

YubiEnroll with Okta

Quick Start Guide

Document Updated: **Jul 7, 2025**

Contents

	2
Introduction	3
Step 1. Install and Launch YubiEnroll	3
Step 2. Configure YubiEnroll in Okta	4
2a. Register the YubiEnroll App	4
2b. 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 Okta. 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 Okta.
3. [Add the provider configuration](#) with an enrollment profile in YubiEnroll.
4. [Enroll your first end user](#) in YubiEnroll.

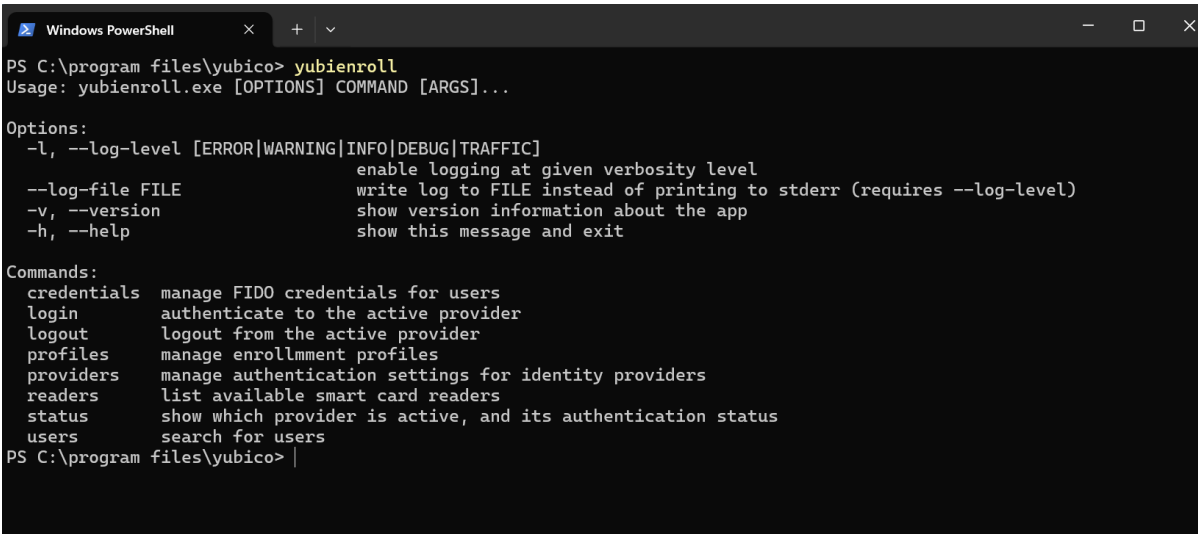
Step 1. Install and Launch YubiEnroll

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

- Windows 11 with administrator privileges.
- Okta Identity Engine (OIE).
- 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 Okta

In this step you will register the YubiEnroll application in the Okta tenant and configure the required user permissions.

