YubiEnroll User Guide

Yubico

May 22, 2026

CONTENTS

1 Introduction **1**
- 1.1 Supported Platforms . . . 1
- 1.2 Supported Identity Providers . . . 1
- 1.3 Hardware . . . 2

2 About YubiEnroll **3**
- 2.1 YubiEnroll CLI . . . 4
- 2.2 Enrollment Profiles . . . 4
- 2.3 Identity Provider Configuration . . . 5
- 2.4 Authentication and Authorization . . . 6

3 Installing YubiEnroll CLI **7**
- 3.1 Prerequisites . . . 7
- 3.2 Downloading . . . 7
- 3.3 Installing on Windows . . . 7

4 Using YubiEnroll CLI **9**
- 4.1 Launching on Windows . . . 9
- 4.2 Adding Provider Configurations . . . 9
- 4.3 Creating Enrollment Profiles . . . 15
- 4.4 Enrolling End Users . . . 17

5 YubiEnroll Identity Providers **23**
- 5.1 Configuring YubiEnroll with Microsoft Entra ID . . . 23
- 5.2 Configuring YubiEnroll with Okta . . . 27
- 5.3 Configuring YubiEnroll with PingOne PingID . . . 30
- 5.4 Configuring YubiEnroll with PingOne AIC . . . 35

6 YubiEnroll Commands **41**
- 6.1 yubienroll . . . 41
- 6.2 yubienroll credentials . . . 42
- 6.3 yubienroll login . . . 44
- 6.4 yubienroll logout . . . 44
- 6.5 yubienroll profiles . . . 45
- 6.6 yubienroll providers . . . 47
- 6.7 yubienroll readers . . . 49
- 6.8 yubienroll status . . . 49
- 6.9 yubienroll users . . . 50

7 Release Notes **51**
- 7.1 2026 . . . 51

7.2 2025 51
7.3 2024 52

8 Copyright **53**
8.1 Trademarks 53
8.2 Disclaimer 53
8.3 Contact Information 53
8.4 Getting Help 54
8.5 Feedback 54
8.6 Document Updated 54

CHAPTER

ONE

INTRODUCTION

YubiEnroll enables administrators in organizations of all sizes to easily enroll YubiKeys on behalf of end users supporting the move to a passwordless and phishing-resistant enterprise.

YubiEnroll is a software application that provides organizations with the ability to create FIDO credentials on YubiKeys, and configure and register the YubiKey with their identity provider on behalf of a user account. Pre-used YubiKeys can also be reset through YubiEnroll. For more information, see *About YubiEnroll*.

YubiEnroll offers a command line interface (CLI) through which an IT administrator can perform desired YubiKey configurations, for example to set minimum PIN length or force PIN change. When the YubiKey is configured, the IT admin can then enroll the YubiKey for a future key holder through the organizations' identity provider (currently Okta, Microsoft Entra ID, and PingOne PingID and PingOne AIC). For more information, see *Using YubiEnroll CLI*.

1.1 Supported Platforms

Yubienroll is compatible with and tested on Windows 11. If end users log in with admin-enrolled YubiKeys to systems on different platforms, they might encounter FIDO2 capabilities that are not yet supported.

The following describes which FIDO CTAP2.1 features are natively supported by a platform.

YubiEnroll Feature	Platforms supporting the feature on a YubiKey
Minimum PIN length	Windows 11, Chrome on MacOS, Linux.
Force PIN change before use	Windows 11, Chrome on MacOS, Linux.
Require always UV	Windows 10*, Windows 11, macOS, Android, iOS, Linux.

* On Windows 10, security keys enabled with `Require always UV` works with Okta, Microsoft Entra ID, PingOne PingID, and PingOne AIC. However, other websites supporting WebAuthn that do not request user verification, might block the user from logging in.

1.2 Supported Identity Providers

YubEnroll must be registered with the identity provider. Then the identity provider is added to YubiEnroll. YubiEnroll works with the following identity providers:

Identity Provider	References
Microsoft Entra ID *	Register YubiEnroll with MS Entra ID, see *Configuring YubiEnroll with Microsoft Entra ID* Add Microsoft Entra ID to YubiEnroll, see *Adding Microsoft Entra ID*
Okta	Register YubiEnroll with Okta, see *Configuring YubiEnroll with Okta* Add Okta to YubiEnroll, see *Adding Okta*
PingOne PingID	Register YubiEnroll with PingOne PingID, see *Configuring YubiEnroll with PingOne PingID* Add PingOne PingID with YubiEnroll, see *Adding PingOne PingID*
PingOne Advanced Identity Cloud (AIC)	Register YubiEnroll with PingOne AIC, see *Configuring YubiEnroll with PingOne AIC* Add PingOne AIC with YubiEnroll, see *Adding PingOne AIC*

* YubiEnroll with Microsoft Entra ID is currently in *Early Access*. For more information, see YubiEnroll.

1.3 Hardware

Configuration of YubiKeys through the YubiEnroll CLI supports the entire current Yubico hardware product portfolio including all types of YubiKeys. Supported interfaces where applicable are USB-A, USB-C, and NFC.

Note: The configuration options `Min PIN length`, `Require always UV`, and `Force PIN change before use` require YubiKeys with firmware version 5.5 and higher.

CHAPTER

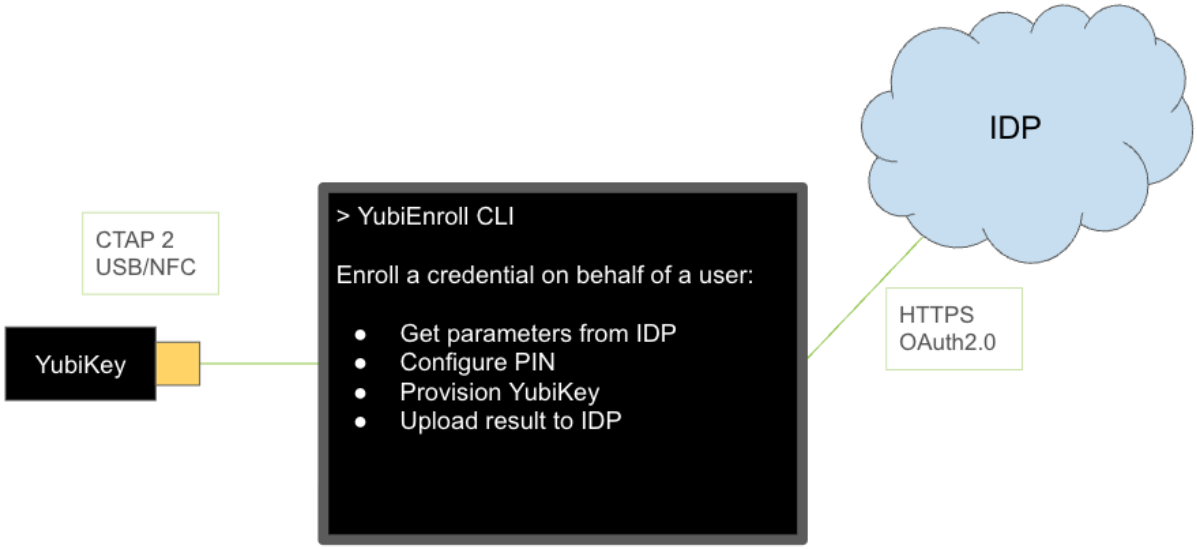
TWO

ABOUT YUBIENROLL

YubiEnroll lets organization IT admins configure and register YubiKeys on behalf of users in the organization and is a complementary solution to Yubico FIDO Pre-reg and part of the Yubico Enrollment Suite.

With Yubico FIDO Pre-reg organizations use the YubiEnterprise API and the organizations' identity provider to request pre-registered, factory-new YubiKeys. Yubico pre-registers the keys which are then shipped to end users or offices through YubiEnterprise Delivery services.

YubiEnroll works as an independent application in an organizations' environment and only communicates with the identity provider. A user, for example the organizations' IT admin, configures and enrolls the YubiKey on behalf of an end user in the organization with YubiEnroll, and delivers the key locally to that end user.



The following are typical enrollment steps performed by an IT admin using YubiEnroll:

1. The IT admin runs the YubiEnroll CLI and authenticates to the identity provider.
2. The IT admin uses YubiEnroll CLI to initiate the enrollment process for an end user's account in the identity provider.
3. YubiEnroll gets the credential creation options from the identity provider.
4. YubiEnroll creates the credentials on a YubiKey which is locally connected or presented to the enrollment workstation.
5. YubiEnroll sets a randomized PIN on the YubiKey.

6. The YubiKey returns the attestation data for the end user's credential to YubiEnroll.
7. YubiEnroll registers the credential for the end user in the identity provider.
8. The IT admin provides the YubiKey and PIN to the end user.

2.1 YubiEnroll CLI

The YubiEnroll Command Line Interface (CLI) tool provides an intuitive interface for interacting with the underlying YubiEnroll solution. You can for example:

- Factory reset the YubiKey
- Set and change the PIN
- Configure Forcing PIN change
- Increase the minimum PIN length
- Configure Always require user verification (AlwaysUV)

For more information, see *Using YubiEnroll CLI*.

2.2 Enrollment Profiles

Enrollment profiles is a YubiEnroll feature that lets users define a combination of preferred configuration option settings, for example `Minimum PIN length` and `Force PIN change` configurations.

Note: The configuration options `Min PIN length`, `Require always UV`, and `Force PIN change before use` require YubiKeys with firmware version 5.5 and higher.

```
PS C:\program files\yubico> yubienroll profiles add entra-reset
Min PIN length [4]: 6
Require always UV? [y/N]: n
Require Enterprise Attestation: [y/N]: n
Force PIN change before use: [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Random PIN length [4]: 6
Assign this profile to the active provider (entra-demo)? [y/N] n
Added profile 'entra-reset'
```

See *Profile Settings* for descriptions of the enrollment profile settings.

The enrollment profile settings are stored with a specific profile name locally on the workstation running YubiEnroll, to be applied when enrolling credentials for end users. Only one enrollment profile can be linked to a provider.

Enrollment profiles can be used with different identity provider configurations, and can also be configured for a provider to be automatically used during enrollment. For more information, see *Identity Provider Configuration*.

2.3 Identity Provider Configuration

When configuring a supported identity provider for YubiEnroll, the following provider-specific configuration parameters are required:

- **NAME** - Name of identity provider.
- **CLIENT_ID** - Identity provider client identifier.
- **REDIRECT_URI** - Authentication resource location.
- **DATA** - Provider-specific data such as `tenant_id` or `domain_name`.

For information on how to obtain these values for supported providers, see the following:

- *Configuring YubiEnroll with Okta*
- *Configuring YubiEnroll with Microsoft Entra ID*
- *Configuring YubiEnroll with PingOne PingID*
- *Configuring YubiEnroll with PingOne AIC*

All provider configurations used by YubiEnroll are stored in a single `yubienroll.toml` file that can be manually edited. The file is located at `%APPDATA%\yubienroll\yubienroll.toml`.

The .toml file accepts a value `cacert` which is the absolute path to the Certificate Authority (CA) bundle. This value lets users specify custom CA bundles if required. CA bundles are expected as a single Privacy-Enhanced Mail (PEM) file containing one or more Root CA certs.

The following example shows a typical provider configuration file. The enrollment profile with the name `profiles.default` is configured to be used by any of the included providers, (in this example, ENTRA and OKTA). The `profiles.default` settings are listed in the `profiles.default` section.

yubienroll.toml

```
active_provider = "entra"

[providers.entra]
provider = "ENTRA"
client_id = "78a1a..."
redirect_uri = "http://localhost/yubienroll-redirect"
tenant_id = "220b41..."
profile = "default"

[providers.okta]
provider = "OKTA"
client_id = "0oahi..."
redirect_uri = "http://localhost:8080/yubienroll-redirect"
domain = "domain.com"
profile = "default"

[profiles.default]
reset = true
min_pin_length = 4
override_always_uv = true
force_pin_change = true
random_pin = true
```

The `active_provider` setting shows the identity provider that is automatically be used when enrolling end users. In the previous example, the active provider is the one named `entra`. There can only be one active provider at the time.

If there are multiple providers configured for an environment, the user can change the active provider by using the command `yubienroll providers activate name`. Where `name` is the name of a configured identity provider.

In addition to activating providers, a user can also create, edit, and delete provider configurations. For more information, see *YubiEnroll Commands*.

2.4 Authentication and Authorization

The user (IT admin, enrollment administrator etc.) authenticates to the identity provider via the system default browser which is automatically launched by YubiEnroll during the login procedure. This includes entering the user account email, and presenting the YubiKey and PIN associated with the user's identity provider account.

During the login procedure an access token is obtained for the identity provider API. The access token lets YubiEnroll interact with the identity provider API to manage end user credentials. The required configuration to connect to the provider, for example tenant name and URL, are either set *manually in the configuration file*, or added *through YubiEnroll*.

YubiEnroll users can log in to the identity provider through the configured system options. Refer to the specific identity provider documentation for details. When setting up and using YubiEnroll, there are a set of user categories typically involved. The permissions for these are defined in the identity provider: Microsoft Entra ID, Okta, PingOne PingID, or PingOne AIC.

