YubiEnroll User Guide

Yubico

Apr 23, 2025

CONTENTS

CHAPTER

ONE

INTRODUCTION

Note: YubiEnroll is currently in *Early Access*. For more information, see YubiEnroll.

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 and Microsoft Entra ID). 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” will work with Okta or Microsoft Entra ID. However, other websites supporting WebAuthn that do not request user verification, might block the user from logging in.

1.2 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” are only supported for YubiKeys with firmware version 5.5 and higher.

CHAPTER

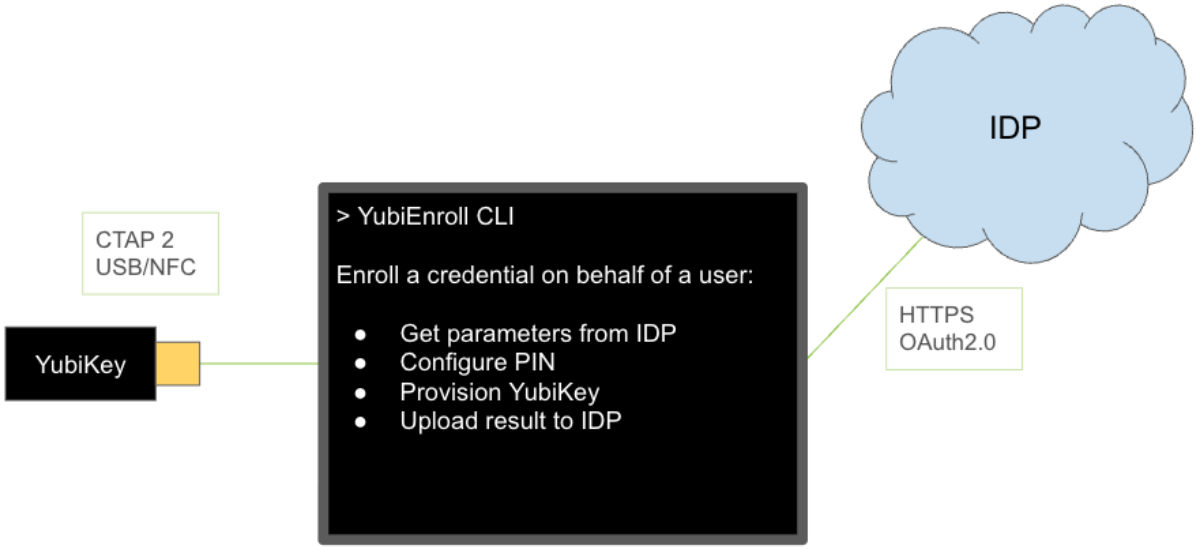
TWO

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" are only supported for 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]: y
Set a new random PIN? [Y/n]: y
Random PIN length [6]: 6
Assign this profile to the active provider (entra)? [y/N]: n
Added profile 'entra-reset'
PS C:\program files\yubico>
```

The following explains the enrollment profile settings in more detail.

1. **Minimum PIN length:** This setting defines the minimum number of characters required for the PIN used with the YubiKey. If not specifically set, the default value is 4. The minimum PIN length can never be lower than 4.
2. **Require always UV:** The "Always require user verification" setting enforces PIN request in all cases regardless of whether the relying party requests it or not. If set to "on", user verification will always be performed. If set to "off" (default) user verification is overridden.
3. **Require Enterprise Attestation? [y/N]**: Configure if enterprise attestation should be required. Default is "no".

4. **Force PIN change before use:** If set to “on”, this setting forces the end user to change the provided PIN when using the YubiKey the first time. Default is “off”.
5. **Factory reset the Security Key:** If set to “true” all credentials on the YubiKey will be removed and the key is completely cleared from previous configurations. This setting is mostly used for keys that have previously been in use. Default is “false”.
6. **Set a new random PIN:** If set to “true”, YubiEnroll generates a random PIN. If set to “false”, the user can specify as specific PIN.
7. **Random PIN length [4]**: Configure the length of the random PIN to be set, if this option was selected.

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 for Okta*
- *Configuring YubiEnroll for Microsoft Entra ID*

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 both the providers, and its profile settings are displayed at the end of the file.

yubienroll.toml

```
active_provider = "entra"

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

[providers.okta]
provider = "OKTA"
```

(continues on next page)

(continued from previous page)

```
client_id = "0oahi..."
redirect_uri = "http://localhost:8080/yubienroll-callback"
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 will 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's default browser which is automatically launched by YubiEnroll during the login procedure. This includes entering the user's 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's API. The access token lets YubiEnroll interact with the identity provider's 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 (Okta or Microsoft Entra ID).

