YubiEnroll User Guide

Yubico

Dec 19, 2024

CONTENTS

CHAPTER

ONE

INTRODUCTION

Note: YubiEnroll is currently in *Limited Early Access* for identity providers Okta and Microsoft Entra. For more information, see YubiEnroll.

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

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). For more information, see *Using YubiEnroll CLI*.

1.1 Supported Platforms

Yubienroll is currently available for identity providers Okta and Microsoft Entra and is compatible with and tested on Windows 11.

1.2 Compatibilities

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.

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 CLI tool provides an intuitive command line interface for interacting with the underlying YubiEnroll solution. You can for example:

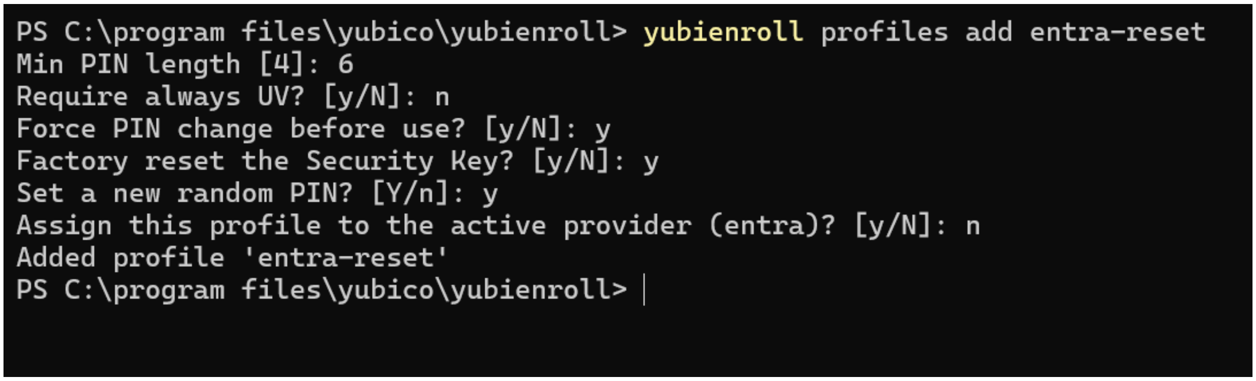
- Factory reset the YubiKey
- Set and change the PIN
- Configure Forcing PIN change
- Increase the minimum PIN length
- Configure Always require user verification (AlwaysUV)

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> yubienroll profiles add entra-reset
Min PIN length [4]: 6
Require always UV? [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
Assign this profile to the active provider (entra)? [y/N]: n
Added profile 'entra-reset'
PS C:\program files\yubico\yubienroll>
```

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 code 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 code 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. **Force PIN change before use:** If set to “on”, this setting forces the end user to change the provided PIN code when using the YubiKey the first time. Default is “off”.
4. **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”.
5. **Set a new random PIN:** If set to “true”, YubiEnroll generates a random PIN code. If set to “false”, the user can specify as specific PIN code.

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*

All provider configurations used by YubiEnroll are stored in a single TOML file located at