The following are typical user categories and their tasks:

- **System administrator:** An employee of an organization responsible for obtaining, installing and configuring the YubiEnroll application.
- **Enrollment administrator:** An employee of an organization responsible for enrolling YubiKey credentials on behalf of their organization's users. Can for example configure PIN settings as required by the organization.
- **End user:** An employee or contractor receiving an enrolled YubiKey to be used to authenticate with services. Might have been granted permission to reset, change the PIN and/or enroll additional keys for themselves as a self-service.
- **Auditor:** An employee of the organization or an external contractor responsible for inspection of logs for audit purposes. Only has read access to the logs.

CHAPTER

THREE

INSTALLING YUBIENROLL CLI

Yubienroll is currently available for identity providers Okta, Microsoft Entra ID, PingOne PingID, and PingOne Advanced Identity Cloud Application (AIC)

3.1 Prerequisites

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

- Windows 11 with administrator privileges.
- Microsoft Entra ID, Okta Identity Engine (OIE), PingOne PingID, or PingOne AIC.
- Permissions to manage users and credentials in the target tenant.

3.2 Downloading

YubiEnroll includes a signed .msi installer for Windows. You can download the YubiEnroll installer from Yubico Downloads.

3.3 Installing on Windows

To install YubiEnroll CLI for Windows, do the following:

1. If not already done, download the installer, see *Downloading*.
2. Open a File Explorer, browse to the **Downloads** folder and double-click the installer.
3. Follow the instructions to complete the YubiEnroll CLI setup steps. The default installation path is `C:\Program Files\Yubico\YubiEnroll\`.

When you have successfully installed YubiEnroll, you are ready to start working with YubiEnroll. For more information, see *Using YubiEnroll CLI*.

CHAPTER

FOUR

USING YUBIENROLL CLI

The following describes how to add identity providers to and enroll end-users with the YubiEnroll CLI.

The examples reference the default installation path. If you choose a different installation path, update the command to point to the path you used. For more information, see also *YubiEnroll Commands*.

Note: Due to Windows restrictions, many commands require administrator privileges. To avoid running the YubiEnroll CLI tool as administrator, the tool itself prompts for elevation when needed through the Windows user account control (UAC) prompt. Launching the YubiEnroll CLI tool as administrator is not recommended.

4.1 Launching on Windows

1. Open a terminal, for example Windows PowerShell.
2. Navigate to the installation path. Default is `C:\Program Files\Yubico\YubiEnroll\`.
3. Run `yubienroll.exe --help` to see the YubiEnroll usage, options, and commands.
4. Run the YubiEnroll commands from the command prompt. See *YubiEnroll Commands*.

4.2 Adding Provider Configurations

The following describes how to add an identity provider configuration and an enrollment profile. The example prompt flows for each identity provider are included. The workflow starts with a first time YubiEnroll log in, where no providers or enrollment profiles exist. However, you can add providers and enrollment profiles at any time.

Note: When adding a provider configuration, you need to provide identity provider-specific values for `Client ID`, `Redirect URI`, and `Tenant/Domain ID`. For information on how to obtain these values, see *Identity Provider Configuration*.

The `yubienroll providers add` command adds a provider configuration of a supported type (Microsoft Entra ID, Okta, PingOne PingID, or PingOne AIC). If no provider configuration exists and you choose to add one, the provider is automatically activated and becomes the default provider for enrolling end users.

To add a provider configuration and an enrollment profile, complete the steps in the following sections for your provider.

4.2.1 Adding Microsoft Entra ID

1. In a terminal, run the command:

```
yubienroll providers add entra-demo
```

   Where `entra-demo` is the provider name. Choose any name that is useful to you.

2. Select the desired provider type.

```
Supported identity providers:
[1] ENTRA
[2] OKTA
[3] PING_ONE
[4] PING_ONE_AIC
Select provider: 1
```

3. Enter the **Client ID** and **Redirect URI**. For provider-specific input values, see *Identity Provider Configuration*.

```
Enter the Client ID: c64e5ed2. . .
Enter the Redirect URI: http://localhost:8080/yubienroll-redirect
```

4. Enter the provider values collected from the identity provider app configuration.

```
Enter the Microsoft Entra Tenant ID: 220b415
Enter the Microsoft Entra Tenant endpoint [https://login.microsoftonline.com]:
Enter the Microsoft Graph endpoint [https/graph.microsoft.com]:
```

   Where Entra specific prompts include values you collected from Entra ID. You can use default values in most cases. If your organization is working with government tenants, you might need to change the endpoints. See *Preparing to Add the Entra ID Provider*.

5. Select if you want to create a new enrollment profile. See *Creating Enrollment Profiles* for descriptions of all the profile options. If you select `Y`, complete the following prompts.

```
Do you want to create and add an enrollment profile? [y/N]: y
Profile name [default]: entra-main
Min PIN length [4]: 6
Require always UV? [y/N]: n
Require Enterprise Attestation: [y/N]: n
Force PIN change before use: [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Random PIN length [4]: 6
Added profile 'entra-main'
```

6. Activate the provider.

   The provider configuration is added together with the enrollment profile. If no provider existed previously, the provider is automatically activated. If this is an additional provider, you are prompted to confirm before activating.

```
Added provider 'entra-demo'.
Activated provider.
```

7. To check provider and authentication status and see available enrollment profiles you can run `yubienroll status` and `yubienroll profiles list`. This example is with Entra ID.

```
PS C:\program files\yubico> yubienroll status
Active provider set to 'entra-demo' using Microsoft Entra ID.
Checking authentication status . . .
You are currently authenticated.
PD C:\progream files\yubico> yubienroll profiles list
Name        Minimum PIN length  Require always UV  Require each  Force PIN change ␣
↪Factory reset  Random PIN
entra-main  6                   False              False         True             ␣
↪False          True
PS C:\program files\yubico>
```

For more information about the `yubienroll providers` command, see *YubiEnroll Commands*.

4.2.2 Adding Okta

1. In a terminal, run the command:

   ```
   yubienroll providers add okta-demo
   ```

   Where `okta-demo` is the provider name. Choose any name that is useful to you.

2. Select the desired provider type.

   ```
   Supported identity providers:
   [1] ENTRA
   [2] OKTA
   [3] PING_ONE
   [4] PING_ONE_AIC
   Select provider: 2
   ```

3. Enter the **Client ID** and **Redirect URI** when prompted. For provider-specific input values, see *Identity Provider Configuration*.

   ```
   Enter the Client ID: 0oalrpp312ZBUw1Xs1d7
   Enter the Redirect URI: http://localhost:8080/yubienroll-redirect
   ```

4. Enter the provider values collected from the identity provider app configuration.

   ```
   Enter the Okta domain (e.g. 'example.okta.com'): yubico-poc.oktapreview.com
   ```

   Okta specific prompts are values you collected from Okta. In this example, `yubico-poc.oktapreview.com` is the Okta domain. See *Using Custom Domains*.

5. Specify if you want to create a new enrollment profile. See *Creating Enrollment Profiles* for descriptions of all the profile options. If you select `Y`, complete the following prompts.

   ```
   Do you want to create and add an enrollment profile? [y/N]: y
   Profile name [default]: okta-main
   Min PIN length [4]: 6
   Require always UV? [y/N]: n
   Require Enterprise Attestation: [y/N]: n
   Force PIN change before use: [y/N]: y
   Factory reset the Security Key? [y/N]: n
   Set a new random PIN? [Y/n]: y
   ```

(continues on next page)

(continued from previous page)

```
Random PIN length [4]: 6
Added profile 'okta-main'
```

6. Activate the provider.

   The provider configuration is added together with the enrollment profile. If no provider existed previously, the provider is automatically activated. If this is an additional provider, you are prompted to confirm before activating.

```
Do you want to activate this provider? [y/N]: y
Added provider 'okta-demo'.
Activated provider.
```

7. To check provider and authentication status and see available enrollment profiles you can run `yubienroll status` and `yubienroll profiles list`. This example is with Entra ID.

```
PS C:\program files\yubico> yubienroll status
Active provider set to 'entra-demo' using Microsoft Entra ID.
Checking authentication status . . .
You are currently authenticated.
PD C:\progream files\yubico> yubienroll profiles list
Name        Minimum PIN length  Require always UV  Require each  Force PIN change ␣
↪Factory reset  Random PIN
entra-main  6                   False              False         True             ␣
↪False          True
PS C:\program files\yubico>
```

For more information about the `yubienroll providers` command, see *YubiEnroll Commands*.

4.2.3 Adding PingOne PingID

1. In a terminal, run the command:

```
yubienroll providers add ping-demo
```

   Where `ping-demo` is the provider name. Choose any name that is useful to you.

2. Select the desired provider type.

```
Supported identity providers:
[1] ENTRA
[2] OKTA
[3] PING_ONE
[4] PING_ONE_AIC
Select provider: 3
```

3. Enter the **Client ID** and **Redirect URI** when prompted. For provider-specific input values, see *Identity Provider Configuration*.

```
Enter the Client ID: 822b253b-4717-4169-9292-b1ef9d7894c2
Enter the Redirect URI: http://localhost/yubienroll-callback
```

4. Enter the provider specific values collected from the identity provider app configuration.

```
Enter the PingOne environment ID: c15efa10-4ebb-449b-9b27-97b3264de073
Do you want to configure a custom domain? [y/N]: N
Do you want to configure a non-default PingOne MFA policy? [y/N]: N
```

Where PingOne PingID specific prompts include values you collected from PingOne PingID. See *Using Custom Domains* and *Enabling MFA and FIDO2 Policies*.

5. Specify if you want to create a new enrollment profile. See *Creating Enrollment Profiles* for descriptions of all the profile options. If you select `Y`, complete the following prompts.

```
Do you want to create and add an enrollment profile? [y/N]: y
Profile name [default]: ping-main
Min PIN length [4]: 6
Require always UV? [y/N]: n
Require Enterprise Attestation: [y/N]: n
Force PIN change before use: [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Random PIN length [4]: 6
Added profile 'ping-main'
```

6. Activate the provider.

   The provider configuration is added together with the enrollment profile. If no provider existed previously, the provider is automatically activated. If this is an additional provider, you are prompted to confirm before activating.

```
Do you want to activate this provider? [y/N]: y
Added provider 'ping-demo'.
Activated provider.
```

7. To check provider and authentication status and see available enrollment profiles you can run `yubienroll status` and `yubienroll profiles list`. This example is with Entra ID.

```
PS C:\program files\yubico> yubienroll status
Active provider set to 'entra-demo' using Microsoft Entra ID.
Checking authentication status . . .
You are currently authenticated.
PD C:\progream files\yubico> yubienroll profiles list
Name        Minimum PIN length  Require always UV  Require each  Force PIN change
↪Factory reset  Random PIN
entra-main  6                   False              False         True
↪False          True
PS C:\program files\yubico>
```

For more information about the `yubienroll providers` command, see *YubiEnroll Commands*.

4.2.4 Adding PingOne AIC

1. In a terminal, run the command:

```
yubienroll providers add ping-aic-demo
```

   Where `ping-aic-demo` is the provider name. Choose any name that is useful to you.

2. Select the desired provider type.

```
Supported identity providers:
[1] ENTRA
[2] OKTA
[3] PING_ONE
[4] PING_ONE_AIC
Select provider: 4
```

3. Enter the **Client ID** and **Redirect URI** when prompted. For provider-specific input values, see *Identity Provider Configuration*.

```
Enter the Client ID: YubiEnrollApp
Enter the Redirect URI: http://localhost:8443/yubienroll-redirect
```

4. Enter the provider specific values collected from the identity provider app configuration.

```
Enter the PingOne Advanced Identity Cloud tenant name (e.g. 'example.forgeblocks.com
↪'): openam-tntp-yubico.forgeblocks.com
Enter the PingOne Advanced Identity Cloud realm name: alpha
Enter the PingOne Advanced Identity Cloud WebAuthn registration journey name:␣
↪YubiEnroll_Admin_Registration
```

   Where PingOne AIC specific prompts include values you collected from PingOne AIC. For example:

   - `openam-tntp-yubico.forgeblocks.com` is the tenant name
   - `alpha` is the realm name
   - `YubiEnroll_Admin_Registration` is the WebAuthn registration journey name

   See *Registering the YubiEnroll App* and *Creating a WebAuthn Registration Journey*.

5. Specify if you want to create a new enrollment profile. See *Creating Enrollment Profiles* for descriptions of all the profile options. If you select `Y`, complete the following prompts.

```
Do you want to add an enrollment profile? [y/N]: y
Profile name [default]: ping-aic-main
Min PIN length [4]: 6
Require always UV? [y/N]: n
Require Enterprise Attestation: [y/N]: n
Force PIN change before use: [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Random PIN length [4]: 6
Added profile 'ping-aic-main'
```

6. Activate the provider.

The provider configuration is added together with the enrollment profile. If no provider existed previously, the provider is automatically activated. If this is an additional provider, you are prompted to confirm before activating.

```
Do you want to activate this provider? [y/N]: y
Added provider 'ping-aic-demo'.
Activated provider.
```

7. To check provider and authentication status and see available enrollment profiles you can run `yubienroll status` and `yubienroll profiles list`. This example is with Entra ID.

```
PS C:\program files\yubico> yubienroll status
Active provider set to 'entra-demo' using Microsoft Entra ID.
Checking authentication status . . .
You are currently authenticated.
PD C:\progream files\yubico> yubienroll profiles list
Name        Minimum PIN length  Require always UV  Require each  Force PIN change␣
↪Factory reset  Random PIN
entra-main  6                   False              False         True             ␣
↪False          True
PS C:\program files\yubico>
```

For more information about the `yubienroll providers` command, see *YubiEnroll Commands*.