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 themself as a self-service.
- **Auditor:** An employee of the organization or an external contractor responsible for inspection of logs for audit purposes. Will only have read access to the logs.

CHAPTER

THREE

INSTALLING YUBIENROLL CLI

Yubienroll is currently available for identity providers Okta and Microsoft Entra ID.

3.1 Prerequisites

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

- Windows 11 with administrator privileges.
- Okta Identity Engine (OIE) and/or Microsoft Entra ID.
- 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 examples of how to work 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 will require administrator privileges. To avoid running the YubiEnroll CLI tool as administrator, the tool itself will prompt 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

Open a terminal, for example Windows PowerShell, navigate to the installation path (default is `C:\Program Files\Yubico\YubiEnroll\`) and run `yubienroll.exe` to see the usage, options, and commands that may be used. Then run the YubiEnroll commands from the command prompt.

4.2 Adding Provider Configurations

The following describes how to add an identity provider configuration and an enrollment profile. The example uses identity provider Microsoft Entra ID, but the procedure is similar for Okta. In this example we assume you log in to YubiEnroll for the first time, and no providers or enrollment profiles exist. However, you can add providers and enrollment profiles at any time.

Note: When adding a provider configuration, you will need to provide identity provider-specific input 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 (Okta or Microsoft Entra ID). If no provider configuration exists and you choose to add one, this will automatically be activated and will be the default provider used when enrolling end users.

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

To add a provider configuration and an enrollment profile, do the following:

1. In the terminal, run `yubienroll providers add entra` where "entra" is the provider name in this example (you can choose a name of your choice).
2. Select the desired provider type, "ENTRA" (1) in this example.
3. Enter the **Client ID**, **Redirect URI**, and **Microsoft Entra Tenant ID** when prompted. For provider-specific input values, see *Identity Provider Configuration*.
4. For Microsoft **Entra ID endpoint** and **Microsoft Graph** endpoint, you can use default values in most cases. If your organization is working with government tenants, you might need to change the endpoints. For more information, see *Adding the Entra ID Provider*.
5. When prompted to specify if you want to add a new enrollment profile [y/N], enter "y".
6. Enter the following when prompted:
    a. **Profile name [default]** - the name to be used for the profile. In this example, the profile is named "entra-main". 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 applied. Default is "no".
    e. **Force PIN change before use? [y/N]** - define if the end user must change the PIN when using the YubiKey for the first time. Default is "no".
    f. **Factory reset the Security Key? [Y/n]** - enter "n" if you will be enrolling a new key. Enter "y" if you will be enrolling a key that has previously been in use. This option will clear the key completely from previous configurations.
    g. **Set a new random PIN [Y/n]** - enter "y" if you want YubiEnroll to set a new PIN for the key. Enter "n" if you want to specify a specific PIN.
    h. **Random PIN length [4]** - define the length of the random PIN to be set, if this option was selected.
7. The provider configuration is added together with the enrollment profile. Because no provider existed previously, the "entra" provider is automatically activated.

```
PS C:\program files\yubico> yubienroll providers add entra
Supported identity providers:
[1] ENTRA
[2] OKTA
Select provider: 1
Enter the Client ID: c64e5ed2…
Enter the Redirect URI: http://localhost/yubienroll-redirect
Enter the Microsoft Entra Tenant ID: 220b415…
Enter the Microsoft Entra ID endpoint [https://login.microsoftonline.com]:
Enter the Microsoft Graph endpoint [https://graph.microsoft.com]:
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'
Added provider 'entra'.
Activated provider.
PS C:\program files\yubico>
```

8. To check provider and authentication status and see available enrollment profiles you can run `yubienroll status` and `yubienroll profiles list`.

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

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

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 choose a name of your choice).
2. Enter the following when prompted:
    a. **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.

b. **Require always UV? [y/N]** - define if the "Always require user verification setting" should always be overridden. Default is "no".

c. **Require Enterprise Attestation? [y/N]** - define if enterprise attestation should be required. Default is "no".

d. **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".

e. **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.

f. **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.

g. **Random PIN length [6]** - define the length of the random PIN to be set, if this option was selected.

h. **Assign this profile to the active provider (entra)? [y/N]** - enter "y" to replace the enrollment profile that is currently assigned to the active provider with the one you are creating. Enter "n" to keep the current enrollment profile for the active provider.