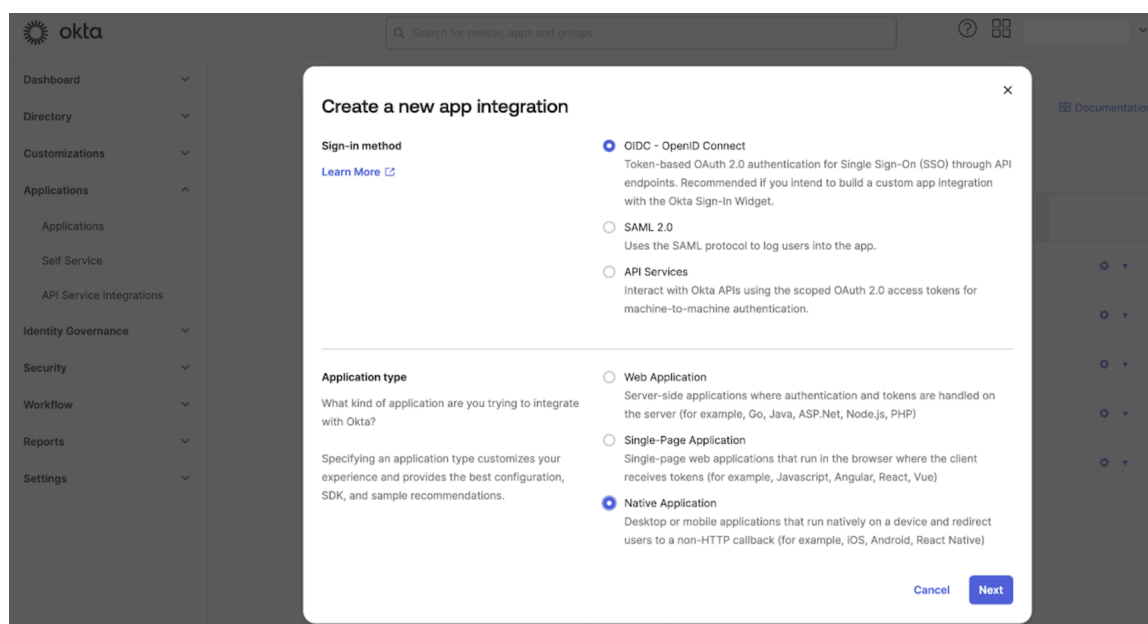
2a. Register the YubiEnroll App

When configuring the Okta provider in YubiEnroll, the following parameter values are needed:

- `client_id`
- `domain (tenant_id)`
- `redirect_uri`

These parameter values are created when registering the YubiEnroll (OAuth) application in Okta. To register the YubiEnroll app, open the **Admin Console**, go to **Applications > Applications**, and click **Create App Integration**.

- When registering YubiEnroll, ensure to select “OIDC - OpenID Connect” as the **Sign-in method** and “Native Application” as the **Application type** in the **Create a new app integration** dialog.



- When adding the redirect URI in the **New Native App Integration** dialog, the **Sign-in redirect URIs** must start with “http://localhost”. You also need to specify a port, for example “http://localhost:8080/yubienroll-redirect”.
- Ensure to select the “Refresh Token” option under **Grant type > Core Grants** so that the YubiEnroll app will issue a refresh token once it expires.

The screenshot shows the 'New Native App Integration' page in the Okta admin console. The left sidebar contains navigation links: Dashboard, Directory, Customizations, Applications, Identity Governance, Security, Workflow, Reports, and Settings. The main content area is titled 'New Native App Integration' and contains a form for 'YubiEnroll-App'.

General Settings

App integration name: YubiEnroll-App

Logo (Optional): A placeholder box with a gear icon and upload/delete buttons.

Proof of possession: ☐ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type: **Core grants**

- ☒ Authorization Code
- ☒ Refresh Token
- ☐ Device Authorization

[Advanced](#) ▾

Sign-in redirect URIs: ☐ Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

[x](#)

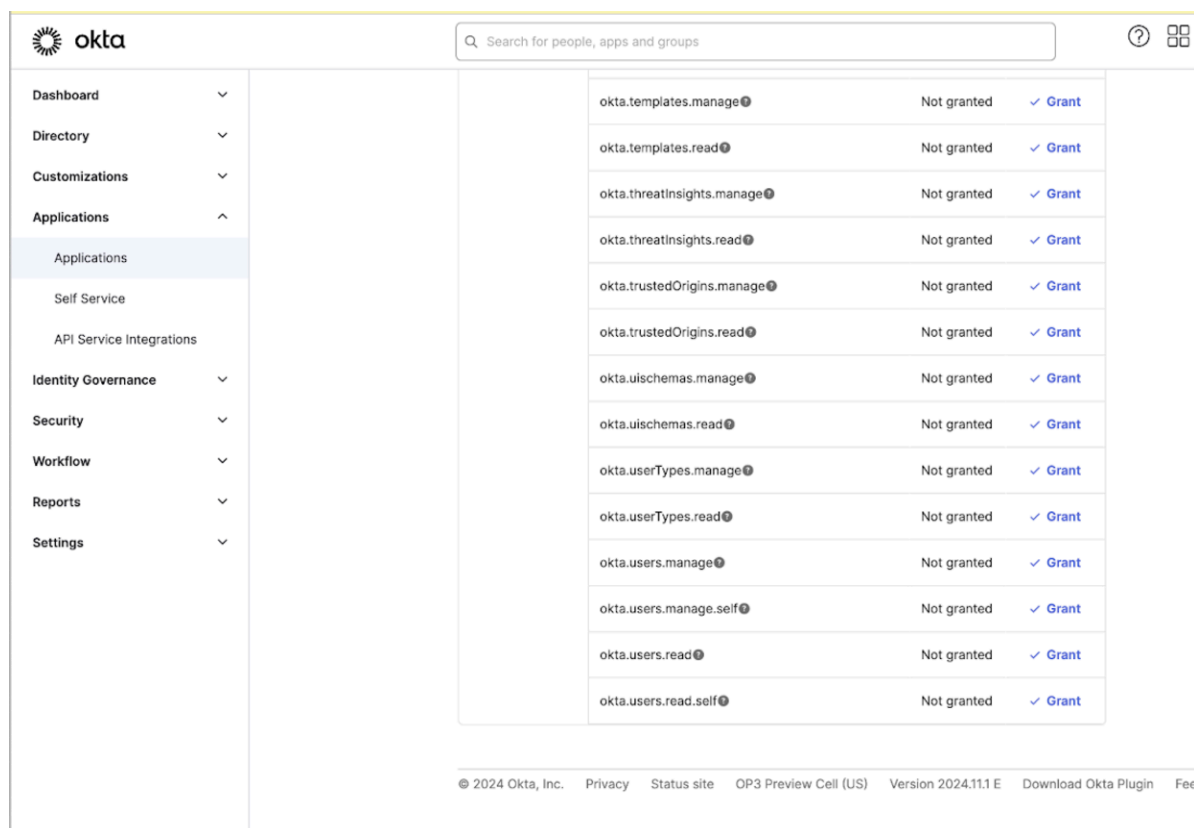
[Learn More](#) [+ Add URI](#)