4.3 Creating Enrollment Profiles

The following describes how to create and add an enrollment profile. You can add an enrollment profile at the same time when you add an identity provider to YubiEnroll. You can also add an enrollment profile at a later occasion and assign this to the active provider. This example is with Entra ID.

To create an enrollment profile for a provider, do the following:

1. In the terminal, run `yubienroll profiles add entra-reset`

   Where `entra-reset` is the profile name in this example. You can enter a name of your choosing.

2. Enter the following when prompted. See *Profile Settings* for a description of each setting.

```
PS C:\program files\yubico> yubienroll profiles add entra-reset
Min PIN length [4]: 6
Require always UV? [y/N]: n
Require Enterprise Attestation: [y/N]: n
Force PIN change before use: [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Random PIN length [4]: 6
Assign this profile to the active provider (entra)? [y/N]: n
```

3. Confirm to add the profile:

```
Assign this profile to the active provider (entra-demo)? [y/N]
Added profile 'entra-reset'
```

   Where `entra-reset` is the provider name assigned in YubiEnroll.

For more information about the `yubienroll profiles` command, see *YubiEnroll Commands*.

4.3.1 Profile Settings

Note: The configuration options `Min PIN length`, `Require always UV`, and `Force PIN change before use` require YubiKeys with firmware version 5.5 and higher.

Profile Option	Description	Setting
Profile name [default]	The name to be used for the profile. Prompted if Name is not included in the command.	If no name entered at prompt, `default` is the name assigned.
Min PIN length [4]	The minimum number of characters required for the PIN used with the YubiKey.	Enter value for PIN length, example `6`. Minimum PIN length is `4`. Default: `4`
Require always UV? [y/N]	Enforces user verification (UV) in all cases, whether the relying party requests it or not.	`Y` requires user verification always. `N` user verification is overridden. Default: `No`.
Require Enterprise Attestation? [y/N]	Should enterprise attestation be required.	`Y` requires enterprise attestation. `N` enterprise attestation not required. Default: `No`.
Force PIN change before use? [y/N]	Force the end user to change the provided PIN when using the YubiKey the first time.	`Y` requires user to reset PIN. `N` allows user to use factory PIN. Default: `No`.
Factory reset the Security Key? [Y/n]	For keys that have previously been in use. Clears existing configurations.	`Y` to enroll previously used key. `N` to enroll a new (blank) key. Default: `Y`.

continues on next page

Table 1 – continued from previous page

Profile Option	Description	Setting
Set a new random PIN [Y/n]	YubiEnroll generates a random PIN for the key.	`Y` YubiEnroll sets the key PIN. `N` you enter the key PIN. Default: `Y`.
Random PIN length [6]	Define the length of the random PIN to be set. Prompt if `Set a new random PIN` is `Y`.	Enter value for PIN length, example `6`. Minimum PIN length is `4`. Default: `6`.
Assign this profile to the active provider (entra)? [y/N]	If there is an existing profile. Select to override the existing profile for the active provider.	`Y` replaces current enrollment profile. `N` keeps the current enrollment profile. Default: `N`

4.4 Enrolling End Users

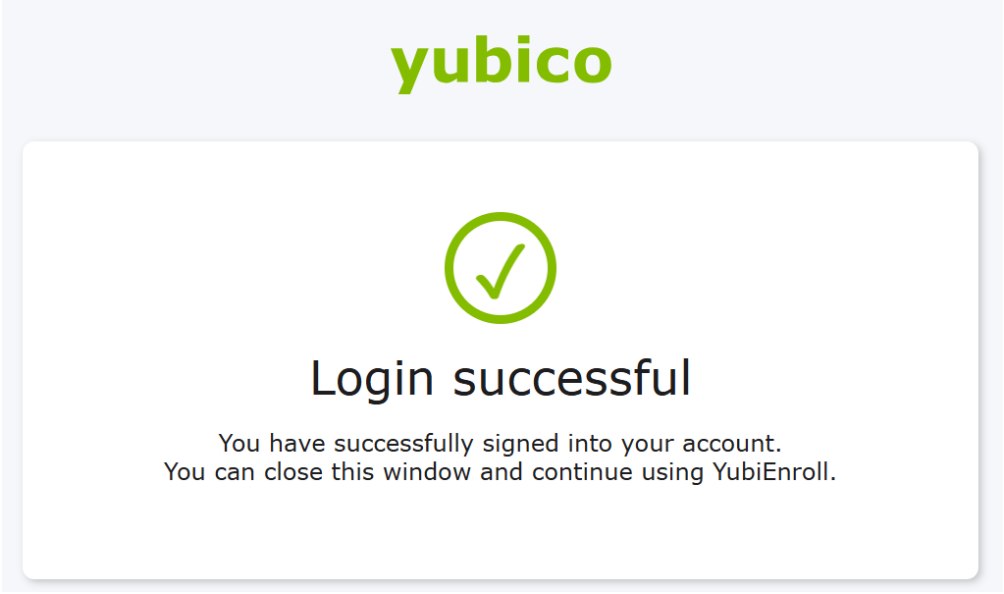
The following describes how to enroll a YubiKey adding credentials on behalf of a specific end user. Ensure you have the YubiKey you want to enroll available, as well as the `ID` or `Username` of the end user.

If you are using Microsoft Entra ID, the `user_id` can be provided either as Object ID (unique identifier), for example `123456-abc-123456-xyz`, or as UPN (User Principal Name), for example `username@yubico123.sample.com`. For information on how to find an end user identifier, see the command *yubienroll users*.

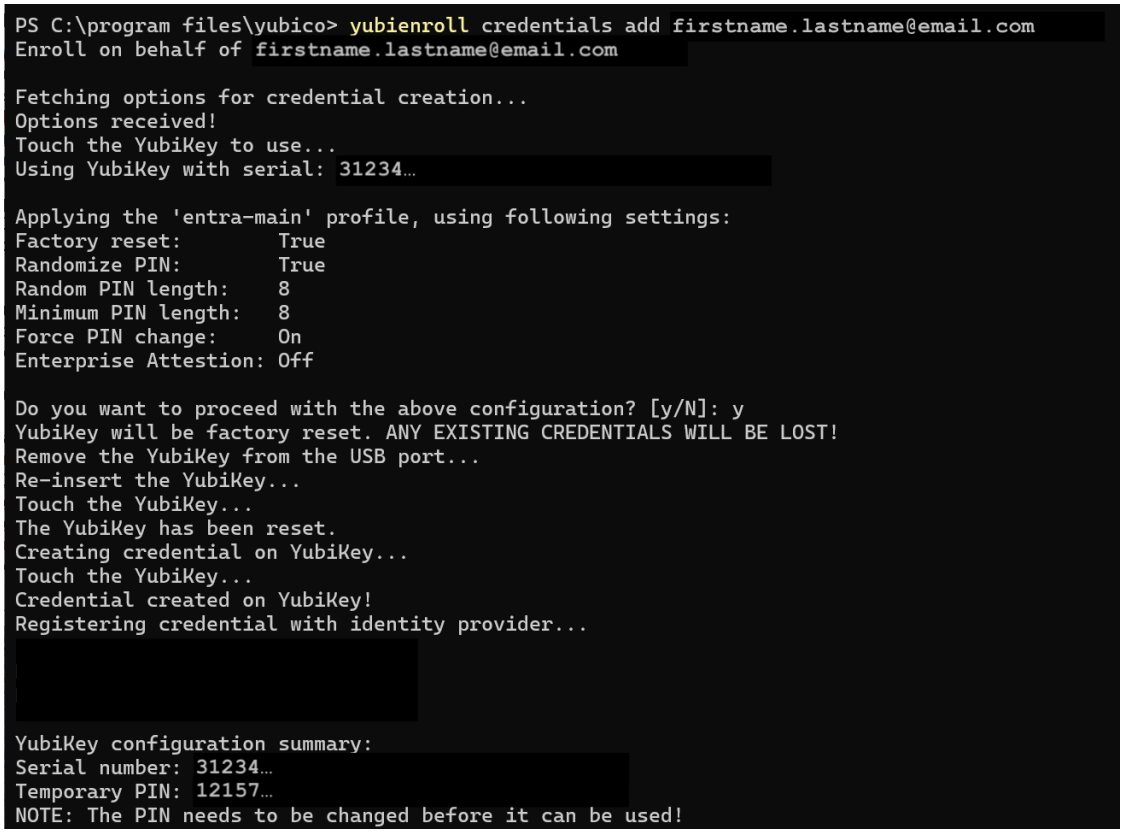
Note: To enroll YubiKeys on behalf of end users, you need to be an administrator with IDP-specific permissions. For more information, see the Configuring Permissions section for the IDP you are using.

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

1. In the terminal, run `yubienroll login` to authenticate with the identity provider.
2. Select the desired provider, `[1] ENTRA` in this example.
3. When prompted, confirm the **Client ID**, **Redirect URI**, and **Tenant ID** for the active provider to continue. For information on how to obtain these values for a provider, see *Identity Provider Configuration*.
4. Follow the steps to complete the authentication. When successfully authenticated, return to the terminal.



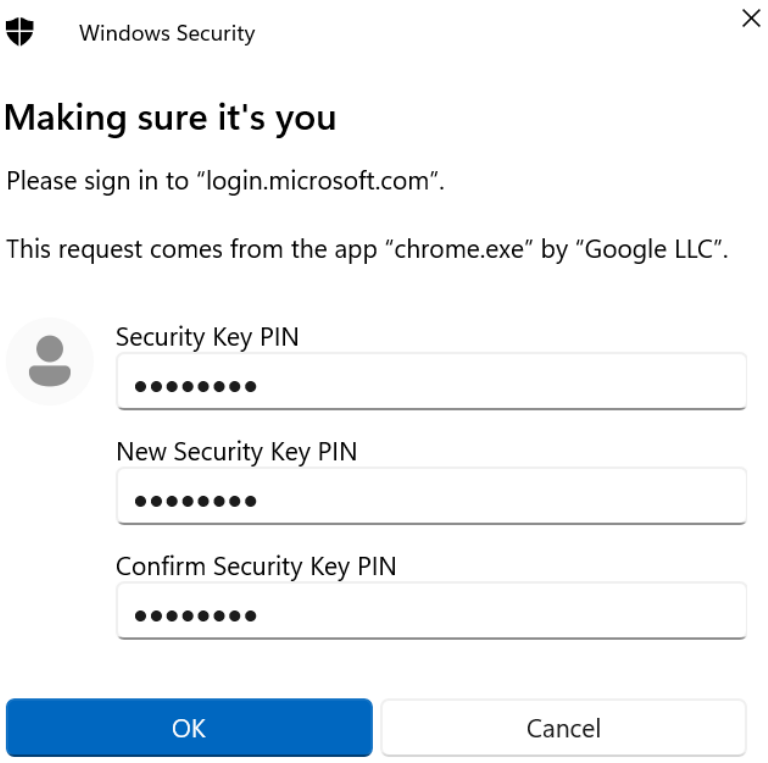
5. Insert or present the YubiKey you want to enroll.
6. Run the command `yubienroll credentials add firstname.lastname@email.com` where `firstname.lastname\@email.com` is the end users' account identifier in this example.
7. YubiEnroll fetches the provider-specific options for creating credentials, and the settings for the enrollment profile to be used are displayed. To use a different enrollment profile than the one assigned to the active provider, see the command *yubienroll profiles*. In this example, the key is reset before the credentials are added.
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 is displayed. See also *yubienroll credentials*.



11. Provide the YubiKey and the temporary PIN to the end user.

4.4.1 Initial Authentication

To authenticate with the identity provider, the end user presents their YubiKey and enters the provided PIN. If `Force PIN change` is set to `True` (and if supported by the platform), the end user is prompted to change the PIN when using the YubiKey for the first time, as in this example.

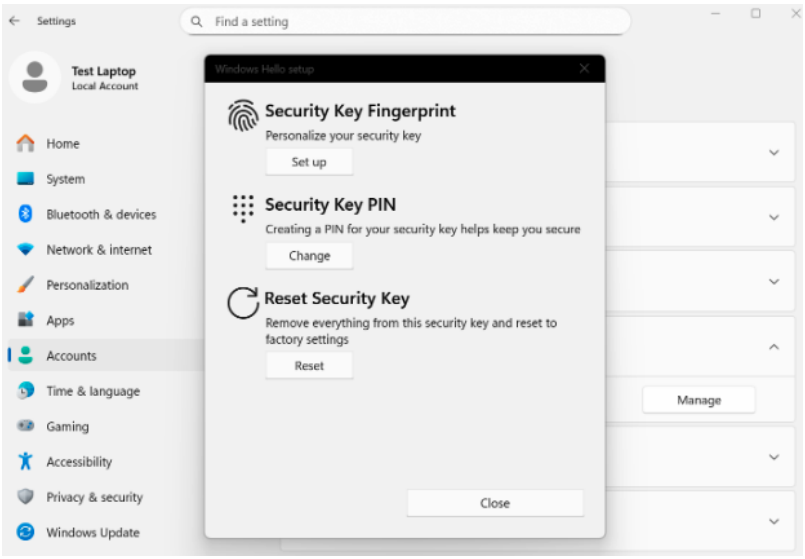


If `Force PIN change` was not set (is `False`), the end user is able to log in without changing the provided PIN, when using the YubiKey for the first time.