3. The new enrollment profile is stored.

```
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]: y
Set a new random PIN? [Y/n]: y
Random PIN length [6]: 6
Assign this profile to the active provider (entra)? [y/N]: n
Added profile 'entra-reset'
PS C:\program files\yubico>
```

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

4.4 Enrolling End Users

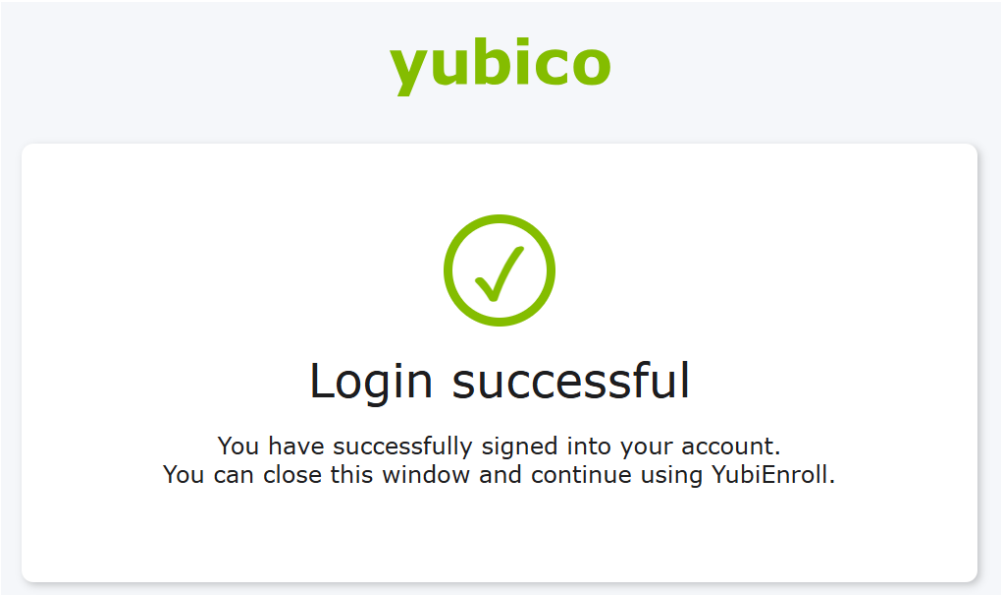
The following describes how to enroll a YubiKey adding credentials on behalf of a specific end user. Ensure you have the YubiKey you want to enroll available, as well as the "ID" or "Username" of the end user. For information on how to find an end user identifier, see the command *yubienroll users*.

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.

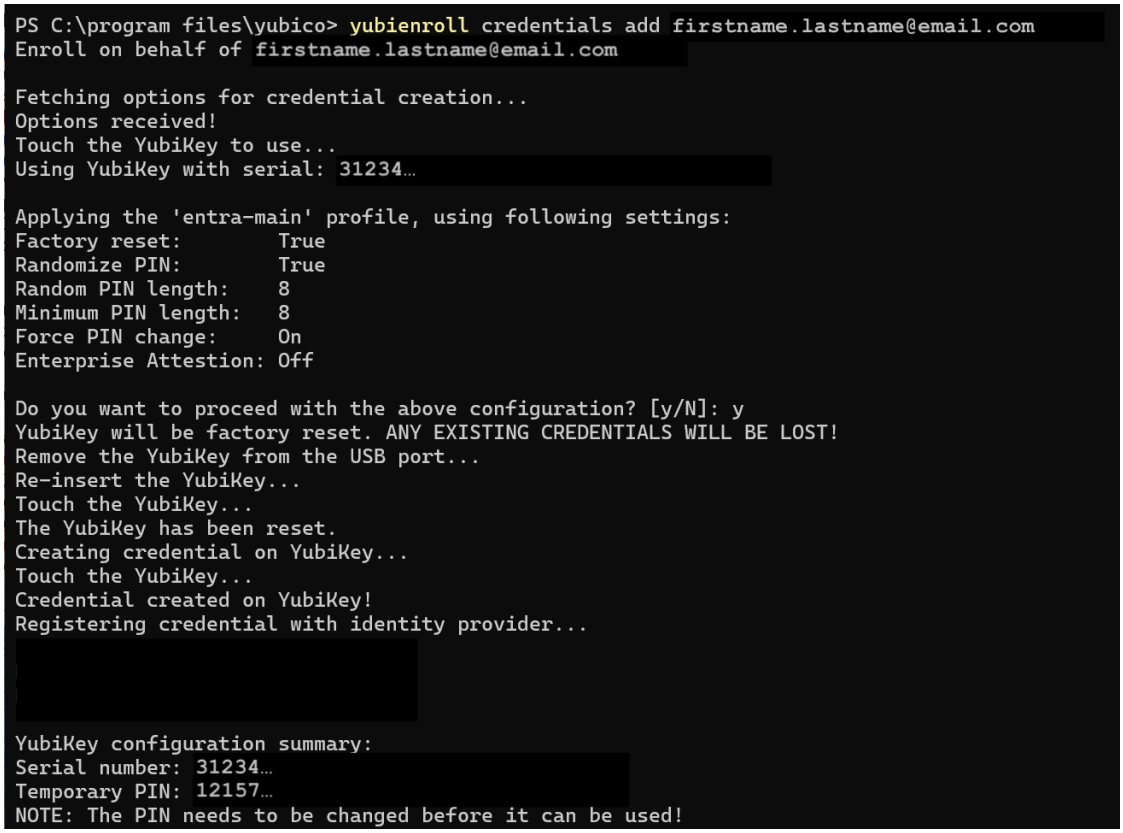
To enroll a YubiKey on behalf of an end user, do the following:

1. In the terminal, run `yubienroll login` to authenticate with the identity provider.
2. Select the desired provider, "ENTRA" (1) 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*.

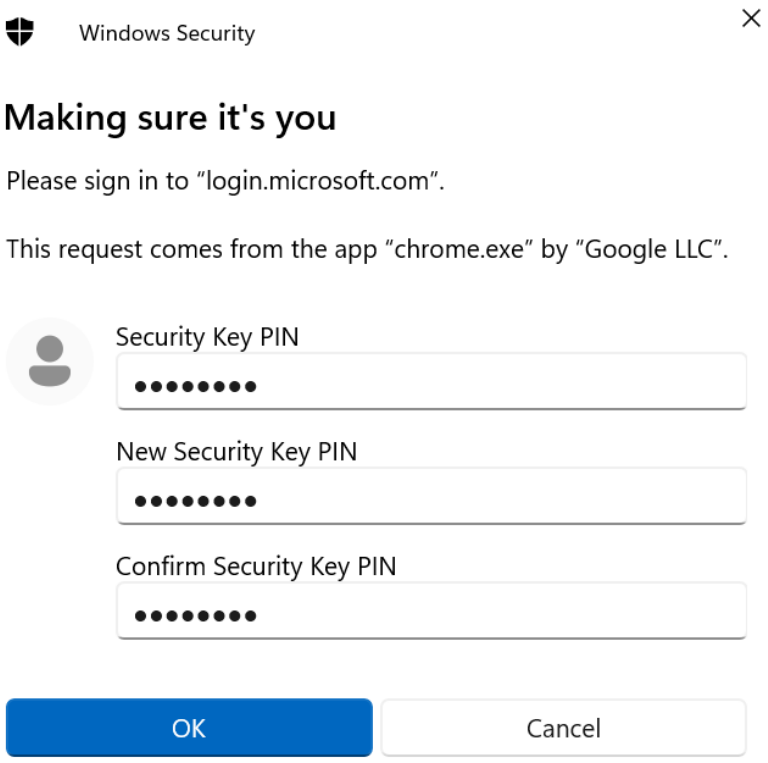
4. Follow the steps to complete the authentication. When successfully authenticated, return to the terminal.



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.



11. Provide the YubiKey and the temporary PIN to the end user.
12. To authenticate with identity provider (Microsoft Entra ID in this example), 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.



For more information about the `yubienroll credentials` command, see *yubienroll credentials*.

CHAPTER

FIVE

YUBIENROLL WITH OKTA

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

5.1 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 Registering the YubiEnroll App

