll-Test-Anfi > App registrations > YubiEnroll-App

YubiEnroll-App | API permissions

Search < Refresh Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting
New support request

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for yubicosi

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
User.ReadBasic.All	Delegated	Read all users' basic profiles	No
UserAuthenticationMethod.ReadWrite.All	Delegated	Read and write all users' authentication methods.	Yes

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

For a user to be able to grant consent to these permissions when setting up the application in Microsoft Entra ID, the user must be assigned the *Global Administrator* role.

The following applies when configuring permissions:

- *Authentication Administrator* role is required for managing passkeys of non-administrators.
- *Privileged Authentication Administrator* role is required for managing passkeys for any type of user including *Global Administrators*.

Note: Even with the *Privileged Authentication Administrator* role, the administrator will not be able to use YubiEnroll to manage passkeys for their own profile.

Step 3. Add Provider and Profile in YubiEnroll

In this step you will add the Microsoft Entra ID identity provider configuration in YubiEnroll together with an enrollment profile. Enrollment profiles lets users define a combination of preferred credential settings when configuring YubiKeys during enrollment.

Note: The configuration options "Min PIN length", "Override always UV", and "Force PIN change before use" are only supported for YubiKeys with firmware version 5.5 and higher.

To add the Microsoft Entra ID provider configuration with an enrollment profile, do the following:

1. In the terminal, run `yubienroll providers add entra` where "entra" is the provider name in this example (you can choose a name of your choice).
2. Select the desired provider type, "ENTRA" (2).
3. When prompted, enter the values for **Client ID**, **Redirect URI**, and **Microsoft Entra Tenant ID** that you obtained when [registering the YubiEnroll app](#) in Microsoft Entra ID.
4. For **Microsoft Entra ID endpoint** and **Microsoft Graph endpoint**, you can use default values in most cases. If your organization is working with government tenants, you might need to change the endpoints.
5. When prompted to specify if you want to add a new enrollment profile [y/N], enter "y".

6. Enter the following when prompted:
 - a. **Profile name [default]:** The name to be used for the profile. If you do not enter a name, "default" will be used.
 - b. **Min PIN length [4]:** Enter the desired PIN length, for example 6. If you do not enter a PIN length, the value "4" will be used. Note that the minimum PIN length can never be shorter than "4".
 - c. **Require always UV? [y/N]:** Define if the "Always require user verification" setting should always be overridden. Default is "no".
 - d. **Require Enterprise Attestation? [y/N]:** Define if enterprise attestation should be required. Default is "no".
 - e. **Force PIN change before use? [y/N]:** Define if the end user must change the PIN when using the YubiKey for the first time. Default is "no".
 - f. **Factory reset the Security Key? [Y/n]:** Enter "n" if you will be enrolling a new key. Enter "y" if you will be enrolling a key that has previously been in use. This option will clear the key completely from previous configurations.
 - g. **Set a new random PIN [Y/n]:** Enter "y" if you want YubiEnroll to set a new PIN for the key. Enter "n" if you want to specify a specific PIN.
 - h. **Random PIN length [4]:** Define the length of the random PIN to be set, if this option was selected.
7. The provider configuration is added together with the enrollment profile. Because no provider existed previously, the "entra" provider is automatically activated.

Step 4. Enroll Your First End User

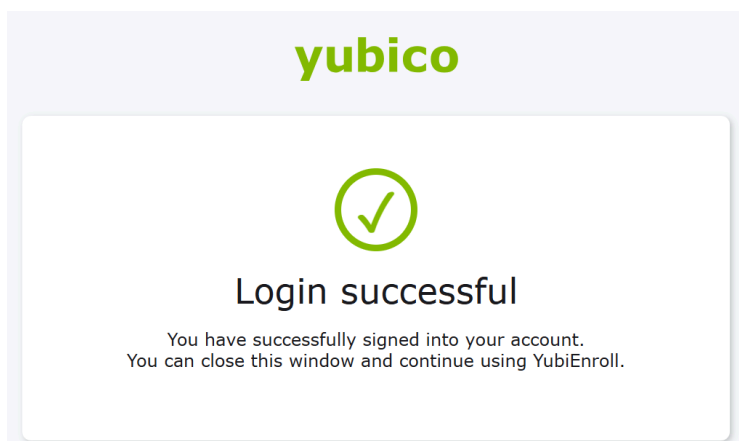
In this step you will enroll a YubiKey and add credentials on behalf of a specific end user. Ensure you have the YubiKey you want to enroll available, as well as the "ID" or "Username" of the end user.

If you do not know the user identifier, you can search for this using the `yubienroll users <query>` command where `query` can be for example the firstname and/or lastname of the end user. The user identifier "ID" and "Username" will be returned.

Note: To enroll YubiKeys on behalf of end users, you need to be an administrator with specific permissions. For more information, see [Configure permissions](#).

To enroll a YubiKey on behalf of an end user, do the following:

1. In the terminal, run the `yubienroll login` to authenticate with the identity provider.
2. Select the desired provider, "ENTRA" (1).
3. When prompted, enter the values for **Client ID**, **Redirect URI**, and **Microsoft Entra Tenant ID** that you obtained when [registering the YubiEnroll app](#) in Microsoft Entra ID.
4. Follow the steps to complete the authentication. When successfully authenticated, return to the terminal.



5. Insert or present the YubiKey you want to enroll.
6. Run the command `yubienroll credentials add firstname.lastname@email.com` where in this example the "firstname.lastname@email.com" is the end user identifier.
7. YubiEnroll fetches the provider-specific options for creating credentials, and the settings for the enrollment profile to be used are displayed. In this example, the key is also reset before the credentials are added (Factory reset: True).
8. When prompted, touch the YubiKey you are enrolling.
9. When prompted, enter "y" to proceed with the configuration.
10. When the credentials have been successfully added, the serial number and temporary PIN to be used are displayed.
11. Provide the YubiKey and the temporary PIN to the end user.
12. To authenticate with identity provider, the end user presents the provided YubiKey and the temporary PIN. If the "Force PIN change" was set to "On", the end user is prompted to change the PIN upon first log in.

Done! You have now enrolled an end user, providing them with a ready-to-use pre-registered YubiKey for a phishing-resistant user experience.