The previous step also applies when using a *YubiKey Bio (FIDO and Multi-Protocol Editions)* where the end user authenticates primarily using fingerprint(s) enrolled on the key (a PIN is required as fallback also when using fingerprint authentication).

Note: In most cases, the end user is *not* automatically prompted to enroll a fingerprint when using a pre-registered YubiKey Bio the first time. Enrolling a fingerprint must be done by the end user in a separate step as described in the following.

Here is an example of how to enroll fingerprints when using *Windows 11*: Navigate to **Settings > Accounts > Sign-in options**, select **Security key**, and click **Manage**. Enter the PIN for the YubiKey Bio, and follow the on-screen instructions, which prompts you to insert the security key and touch it to enroll a fingerprint. When done, you is prompted to provide the fingerprint (instead of the PIN) when logging in.



Different platforms (device/OS/browser) have different flows with regards to enrolling fingerprints on YubiKeys. Refer to the account security settings information for each platform for instructions on how to enroll fingerprints. For more examples of fingerprint enrollment, see YubiKey Bio Series Specifics.

Yubico Authenticator is a convenient tool that can also be used to enroll fingerprints on a YubiKey Bio. For instructions on how to install Yubico Authenticator and enroll fingerprints, see Install the App and Enroll a fingerprint.

Select the method that is applicable to your organization's IT platform when providing recommendations for your end users on how to enroll fingerprints on their pre-registered YubiKey Bio.

CHAPTER

FIVE

YUBIENROLL IDENTITY PROVIDERS

Each integrated identity provider (IdP) requires specific setup.

5.1 Configuring YubiEnroll with Microsoft Entra ID

The following describes how to set up YubiEnroll in the Microsoft Entra ID tenant and configure the required user permissions.

5.1.1 Configuration Steps

The configuration steps involve the following:

- *Enabling multi-factor authentication for YubiKeys in Microsoft Entra ID*.
- *Registering the YubiEnroll application in Microsoft Entra ID*.
- *Configuring the YubiEnroll permissions in Microsoft Entra ID*.
- *Adding the Microsoft Entra ID provider in YubiEnroll*.

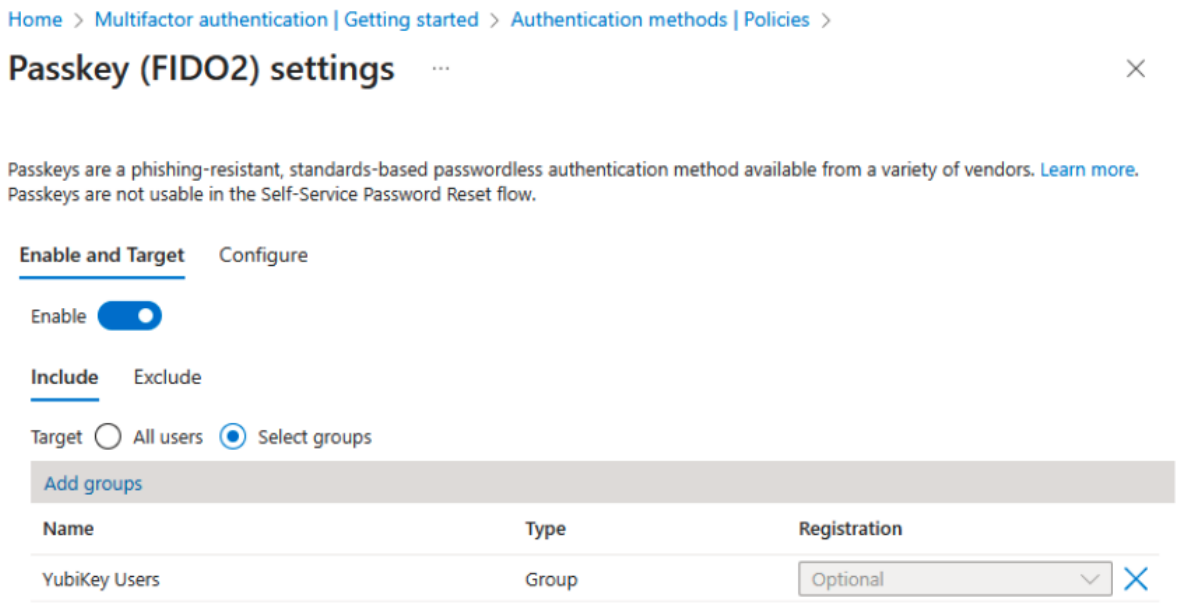
When you have successfully completed these steps, you are ready to *enroll YubiKeys on behalf of end users in your organization*.

5.1.2 Enabling 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 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 Entra ID, see Enable passkeys (FIDO2) for your organization (Microsoft documentation).



5.1.3 Registering the YubiEnroll App

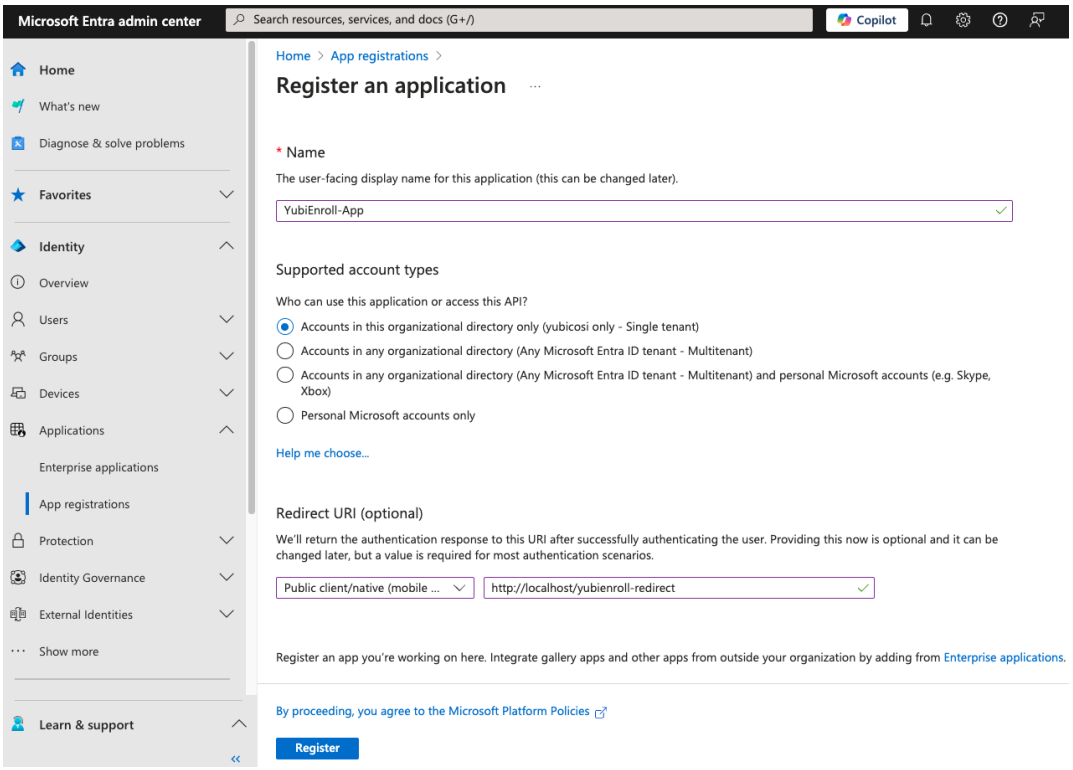
When configuring the Microsoft Entra ID provider in YubiEnroll, the following parameter values are needed:

- `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, log in to the Entra admin center, go to **Application > App registrations** and select **New registration**.

When registering the YubiEnroll app, ensure the following:

- 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.



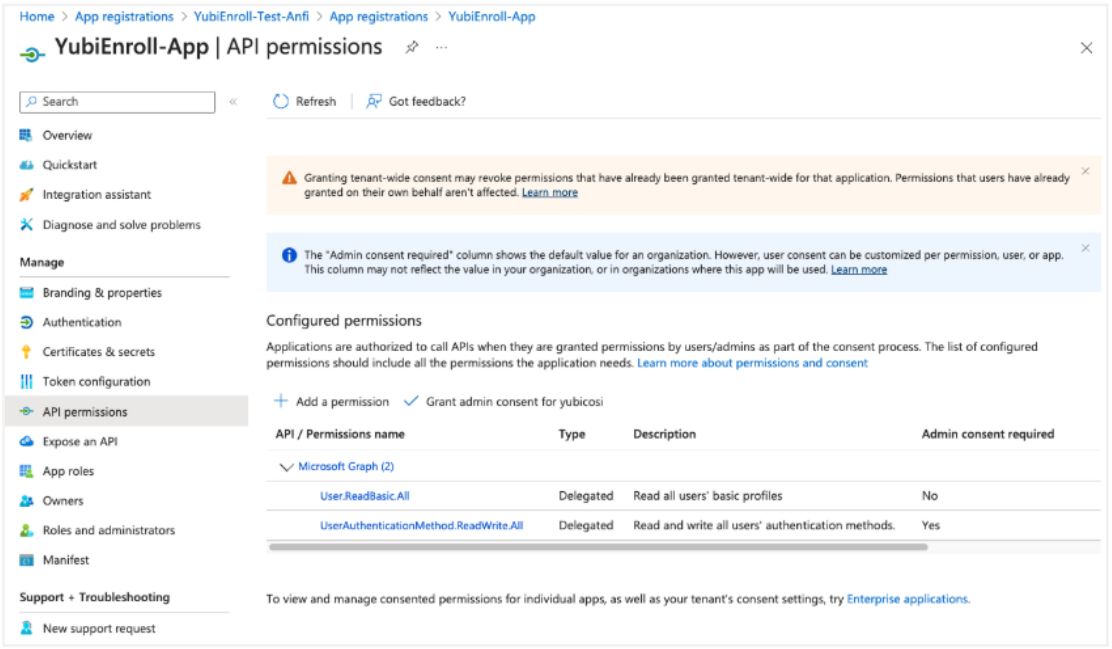
For more details on how to register the YubiEnroll app, see Register an application with the Microsoft identity platform (Microsoft documentation).

5.1.4 Configuring 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**.



Note: When registering an app in Microsoft Entra ID, two types of Microsoft Graph permissions can be assigned: *Application* and *Delegated*. For YubiEnroll it is crucial to only configure *Delegated* permissions to ensure that the app's access is limited to the logged in user's permissions.

When combined with the Microsoft Entra ID feature **Administrative units**, this setup allows for fine-grained control of access based on groups, users, or specific properties such as location. An example where this can be leveraged is where an administrator could be allowed to manage YubiKey enrollments only for users in their administrative unit. To review permissions granted to a registered app, check the **Type** settings under **API permissions** for the app.

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.

For more information about app permissions, see Overview of Microsoft Graph permission (Microsoft documentation).

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.

Important: Even with the *Privileged Authentication Administrator*, an administrator is not able to use YubiEnroll to manage passkeys for their own profile.

For more information, see Authentication Administrator (Microsoft documentation) and Privileged Authentication Administrator (Microsoft documentation).

5.1.5 Preparing to Add the Entra ID Provider

Before you can run YubiEnroll with Microsoft Entra ID, you must add the provider configuration in YubiEnroll.

When adding a provider configuration in YubiEnroll you need the following values, created when the *app was registered*.

- Application (client) ID
- Directory (tenant) ID
- Redirect URI

To find these values in Microsoft Entra ID, locate the YubiEnroll app and select **Overview**. The values are displayed in the **Essentials** section for the app.

For information on how to add a provider configuration in YubiEnroll, see *Adding Provider Configurations* and *YubiEnroll Commands*.

Note: When configuring a Microsoft Entra ID provider, you are prompted to specify the *Microsoft Entra ID endpoint* which defaults to `\https://login.microsoftonline.com`, and the *Microsoft Graph endpoint* which defaults to `\https://graph.microsoft.com`. The normal case is to use these default values. However, if you are using *national cloud deployments* you need to change these endpoints. For more information, see Microsoft Graph national cloud deployments (Microsoft documentation).

5.2 Configuring YubiEnroll with Okta

The following describes how to set up YubiEnroll in the Okta tenant and configure the required user permissions.

5.2.1 Configuration Steps

The configuration steps involve the following:

1. *Registering the YubiEnroll application in Okta*.
2. *Configuring the YubiEnroll permissions in Okta*.
3. *Adding the Okta provider in YubiEnroll*.

When you have successfully completed these steps, you are ready to *enroll YubiKeys on behalf of end users in your organization*.