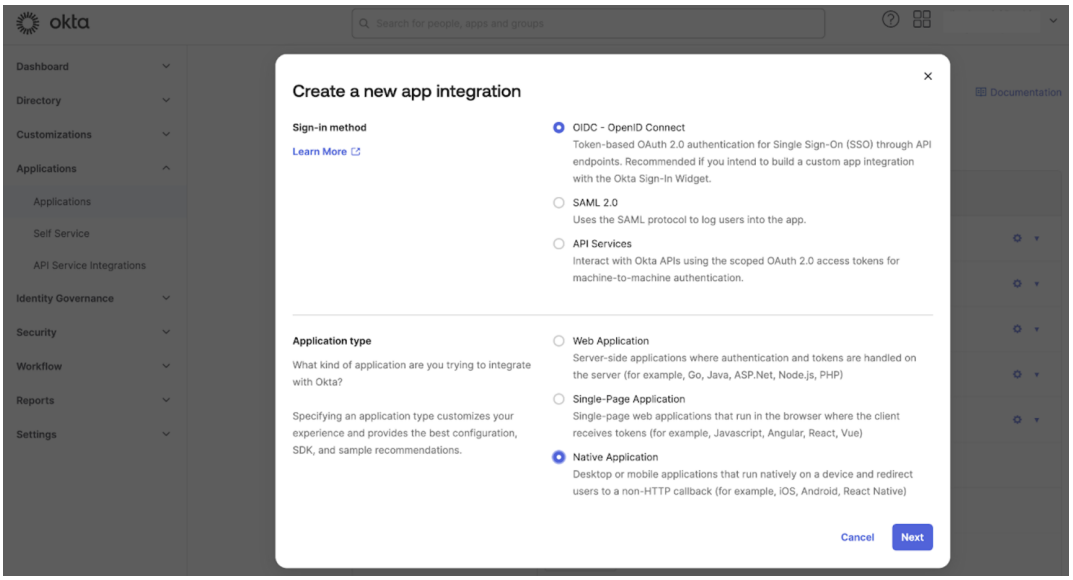
Note: To register the YubiEnroll app in the Okta tenant as described in the following, you will need *Super Admin* or *Application Admin* permissions. For more information, see *Configuring Permissions*.

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

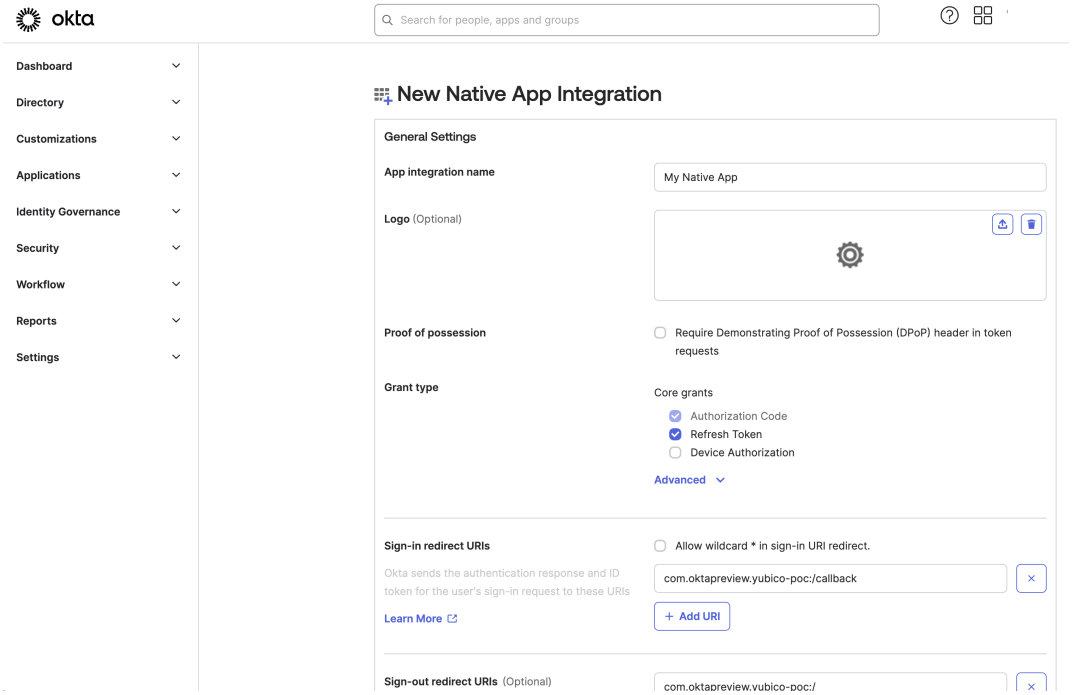
- `client_id`
- `domain`
- `redirect_uri`

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 will issue a refresh token once it expires.