For more details on how to register the YubiEnroll app, see [Create an OAuth 2.0 app in Okta \(Okta documentation\)](#).

To find the values for **Client ID** and **Redirect URI** needed when adding the provider in YubiEnroll, go to the **General** tab in the **Applications** view in Okta. The **Okta Domain (tenant ID)** can be found in the Okta admin dashboard when clicking on the admin profile in the upper right corner. The domain is displayed under the email address. Copy and save the values for later use.

2b. Configure Permissions

The permissions required by YubiEnroll in Okta are *okta.users.manage* and *okta.users.read*. To configure these, open the YubiEnroll app in Okta, select “Okta API scopes”, locate the scopes and click **Grant** for each of them.



To be able to perform enroll on behalf of an end user, the user (IT admin) must have either the *Super Administrator*, *Group Administrator*, or *Organization Administrator* role in Okta.

Step 3. Add Provider and Profile in YubiEnroll

In this step you will add the Okta 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 Okta provider configuration with an enrollment profile, do the following:

1. In the terminal, run `yubienroll providers add okta` where “okta” is the provider name in this example (you can choose a name of your choice).
2. Select the desired provider type, “OKTA” (2).
3. When prompted, enter the values for **Client ID**, **Redirect URI**, and **Okta Tenant ID** that you obtained when [registering the YubiEnroll app](#) in Okta.
4. When prompted to specify if you want to add a new enrollment profile [y/N], enter “y”.
5. 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.
6. The provider configuration is added together with the enrollment profile. Because no provider existed previously, the “okta” provider is automatically activated.

Step 4. Enroll Your First End User

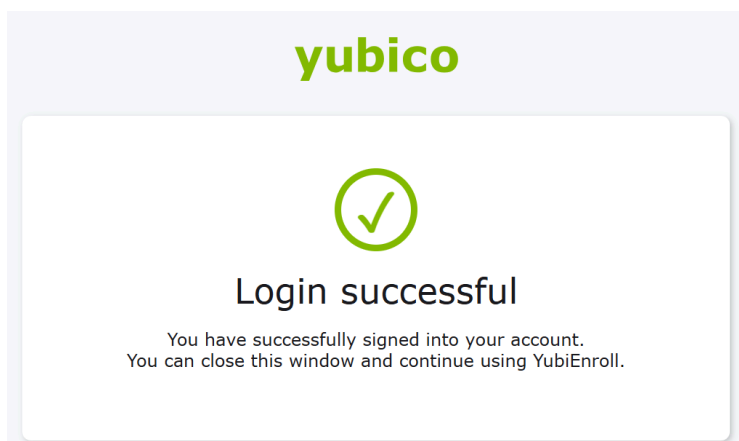
In this step you will enroll a YubiKey and add credentials on behalf of a specific end user. Ensure you have the YubiKey you want to enroll available, as well as the “ID” or “Username” of the end user.

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, “OKTA” (2).
3. When prompted, enter the values for **Client ID**, **Redirect URI**, and **Okta Tenant ID** that you obtained when [registering the YubiEnroll app](#) in Okta.
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.