5.2.2 Registering the YubiEnroll App

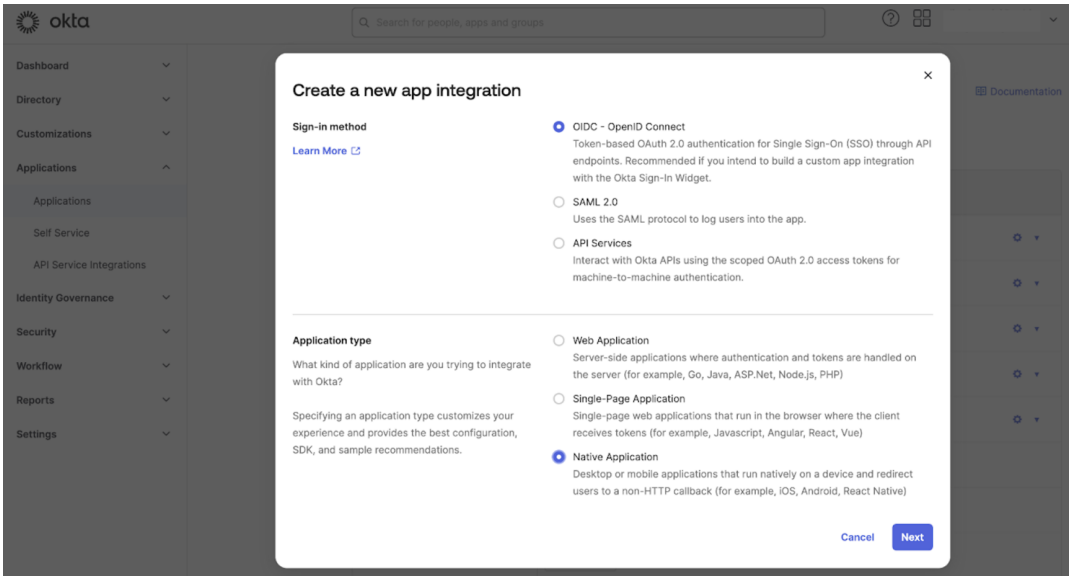
Note: To register the YubiEnroll app in the Okta tenant as described in the following, you need *Super Admin* or *Application Admin* permissions. For more information, see *Configuring Permissions*.

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

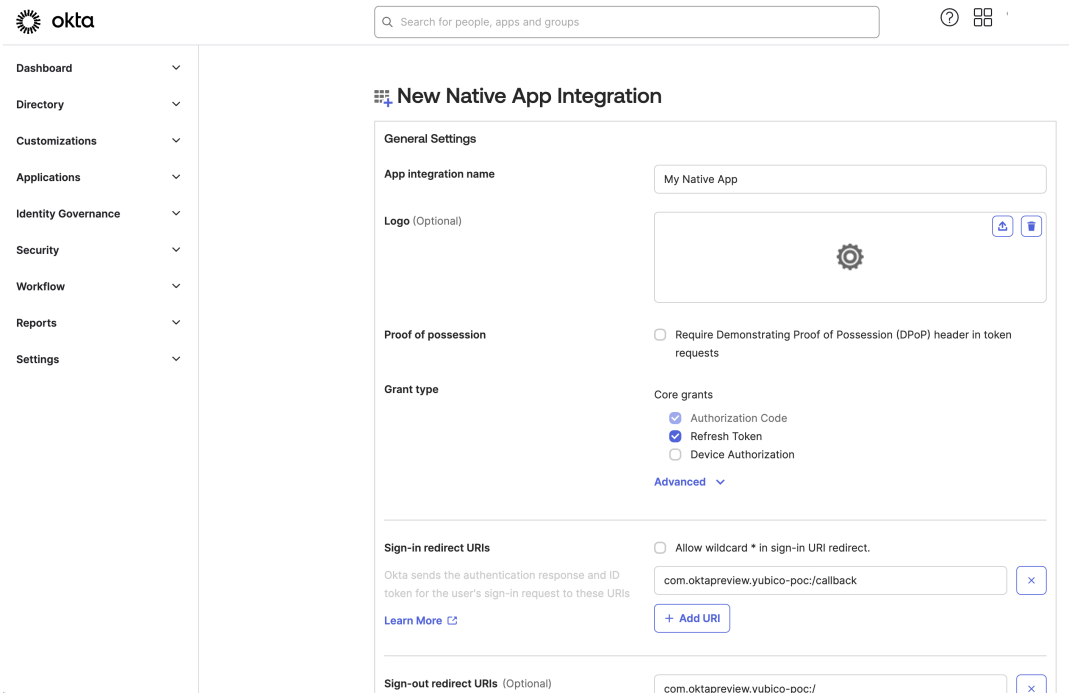
- `client_id`
- `domain`
- `redirect_uri`

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 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 issues a refresh token once it expires.



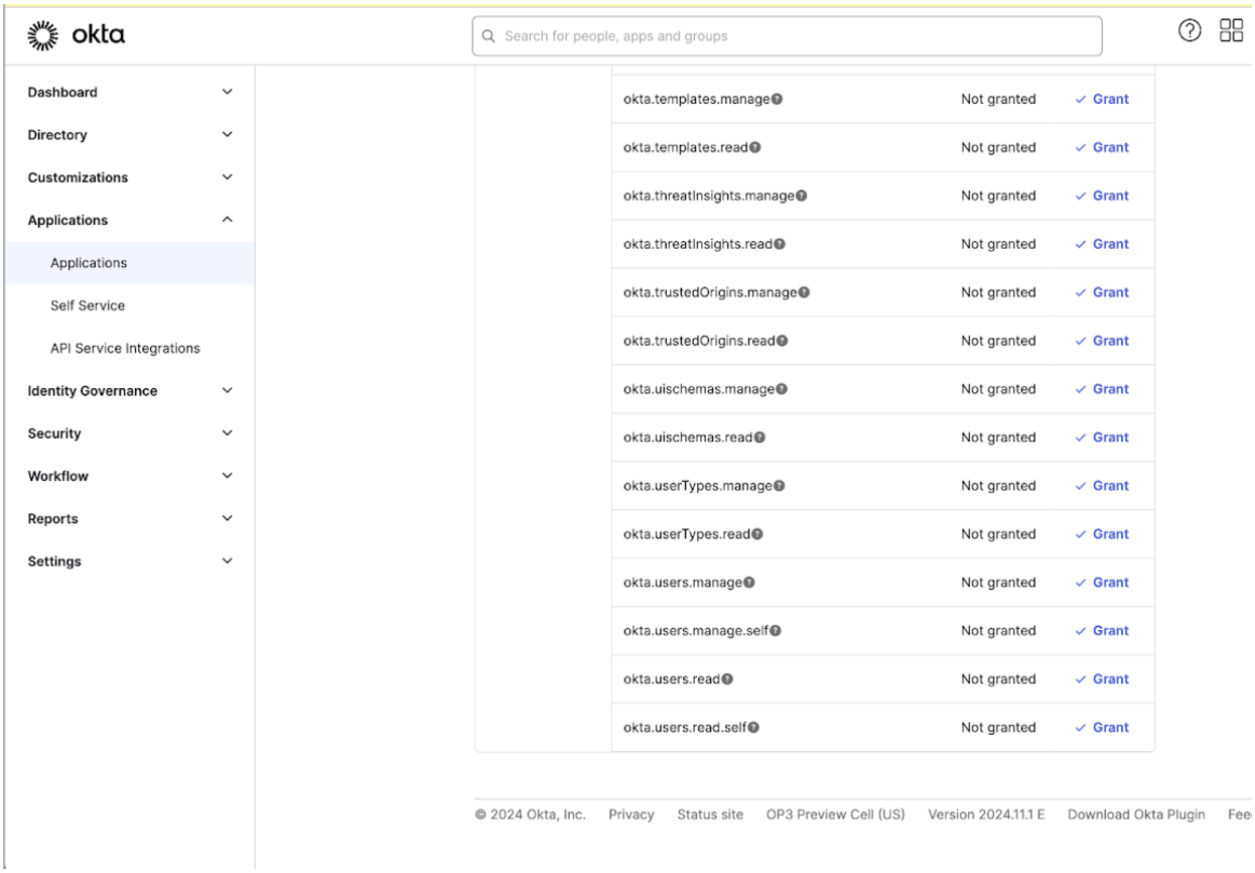
For more details on how to register the YubiEnroll app, see Create an OAuth 2.0 app in Okta (Okta documentation).

During registration, the following values needed to configure YubiEnroll are created:

- Application (client) ID
- Directory (tenant) ID
- Sign-in redirect URI

5.2.3 Configuring 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 for example) must have either the *Super Administrator*, *Group Administrator*, or *Organization Administrator* role in Okta.

5.2.4 Preparing to Add the Okta Provider

Before you can run YubiEnroll with Okta, you must add the provider configuration in YubiEnroll.

When adding a provider configuration in YubiEnroll you need the following values, created when the *app was registered*:

- Application (client) ID
- Directory (tenant) ID
- Redirect URI

The **Client ID** and **Redirect URI** can be found in 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, it is displayed under the email address.

For information on how to add a provider configuration in YubiEnroll, see *Adding Provider Configurations*.

5.2.5 Using Custom Domains

If you are using a custom domain with Okta, some applications might still require an `\*\.okta.com` sub-domain instead of a custom second level domain.

The FIDO2 credentials are registered per domain, and in cases with two domains the credentials must be registered on both. For more information, see Register FIDO2 (WebAuthN) Keys under both Custom Domain URL and Okta Org URL (Okta documentation).

In a scenario when using YubiEnroll with a default Okta domain and a custom domain, you need to register two FIDO2 credentials for an end user account. You can address this by having two enrollment profiles pointing to the same Okta tenant, but with different domains. This results in two FIDO2 credentials being pre-registered on the YubiKey for the end user. For more information, see *Creating Enrollment Profiles* and *yubienroll profiles*.

You can also customize your Okta domain name with your company's own domain name. For example, instead of the default *<companyname>.okta.com*, you can create *login.companyname.com*.

To ensure YubiEnroll is configured to use the correct domain, review the domain configuration during the provider setup. Ensure user credentials are being enrolled for the domain for which they need access. If a user requires access to both the default Okta domain and the custom domain, configure an additional Okta Provider using the same application, but using the custom domain name in the configuration. For more information, see Customize domain and email address (Okta documentation).

5.2.6 Searching for Users

In Okta a user needs to have a *username* and an *email*. By default the username is an email address, and usually the username and the email are identical, but they do not have to be.

When connected to the Okta IDP, you can search for a user either by display name (firstname + lastname), username, or primary email address. The returned search result includes the **ID**, **Display Name**, **Username**, and **Email** for each user.

Note: When performing enrollment operations on behalf of a user, you can only use the **username** or **user ID** values. Using the email address does not work. For search examples, see *YubiEnroll Commands*.

5.3 Configuring YubiEnroll with PingOne PingID

The following describes how to set up YubiEnroll in the PingOne PingID tenant and configure the required user permissions.

5.3.1 Configuration Steps

The configuration steps involve the following:

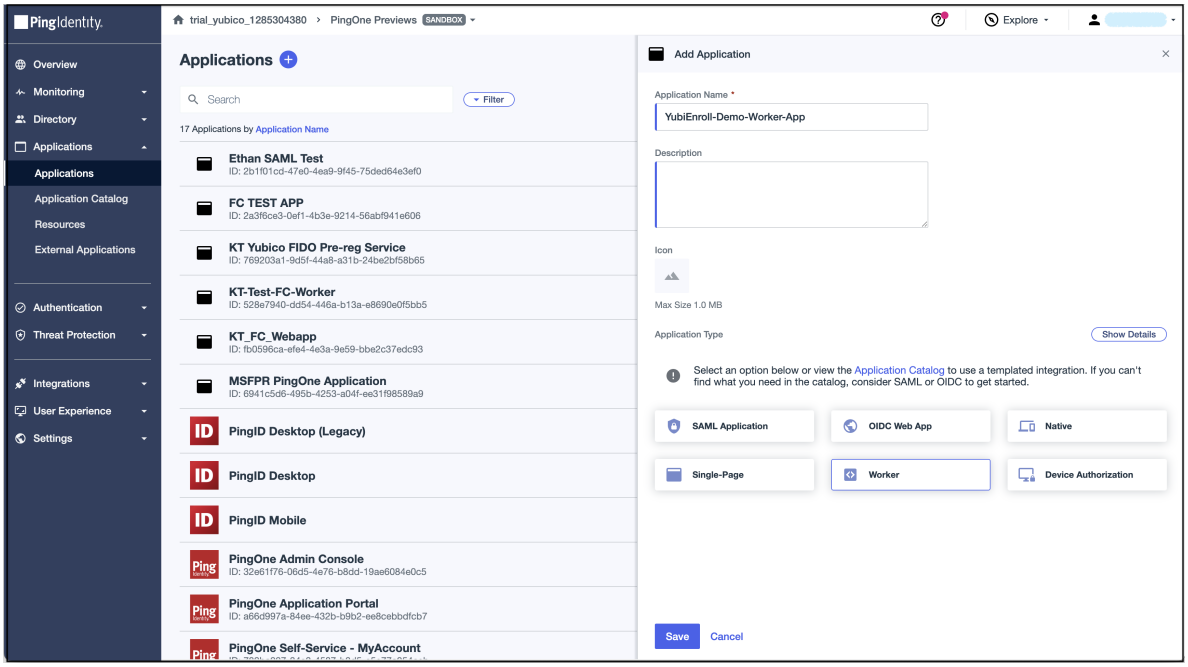
1. *Registering the YubiEnroll App*
2. *Configuring Permissions*
3. *Preparing to Add the PingOne PingID Provider*
4. Optional, *Enabling MFA and FIDO2 Policies*
5. Optional, *Using Custom Domains*

When you have successfully completed these steps, you are ready to *enroll YubiKeys on behalf of end users in your organization*.