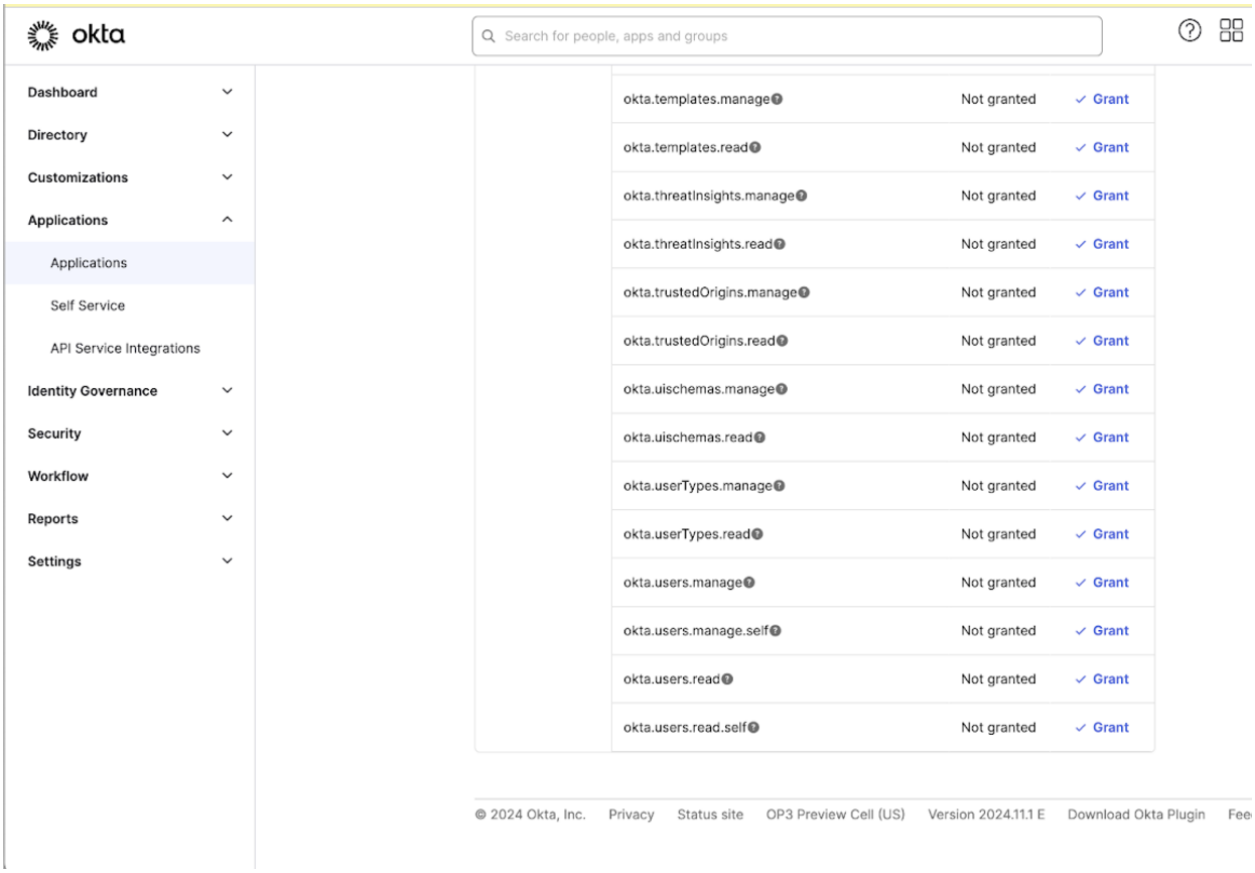
For more details on how to register the YubiEnroll app, see Create an OAuth 2.0 app in Okta (Okta documentation).

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

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

5.3 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.

5.4 Adding 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 will 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 will be displayed under the email address.

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

5.5 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 will 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 will result 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).

5.6 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 will 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** values. Using the email address will not work. For search examples, see *YubiEnroll Commands*.

CHAPTER

SIX

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.

6.1 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*.

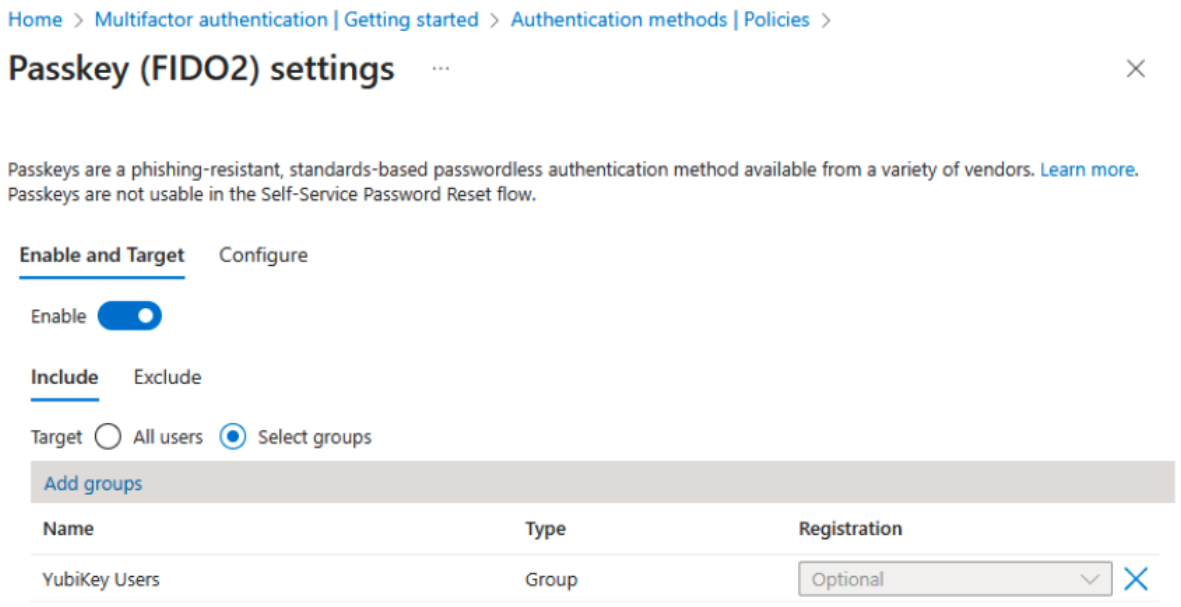
When you have successfully completed these steps, you are ready to *enroll YubiKeys on behalf of end users in your organization*.

6.2 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).



6.3 Registering the YubiEnroll App

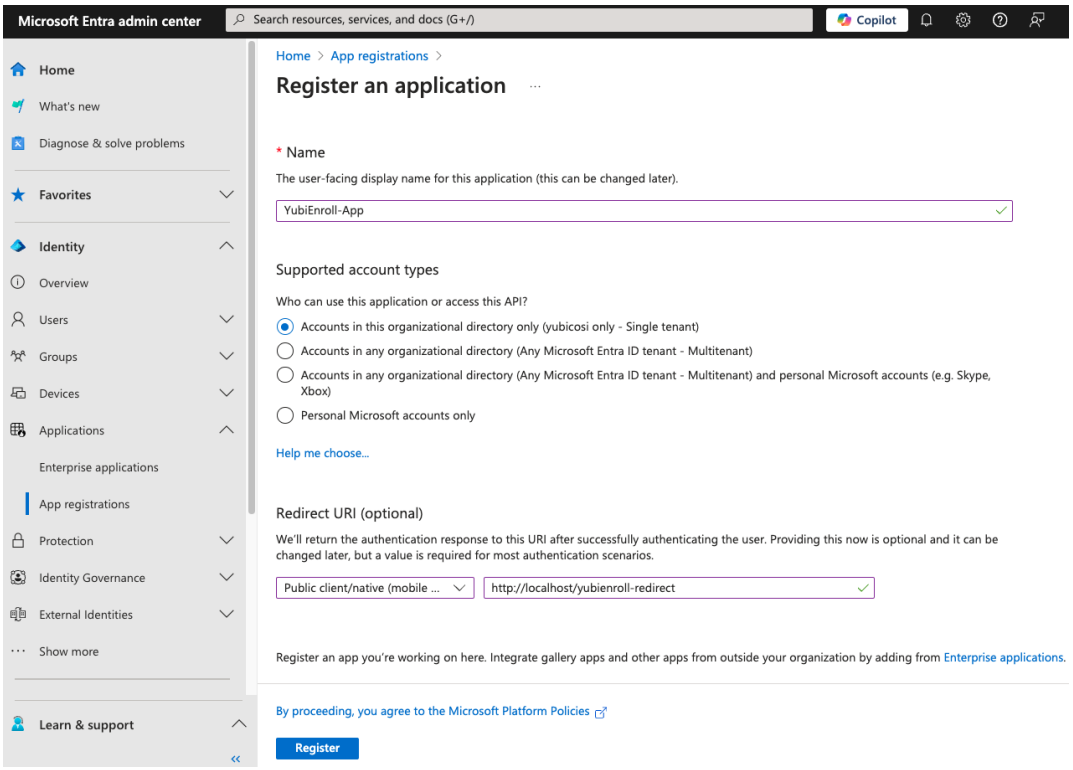
When configuring the Microsoft Entra ID provider in YubiEnroll, the following parameter values are needed:

- `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.