5.3.2 Registering the YubiEnroll App

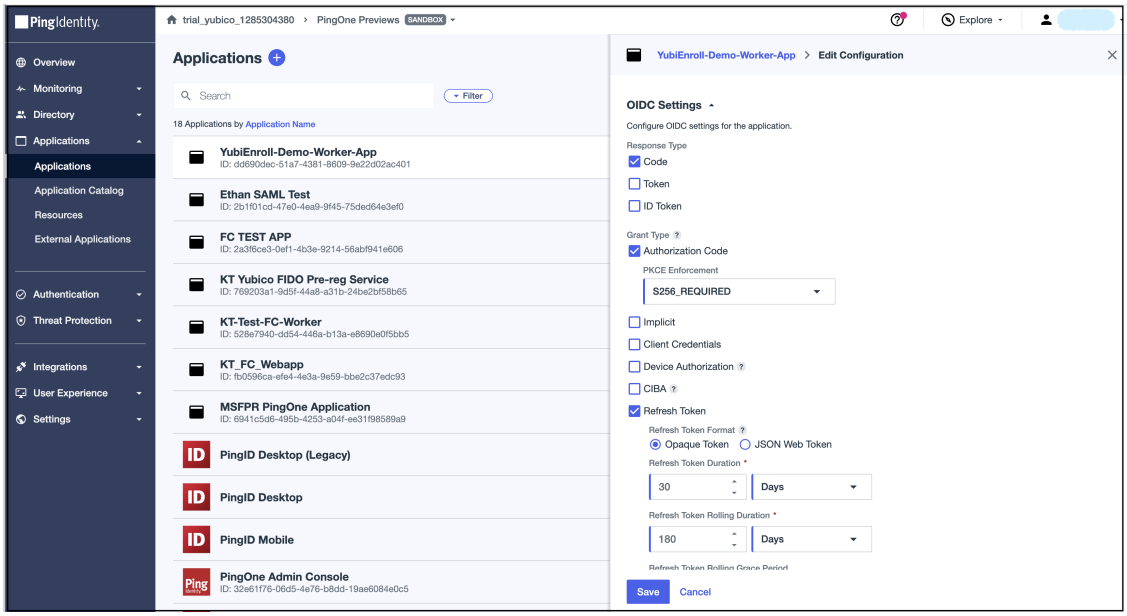
Register the YubiEnroll app as an OAuth2 app. Complete the steps:

1. Create a new application.
    a. Log in to the PingOne PingID Console.
    b. From the left panel, select **Applications**.
    c. Click the plus (**+**) to add a new application.
    d. Enter an **Application Name**. The example shows `YubiEnroll-Demo-Worker-App`.
    e. Select Application Type, **Worker**.
    f. Click **Save**.



2. Set the Configuration.
    a. Select the **Configuration** tab.
    b. In OIDC Settings, select:

- Response Type, check **Code**.
- Grant Type:
  - Check **Authorization Code**
  - Select PKCE Enforcement under Authorization Code, **S256_REQUIRED**.
  - Check **Refresh Token**.

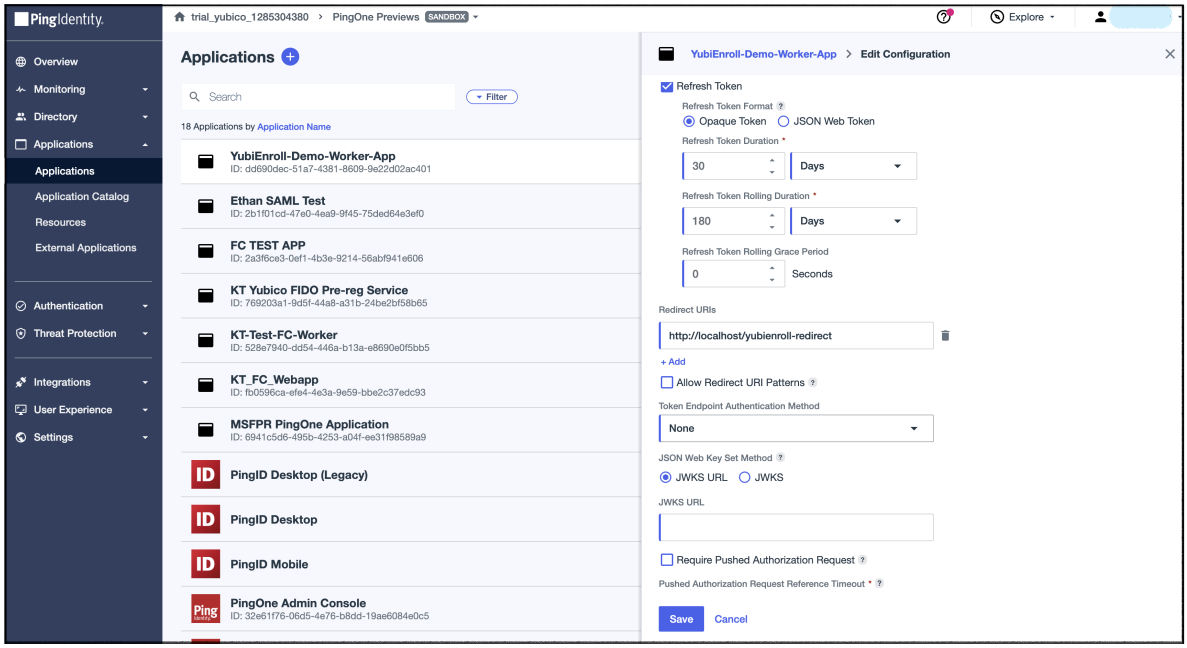


c. Enter a Redirect URI. For example, http://localhost:9443/yubienroll-callback.

You must specify a port if you are not using URI patterns.

d. Select Token Endpoint Authentication Method, **None**.

e. Click **Save**.



3. Activate the app. Click the activation toggle **On**.



For PingOne PingID source content, see PingOne PingID Adding an Application.

5.3.3 Configuring Permissions

To enroll YubiKeys on behalf of an end user, the YubiEnroll app user, for example an IT admin, must have PingOne PingID roles: `Identity Data Admin` and `Environment Admin`.

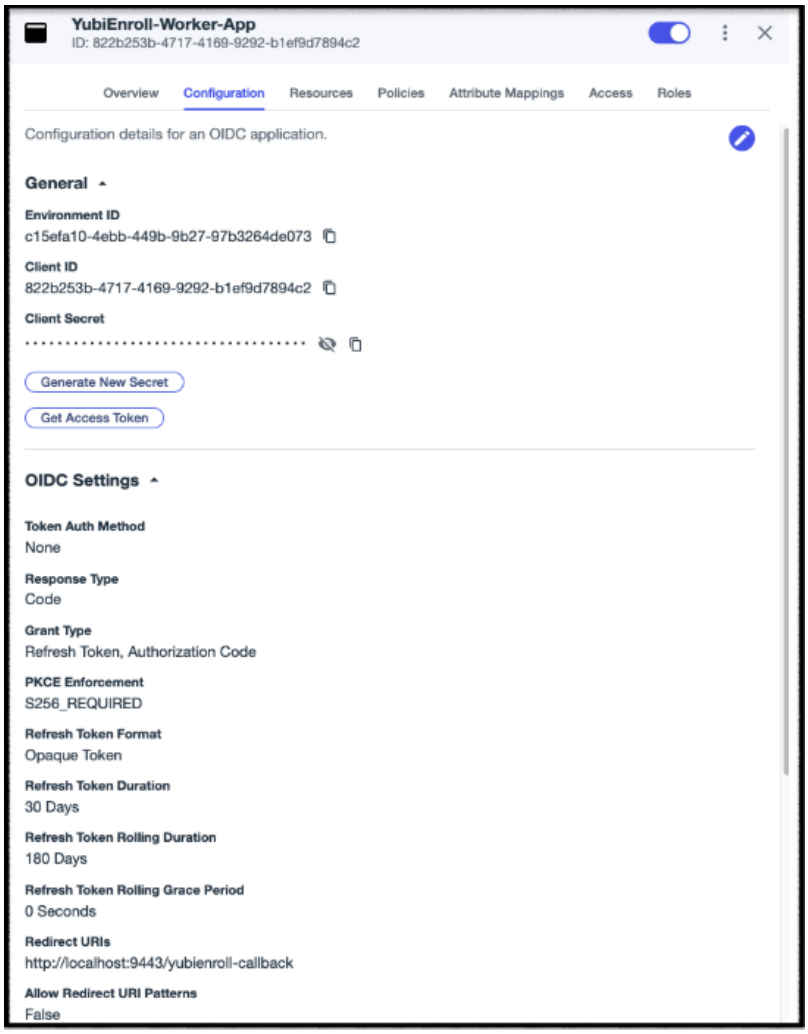
5.3.4 Preparing to Add the PingOne PingID Provider

When adding a provider configuration in YubiEnroll you need the following values from PingOne PingID. These were created in step *Registering the YubiEnroll App*.

1. From the PingOne PingID Console, select the YubiEnroll app you created. The example name is `YubiEnroll-Worker-App`.
2. Locate required values:

Item	Location
`Client ID`	General section
`Environment ID`	General section
`Redirect URI`	OIDC Settings section
`custom_domain`	optional value
`policy_id`	optional value

Most of the value are listed on the Configuration tab.



To add PingOne PingID in YubiEnroll, see *Adding Provider Configurations*.

5.3.5 Enabling MFA and FIDO2 Policies

To enable authentication with FIDO2 devices one must create a FIDO2 policy and include it in the relevant MFA policy. By default YubiEnroll uses the default MFA policy. It is possible to use non-default policy by specifying the `policy_id` when creating/editing the PingOne PingID provider. More info on FIDO2 policies can be found at Adding a FIDO policy.

5.3.6 Using Custom Domains

PingOne PingID supports the mapping of customer-owned and controlled domain names that are used to access user interfaces and services. By default YubiEnroll assumes no custom domains are used. It is possible to specify a custom domain by specifying the custom_domain when creating/editing the PingOne PingID provider. More info on custom domains can be found at Setting up a custom domain.

5.4 Configuring YubiEnroll with PingOne AIC

The following describes how to set up YubiEnroll in the PingOne Advanced Identity Cloud Application (AIC) tenants and configure the required user permissions.

5.4.1 Configuration Steps

The configuration steps involve the following:

1. *Registering the YubiEnroll App*
2. *Creating a WebAuthn Registration Journey*
3. *Configuring Permissions*
4. *Preparing to Add the PingOne AIC Provider*

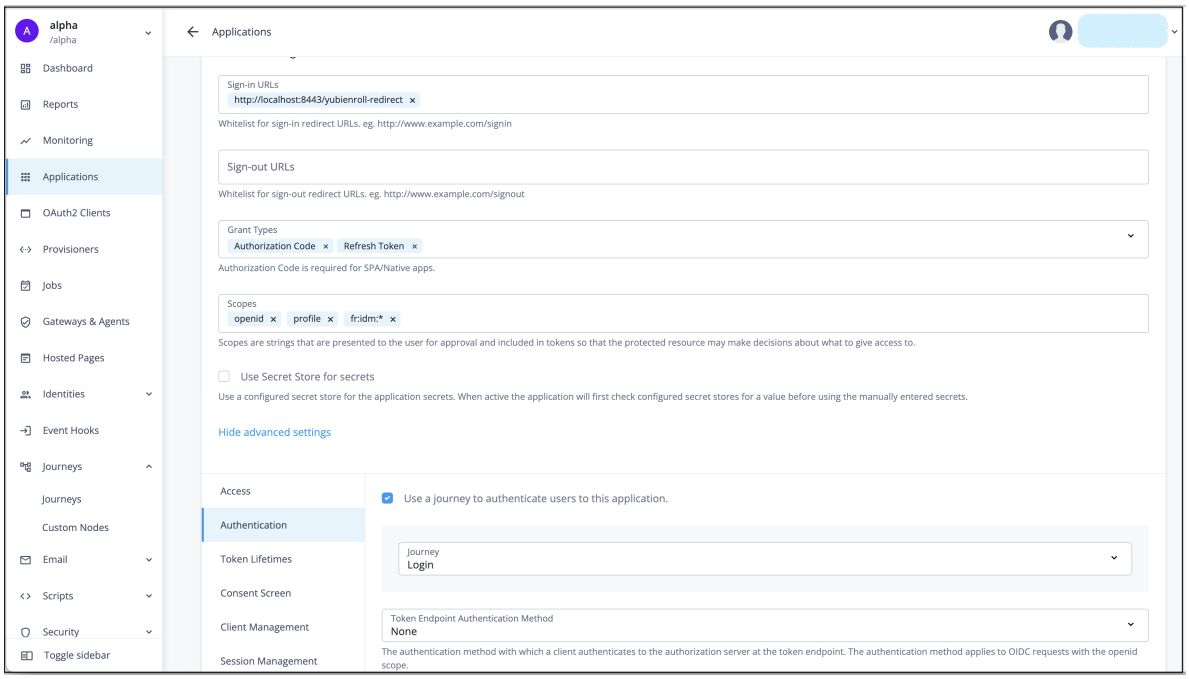
When you have successfully completed these steps, you are ready to *enroll YubiKeys on behalf of end users in your organization*.