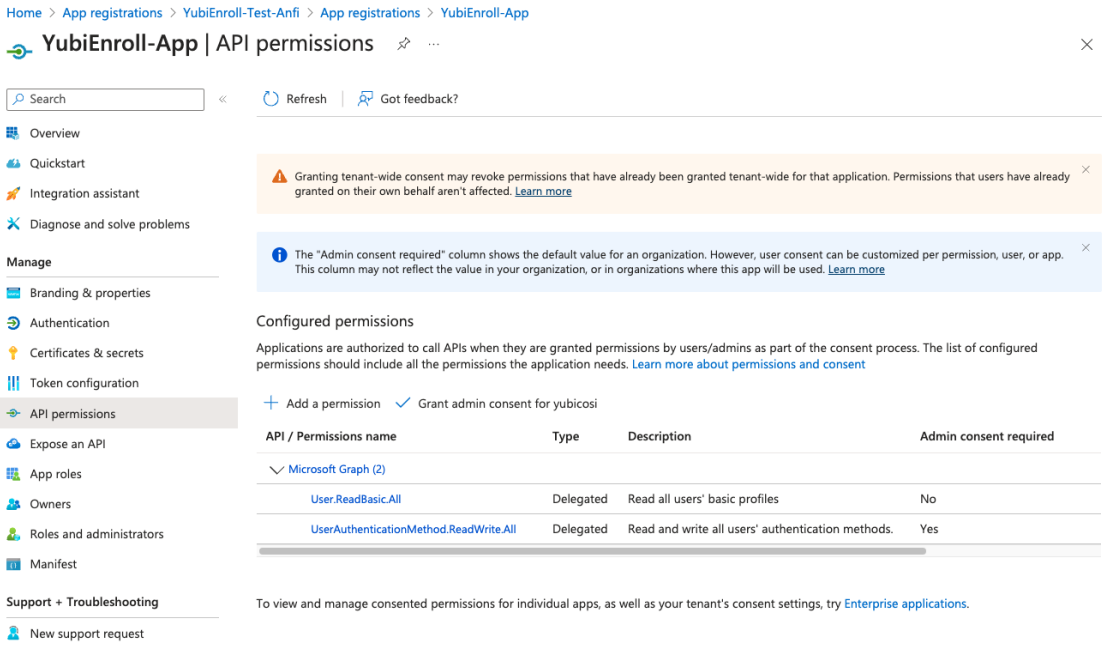
For more details on how to register the YubiEnroll app, see Register an application with the Microsoft identity platform (Microsoft documentation).

6.4 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.

Note: Even with the *Privileged Authentication Administrator* role, the administrator will not be 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).

6.5 Adding 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 will 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 will be 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 will need to change these endpoints. For more information, see Microsoft Graph national cloud deployments (Microsoft documentation).

CHAPTER

SEVEN

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*.

7.1 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.

7.2 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.

7.2.1 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 will be applied. If no authenticator settings or enrollment profile exist, you will be prompted to provide these.

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.

7.2.2 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 will be listed and you will be 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.

7.2.3 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`

7.3 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.

7.4 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.

7.5 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 will remove 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.

7.5.1 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.

7.5.2 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.

7.5.3 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.

7.6 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 will automatically activate 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.

7.6.1 yubienroll providers activate

`yubienroll providers activate [OPTIONS] NAME`

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

7.6.2 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]`	The identity provider to choose.
`-a, -- activate`	Activate configuration.
`-h, --help`	Show this message and exit.

7.6.3 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.

7.7 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.

7.8 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.

7.9 yubienroll users

`yubienroll users [OPTIONS] [QUERY]`

When enrolling an end user, you will 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 result will 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 will 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

EIGHT

RELEASE NOTES

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

8.1 2025

8.1.1 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 *Adding 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.

8.2 2024

8.2.1 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

NINE

COPYRIGHT

9.1 Trademarks

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

9.2 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.

9.3 Contact Information

Yubico AB
Gävlegatan 22
113 30 Stockholm
Sweden

9.4 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

9.5 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/hc/en-us and provide as much detail as you can.

9.6 Document Updated

2025-04-23 08:48:54 UTC