5.4.2 Registering the YubiEnroll App

To use PingOne AIC in YubiEnroll you must first register an OAuth2 Client in your realm. Complete the steps:

1. Create a new application.
    a. Login to the PingOne AIC Admin Console.
    b. From the left panel, select **Applications**.
    c. Select **Custom applications** to add a new application.
    d. Select Sign-in Method, **OIDC - OpenID Connect**.
    e. Select Application Type, **Native/SPA**.
    f. Enter a Tenant Name and Owner for the app.
    g. Click **Next**.
2. Set the Applications > Sign-on tab configuration.
    a. For Sign-In URLs/Redirect URI.

       Specifying port seems to work best. For example, http://localhost:8443/yubienroll-redirect
    b. Select Grant Types, **Authorization Code** and **Refresh Token**.
    c. Select Scopes, **openid**, **profile**, and **fr:idm:***.
    d. Select **Show advanced settings**.
3. Set the Applications > Authentication tab configuration.
    a. Set Token Endpoint Authentication Method to **None**.
    b. Enable **Use a journey to authenticate users to this application.**. Select an appropriate authentication journey. For example **Login**.



4. Click **Save** to push the updates.

5.4.3 Creating a WebAuthn Registration Journey

To enable WebAuthn registration with PingOne AIC in YubiEnroll, you must first create a WebAuthn registration journey. While these journeys are highly customizable, YubiEnroll requires a specific configuration to ensure seamless API communication with the IDP.

Journeys in PingOne AIC are highly customizable. Since YubiEnroll does not provide such flexibility on API communication with the Identify Provider (IdP) we need to enforce some requirements.

Journey Structure

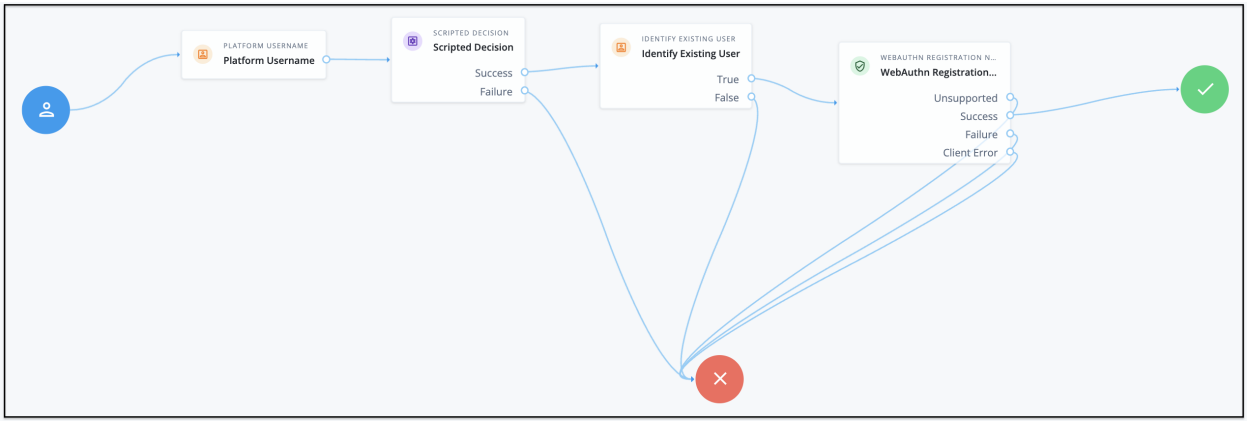
The journey must follow this structure:

```
Start → Username Collection → [Server-side nodes] → WebAuthn Registration Node →␣
↪Success
                                  ↓ (false)
                                Failure
```

For example:

```
Start → Page Node (Platform Username) → Identify Existing User → Scripted Decision␣
↪Node → WebAuthn Registration Node → Success
                                                                  ↓ (false)
                                                                Failure
```

The following image lists possible errors along the path to a successful journey.



Node 1 — Username collection

The first node in the journey must collect the username. You can use either a **Page Node** containing a **Platform Username** node, or a standalone **Username Collector** node.

YubiEnroll submits the `userName` of the target user into this node. You can then add server-side nodes such as **Identify Existing User**, additional **Scripted Decision Nodes**, or **Inner Tree Evaluator** nodes to process the user identity before reaching the WebAuthn Registration Node.

Node 2 — Scripted Decision Node (authorization)

YubiEnroll sends the operator's OAuth2 access token in the `Authorization` header on every call to the journey. We recommend adding a **Scripted Decision Node** to verify that the operator is authorized to register credentials on behalf of other users.

Configure the node with two outcomes: `Success` (continues to the WebAuthn Registration Node) and `Failure` (routes to a Failure Node).

The script needs to introspect the access token to identify the caller. This requires a separate OAuth2 client configured in PingOne AIC with the `am-introspect-all-tokens` scope. Store the client ID and client secret as ESV (Environment Secret & Variable) secrets so they are not hardcoded in the script.

The following ESVs are used in the example below:

ESV	Description
`esv.yubienroll.introspect.client.id`	Client ID of the OAuth2 client used for token introspection
`esv.yubienroll.introspect.client.secret`	Client secret of the OAuth2 client used for token introspection
`esv.yubienroll.tenant`	The tenant hostname. For example, `mycompany.forgeblocks.com`

Below is an example script that introspects the access token and checks whether the caller is a member of an authorized group. Adjust the group name and ESV keys to match your environment:

```
var NodeOutcome = {
   SUCCESS: "Success",
   FAILURE: "Failure"
};

// ESV references - adjust these to match your environment
var INTROSPECT_CLIENT_ID = "esv.yubienroll.introspect.client.id";
var INTROSPECT_CLIENT_SECRET = "esv.yubienroll.introspect.client.secret";
var TENANT = "esv.yubienroll.tenant";

// The group that authorized operators must be a member of
var AUTHORIZED_GROUP_CN = "cn=webauthn-admins,";

(function () {
   try {
      // 1. Extract the Bearer token from the Authorization header
      var authHeader = requestHeaders.get("Authorization");
      if (!authHeader || authHeader.isEmpty()) {
         logger.error("No Authorization header present");
         action.goTo(NodeOutcome.FAILURE);
         return;
      }
      var token = authHeader.get(0).replace("Bearer ", "");

      // 2. Introspect the token using the configured OAuth2 client
      var clientId = systemEnv.getProperty(INTROSPECT_CLIENT_ID);
      var clientSecret = systemEnv.getProperty(INTROSPECT_CLIENT_SECRET);
      var tenant = systemEnv.getProperty(TENANT);
      var introspectUrl = "https://" + tenant + "/am/oauth2/realms/root/realms/
↪alpha/introspect";

      var response = httpClient.send(introspectUrl, {
         method: "POST",
         form: {
            token: token,
            client_id: clientId,
            client_secret: clientSecret
         }
      }).get();

      var result = response.json();

      // 3. Verify the token is active
      if (String(result.active) !== "true") {
         logger.error("Access token is not active");
         action.goTo(NodeOutcome.FAILURE);
         return;
      }
```

(continues on next page)

(continued from previous page)

```
    // 4. Resolve the caller's identity
    var callerUsername = result.username;
    if (!callerUsername) {
       logger.error("No username in introspection response");
       action.goTo(NodeOutcome.FAILURE);
       return;
    }

    var identity = idRepository.getIdentity(callerUsername);
    if (!identity.exists()) {
       logger.error("Identity not found for " + callerUsername);
       action.goTo(NodeOutcome.FAILURE);
       return;
    }

    // 5. Check group membership
    var memberOf = identity.getAttributeValues("isMemberOf");
    var authorized = false;
    for (var i = 0; i < memberOf.length; i++) {
       if (String(memberOf[i]).startsWith(AUTHORIZED_GROUP_CN)) {
          authorized = true;
          break;
       }
    }

    if (authorized) {
       logger.info("Authorized: " + callerUsername);
       action.goTo(NodeOutcome.SUCCESS);
    } else {
       logger.error("Not authorized: " + callerUsername);
       action.goTo(NodeOutcome.FAILURE);
    }

  } catch (e) {
    logger.error("Authorization check error: " + e);
    action.goTo(NodeOutcome.FAILURE);
  }
}());
```

Node 3 — WebAuthn Registration Node

Add a **WebAuthn Registration Node** after the server-side nodes. Configure it with the appropriate relying party ID and attestation settings for your environment. YubiEnroll receives the registration challenge from this node, create the credential on the YubiKey, and submit the attestation result back.

Terminal nodes

Connect the WebAuthn Registration Node to a **Success Node**. Connect the `false` outcome of the Scripted Decision Node to a **Failure Node**.

Important notes

- Do not add nodes that produce callbacks (interactive nodes) between the username collection and the WebAuthn Registration Node. Server-side nodes such as additional Scripted Decision Nodes or Inner Tree Evaluator nodes are fine, as they execute without prompting the client. YubiEnroll expects exactly one username prompt followed by the WebAuthn registration challenge — any additional prompts cause the registration to fail.
- The journey must be in the realm configured in YubiEnroll (the `realm` parameter in the provider configuration).

5.4.4 Configuring Permissions

To enroll YubiKeys on behalf of an end user, the YubiEnroll app user, for example an IT admin, must have the PingOne Ping AIC role: `openidm-admin` and have the correct permissions as defined by the WebAuthn Registration Journey (e.g. be a member of an authorized group).

5.4.5 Preparing to Add the PingOne AIC Provider

When adding a provider configuration in YubiEnroll you need the following values from PingOne AIC. These were created in steps *Registering the YubiEnroll App* and *Creating a WebAuthn Registration Journey*.

The table lists where the values can be found.

Item	Location
`Client ID`	The OAuth2 client you created
`Redirect URI`	The OAuth2 client you created
`tenant`	This is PingOne AIC tenant name. Find it on the PingOne AIC Tenant Settings.
`realm`	This is the PingOne AIC realm where the client was registered.
`journey`	This is the PingOne AIC WebAuthn registration name. Copy the name from journey you created.

To add PingOne AIC in YubiEnroll, see *Adding Provider Configurations*.

CHAPTER

SIX

YUBIENROLL COMMANDS

The following describes commands available when using the YubiEnroll CLI, together with usage examples. For more examples of how to add providers and enrollment profiles and enroll end users, see *Using YubiEnroll CLI*.

6.1 yubienroll

`yubienroll [OPTIONS] COMMAND [ARGS]...`

Run `yubienroll` at the command prompt to see available options and commands.

Options

Option	Description
`-l, - -log-level [ERROR|WARNING|INFO|DEBUG|]`	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

Command	Description
`credentials`	Manage FIDO credentials for users.
`login`	Authenticate to the active provider.
`logout`	Log out 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.

6.2 yubienroll credentials

`yubienroll credentials [OPTIONS] COMMAND [ARGS]...`

Lets users enroll, list and delete credentials on behalf of an end user. Subcommands require a `User_ID`, which can be the ID or username for an end user. Use the `yubienroll users [query]` command to get these values, see *yubienroll users*.

Options

Option	Description
`-h, --help`	Show this message and exit.

Commands

Command	Description
`add`	Enroll a FIDO credential on behalf of an end user.
`delete`	Delete FIDO credential(s) for an end user.
`list`	List FIDO credentials for an end user.

6.2.1 yubienroll credentials add

`yubienroll credentials add [OPTIONS] USER_ID`

Add credentials on behalf of an end user enrolling them with the identity provider. `User_ID` is the ID or username for an end user. Use the `yubienroll users [query]` command to get these values, see *yubienroll users*.

The `yubienroll credentials add` command creates a FIDO credential on the YubiKey and registers it with the identity provider for the specified user.

You can configure YubiKey settings, for example minimum PIN length or force PIN change on first use, either through the CLI options or by using an enrollment profile. This can be specified with the `--profile` option or automatically applied if assigned to the active provider.

If not specified, the enrollment profile associated with the active identity provider is applied. If no authenticator settings or enrollment profile exist, you are prompted to provide them.

Examples

- Add credentials and enroll end user with `user_ID` `firstname.lastname\@email.com`.

  ```
  > yubienroll credentials add firstname.lastname@mail.com
  ```

- Apply a different (configured) enrollment profile named `another-profile` than the one used by the active provider.

  ```
  > yubienroll credentials add firstname.lastname@email.com --profile another-profile
  ```

Options

Option	Description
`-r, --reader NAME`	Enroll a FIDO credential on behalf of a user.
`-p, --profile TEXT`	Set the enrollment profile to use.
`-d, --display-name TEXT`	Display name to set for the Security Key.
`--min-pin-length INTEGER RANGE`	Set the minimum length allowed for PIN [4<=x<=63].
`--require-always-uv`	Always require UV.
`--no-require-always-uv`	Do not always require UV.
`--require-ea`	Require Enterprise Attestation.
`--no-require-ea`	Do not require Enterprise Attestation.
`--force-pin-change`	Force PIN change before use.
`--no-force-pin-change`	Do not force PIN change before use.
`--reset`	Factory reset and re-initialize key.
`--no-reset`	Do not factory reset and re-initialize key.
`--random-pin`	Set a new random PIN.
`--no-random-pin`	Do not set a new random PIN.
`--random-pin-length INTEGER RANGE`	Set the random PIN length [4<=x<=63].
`-f, --force`	Confirm settings without prompting.
`-h, --help`	Show this message and exit.

6.2.2 yubienroll credentials delete

`yubienroll credentials delete [OPTIONS] USER_ID [CREDENTIAL_IDS]...`

Delete one or more credentials for an end user available in the identity provider. If no credential IDs are provided, all credentials for the end user are listed and you are prompted to select the desired ones to delete.

Examples

- Delete credentials in the identity provider for the end user with `user_ID` `4321` and `credential_ID` `123XYZ`.

  ```
  > yubienroll credentials delete 4321 123XYZ
  ```

- Delete *multiple* credentials for a user by passing a space-separated list of credentials. For example, a user with user ID `X` has two credentials with ID `Y` and `Z`, and you want to delete both in one go.

  ```
  > yubienroll credentials delete X Y Z
  ```

Options

Option	Description
`-f, --force`	Confirm deletion without prompting.
`-h, --help`	Show this message and exit.

6.2.3 yubienroll credentials list

`yubienroll credentials list [OPTIONS] USER_ID`

List active credentials registered for an end user available in the identity provider.

Examples

- List available credentials for end user with `user_ID` `firstname.lastname\@email.com`.

  `> yubienroll credentials list firstname.lastname@email.com`

6.3 yubienroll login

`yubienroll login [OPTIONS]`

Authenticate to the active provider. Starts a web-based authentication flow to get access credentials for the user account.

Examples

- Show supported identity providers to select and log in to the desired one.

  `> yubienroll login`

- Use `--no-launch-browser` if you do not want the command to launch the default system browser. This prints the authorization URL in the terminal so you can manually open the URL in a desired browser.

  `> yubienroll login --no-launch-browser`

Options

Option	Description
`--no-launch-browser`	Do not open browser automatically.
`-h, --help`	Show this message and exit.

Commands

Command	Description
`login`	Authenticate with an identity provider.

6.4 yubienroll logout

`yubienroll logout [OPTIONS]`

Log out the YubiEnroll user from the active identity provider.

Note: This command is currently only supported for the Okta identity provider.

Options

Option	Description
`-h, --help`	Show this message and exit.

Commands

Command	Description
`logout`	Log out from the active provider.

6.5 yubienroll profiles

`yubienroll profiles [OPTIONS] COMMAND [ARGS]...`

Manage enrollment profiles for an identity provider. Profiles are presets of configuration parameters used when enrolling credentials. You can for example enforce minimum PIN length or force PIN change prior to use. You can edit profile settings or delete the profile from the provider configuration. Deleting an enrollment profile removes it from any provider using it.

Examples

- Add an enrollment profile with the name `standard` to the (active) provider.

  `> yubienroll profiles add standard`

- Show enrollment profiles available for the provider.

  `> yubienroll profiles list`

- To unset a profile from a provider, run the following command and select `0`.

  `> yubienroll profiles edit <provider_name>`

Options

Option	Description
`-h, --help`	Show this message and exit.

Commands

Command	Description
`add`	Create a new profile.
`delete`	Delete a profile.
`edit`	Modify an existing profile.
`list`	List profiles.

6.5.1 yubienroll profiles add

`yubienroll profiles add [OPTIONS] NAME`

Creates a new profile where `NAME` is the name of the new profile.

Options

Option	Description
`--min-pin-length INTEGER RANGE`	Set the minimum length allowed for PIN [4<=x<=63].
`--require-always-uv`	Require always UV.
`--no-require-always-uv`	Do not require always UV.
`--require-ea`	Require Enterprise Attestation.
`--no-require-ea`	Do not require Enterprise Attestation.
`--force-pin-change`	Force PIN change before use.
`--no-force-pin-change`	Do not force PIN change before use.
`--reset`	Factory reset and re-initialize key.
`--no-reset`	Do not factory reset and re-initialize key.
`--random-pin`	Set a new random PIN.
`--no-random-pin`	Do not set a new random PIN.
`--random-pin-length INTEGER RANGE`	Set the random PIN length [4<=x<=63].
`-h, --help`	Show this message and exit.

6.5.2 yubienroll profiles delete

`yubienroll profiles delete [OPTIONS] NAME`

Deletes an existing profile with the name `NAME`.

Options

Option	Description
`-f, --force`	Confirm deletion without prompting.
`-h, --help`	Show this message and exit.

6.5.3 yubienroll profiles edit

`yubienroll profiles edit [OPTIONS] NAME`

Modifies an existing profile with the name `NAME`.

Options

Option	Description
`--min-pin-length INTEGER RANGE`	Set the minimum length allowed for PIN [4<=x<=63].
`--require-always-uv`	Require always UV.
`--no-require-always-uv`	Do not require always UV.
`--require-ea`	Require Enterprise Attestation.
`--no-require-ea`	Do not require Enterprise Attestation.
`--force-pin-change`	Force PIN change before use.
`--no-force-pin-change`	Do not force PIN change before use.
`--reset`	Factory reset and re-initialize key.
`--no-reset`	Do not factory reset and re-initialize key.
`--random-pin`	Set a new random PIN.
`--no-random-pin`	Do not set a new random PIN.
`--random-pin-length INTEGER RANGE`	Set the random PIN length [4<=x<=63].
`-h, --help`	Show this message and exit.

6.5.4 yubienroll profiles list

`yubienroll profiles list [OPTIONS]`

Shows enrollment profiles available for the provider.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.6 yubienroll providers

`yubienroll providers [OPTIONS] COMMAND [ARGS]...`

Manage authentication configurations stored in named provider objects for identity providers. You can add, activate, or delete authentication configurations. The active provider is the provider and tenant with which YubiEnroll communicates. Only one provider at the time can be active.

Note: If there are no existing provider configurations and you add one, YubiEnroll automatically activates it. To explicitly activate a provider, use `yubienroll providers activate`. An active provider configuration can be deleted.

Examples

- Add a provider configuration with the name `entra`.

  `> yubienroll providers add entra`

- Show the configuration for the provider with the name `entra`.

  `> yubienroll providers show entra`

- Delete the provider configuration named `entra` without prompting.

  `> yubienroll providers delete --force entra`

Options

Option	Description
`-h, --help`	Show this message and exit.

Commands

Command	Description
`activate`	Select which provider to use for other commands.
`add`	Create a new provider configuration.
`delete`	Delete a provider configuration.
`edit`	Modify an existing provider configuration.
`list`	List all provider configurations.
`show`	Show the full configuration for a provider.

6.6.1 yubienroll providers activate

`yubienroll providers activate [OPTIONS] NAME`

Activates an existing provider configuration with the name `NAME` to be used for other provider commands.

6.6.2 yubienroll providers add

`yubienroll providers add [OPTIONS] NAME`

Creates a new provider configuration with the name `NAME`. This command lets you define authentication settings for an identity provider. Settings include `CLIENT_ID`, `REDIRECT_URI`, and other OAuth2-specific configurations.

Note: The command requires an OAuth app to be registered with your identity provider.

Options

Option	Description
`-p, -- provider [ENTRA|OKTA|PING_ONE|PING_ONE_AIC]`	The identity provider to choose.
`-a, -- activate`	Activate configuration.
`-h, --help`	Show this message and exit.

6.6.3 yubienroll providers delete

`yubienroll providers delete [OPTIONS] NAME`

Deletes a provider with the name `NAME`.

Options

Option	Description
`-f, --force`	Confirm deletion without prompting.
`-h, --help`	Show this message and exit.

6.6.4 yubienroll providers edit

`yubienroll providers edit [OPTIONS] NAME`

Modifies the configuration of an existing provider with the name `NAME`. The command lets you step through the various configuration settings for a provider, for example to change the `client_id`.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.6.5 yubienroll providers list

`yubienroll providers list [OPTIONS]`

Lists all configured providers, for example to see which one is active. To get configuration details for a *specific* provider, use `yubienroll providers show`.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.6.6 yubienroll providers show

`yubienroll providers show [OPTIONS] NAME`

Shows the full configuration of a provider with the name `NAME`. Configurations include `client_id`, `redirect_uri`, `tenant_id`, and the status of the provider.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.7 yubienroll readers

`yubienroll readers [OPTIONS]`

Lists available smart card readers.

You can use a smart card reader to enroll a YubiKey over NFC. Use the `--reader` option in the `yubienroll credentials add` command to specify the name of the reader you want to use. Use the `yubienroll readers` command to find the name of the reader you want to use.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.8 yubienroll status

`yubienroll status [OPTIONS]`

Shows the name of the active provider configuration (used by default when enrolling end users), the identity provider used, and whether the user is authenticated with the provider or not.

Options

Option	Description
`-h, --help`	Show this message and exit.

6.9 yubienroll users

`yubienroll users [OPTIONS] [QUERY]`

When enrolling an end user, you need the user identifiers `ID` and `Username`. To get these values you can search for users in the identity provider using the `yubienroll users <query>` command where `query` is a substring match of display name, username, or email.

`query` can be for example the display name (firstname + lastname), username, or primary email address. The returned search results include the **ID**, **Display Name**, **Username**, and **Email** for each user.

Note: When performing enrollment operations on behalf of a user, you can *only use the username or user ID value*. Using the email address does not work.

Examples

- Search for an end user with the name `firstname lastname` in the identity provider. If no query is specified, all users are returned.

  ```
  > yubienroll users firstname lastname
  ```

Options

Option	Description
`-h, --help`	Show this message and exit.

Commands

Command	Description
`users`	Search for users.

CHAPTER

SEVEN

RELEASE NOTES

The following lists new features, resolved issues, and known limitations for new versions of YubiEnroll.

7.1 2026

7.1.1 Release 1.2.0 (15 May)

New Features & Enhancements

- Support for identity provider, PingOne PingID. For more information see *Configuring YubiEnroll with PingOne PingID*.
- Support for identity provider, PingOne Advanced Identity Cloud (AIC). For more information see *Configuring YubiEnroll with PingOne AIC*.

7.1.2 Release 1.1.2 (15 April)

Maintenance Update

- Updated dependencies for stability and compatibility improvements.

7.2 2025

7.2.1 Release 1.1.1 (9 July)

Resolved Issues

- **Reauthenticate if corrupt** `tokens.json`**:** YubiEnroll stores encrypted API tokens to maintain the login state. If the encryption key changes or the file gets corrupted, the tool can no longer access the contents. This version introduces improved error handling for these scenarios, and the YubiEnroll CLI now prompts for re-authentication in case of a non-decryptable `tokens.json` file.
- **NFC error with some readers:** Enrolling a YubiKey over NFC on Windows could occasionally fail during the initial connection phase over NFC, especially if the key has not already been placed on the reader when the enrollment began. This version improves the NFC handling for greater reliability and robustness.

7.2.2 Release 1.1.0 (23 April)

New Features & Enhancements

- Enhanced language and messaging for improved clarity and usability.
- Added support for listing available NFC readers for YubiKey/Security Key connections.
- Added new enrollment profile option to set random PIN length independently of minimum PIN length, enabling configuration on pre-5.7 keys.
- Introduced a new `--force` flag that can be used with `yubienroll credentials add`, `yubienroll credentials delete`, `yubienroll profiles delete` and `yubienroll providers delete` commands to enhance scripting support for YubiEnroll.
- Enhanced search for Okta providers to include `username`, `firstName`, `lastName`, and `email`; added `email` field to the `users` command output. For more information, see *Searching for Users*.
- The provider `show` command now indicates whether a provider is currently active.
- Base URLs for MS Entra ID and Graph are now optionally configurable to support scenarios like government tenants. For more information, see *Preparing to Add the Entra ID Provider*.
- Added a new option to require Enterprise Attestation.

Resolved Issues

- Resolved an issue causing an error when attempting to delete a profile with no providers configured.

7.3 2024

7.3.1 Release 1.0.0 (18 December)

First release of YubiEnroll.

Features Included

- Command line tool (CLI) for Windows.
- Enabling of enrollment of FIDO credential on behalf of an end user.
- Support for all YubiKey and Security Key form factors.
- Setting and managing of PINs.
- Configuration options include forced PIN changes, minimum PIN length, and user verification.
- Factory reset of YubiKeys and Security Keys.
- Support for connecting via NFC or USB.
- Support for identity providers Okta and Microsoft Entra ID.

CHAPTER

EIGHT

COPYRIGHT

© 2021-2026 Yubico AB. All rights reserved.

8.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

8.2 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

8.3 Contact Information

Yubico AB
Gävlegatan 22
113 30 Stockholm
Sweden

8.4 Getting Help

Documentation is continuously updated on https://docs.yubico.com/ (this site). Additional support resources are available in the Yubico Knowledge Base.

Click the links to:

- Submit a support request
- Contact our sales team

8.5 Feedback

Yubico values and welcomes your feedback. If you think you may have discovered a flaw in our product, please submit a support request at https://support.yubico.com/s/ and provide as much detail as you can.

8.6 Document Updated

2026-05-22 21:55:11 UTC