```
%APPDATA%\yubienroll\yubienroll.toml
```

This expands by default to

```
C:\Users\username\AppData\Roaming\yubienrolll\yubienroll.toml
```

where “username” is the user name of the current user. The file can be manually edited.

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"
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 code 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).

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 code 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 code 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

3.1 Downloading

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

3.2 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, 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). 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. When prompted to specify if you want to add a new enrollment profile [y/N], enter “y”.
5. Enter the following when prompted:

   a. **Profile name [default]** - the name to be used for the profile. 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 code length, for example 6. If you do not enter a PIN code length, the value “4” will be used. Note that the minimum PIN code length can never be shorter than “4”.

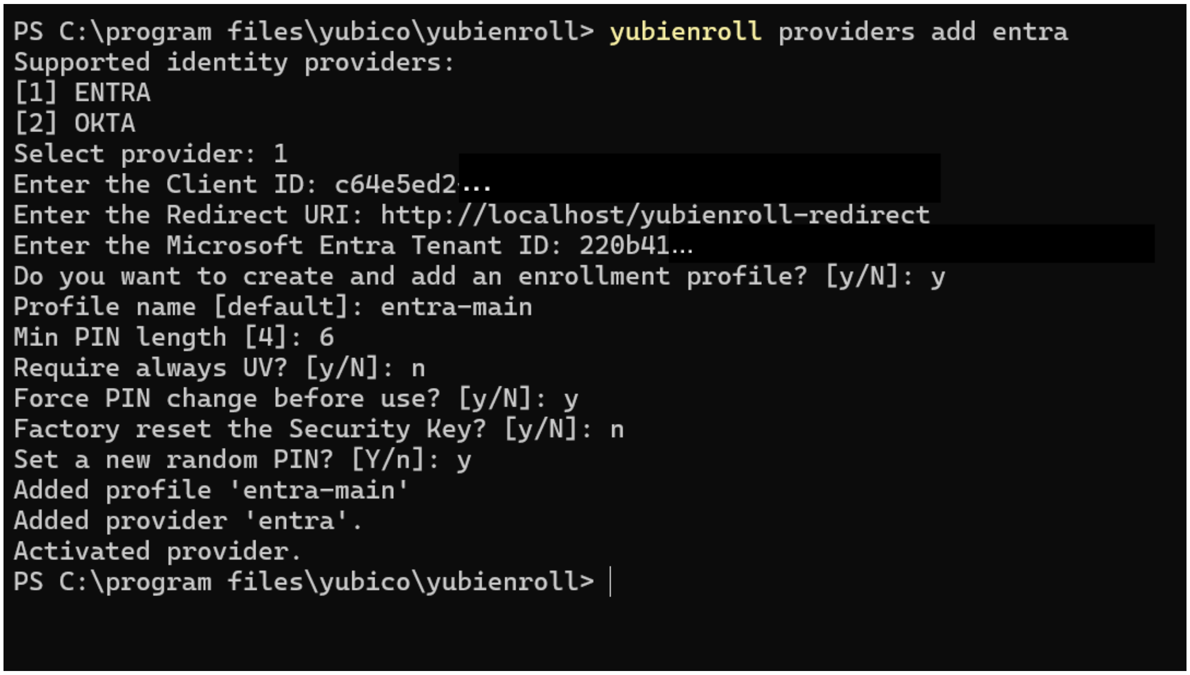
   c. **Require always UV? [y/N]** - define if the “Always require user verification” setting should always be overridden. Default is “no”.

   d. **Force PIN change before use? [y/N]** - Define if the end user must change the PIN code 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.

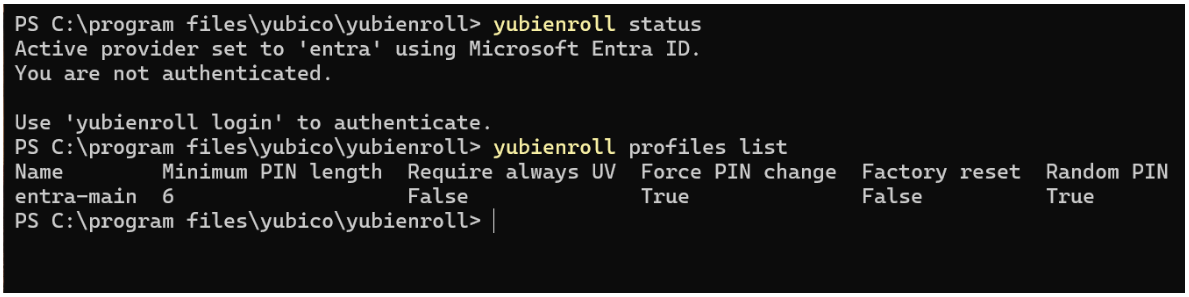
   f. **Set a new random PIN [Y/n]** - Enter “y” if you want YubiEnroll to set a new PIN code for the key. Enter “n” if you want to specify a specific PIN code.

6. 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> yubienroll providers add entra
Supported identity providers:
[1] ENTRA
[2] OKTA
Select provider: 1
Enter the Client ID: c64e5ed2... [redacted]
Enter the Redirect URI: http://localhost/yubienroll-redirect
Enter the Microsoft Entra Tenant ID: 220b41... [redacted]
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
Force PIN change before use? [y/N]: y
Factory reset the Security Key? [y/N]: n
Set a new random PIN? [Y/n]: y
Added profile 'entra-main'
Added provider 'entra'.
Activated provider.
PS C:\program files\yubico\yubienroll> 
```

7. 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> yubienroll status
Active provider set to 'entra' using Microsoft Entra ID.
You are not authenticated.

Use 'yubienroll login' to authenticate.
PS C:\program files\yubico\yubienroll> yubienroll profiles list
Name        Minimum PIN length  Require always UV  Force PIN change  Factory reset  Random PIN
entra-main  6                   False              True              False          True
PS C:\program files\yubico\yubienroll> |
```

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 code length, for example 6. If you do not enter a PIN code 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”.

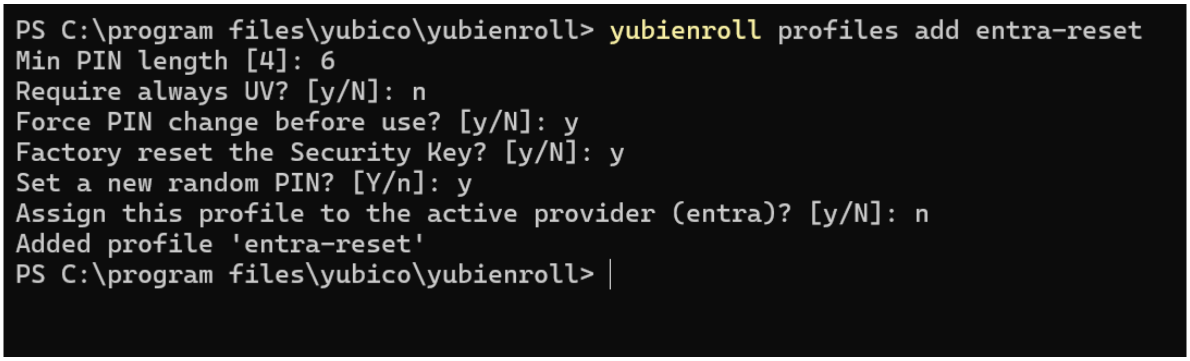
   c. **Force PIN change before use? [y/N]** - Define if the end user must change the PIN code when using the YubiKey for the first time. Default is “no”.

   d. **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.

   e. **Set a new random PIN [Y/n]** - Enter “y” if you want YubiEnroll to set a new PIN code for the key. Enter “n” if you want to specify a specific PIN code.

   f. **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> yubienroll profiles add entra-reset
Min PIN length [4]: 6
Require always UV? [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
Assign this profile to the active provider (entra)? [y/N]: n
Added profile 'entra-reset'
PS C:\program files\yubico\yubienroll>
```

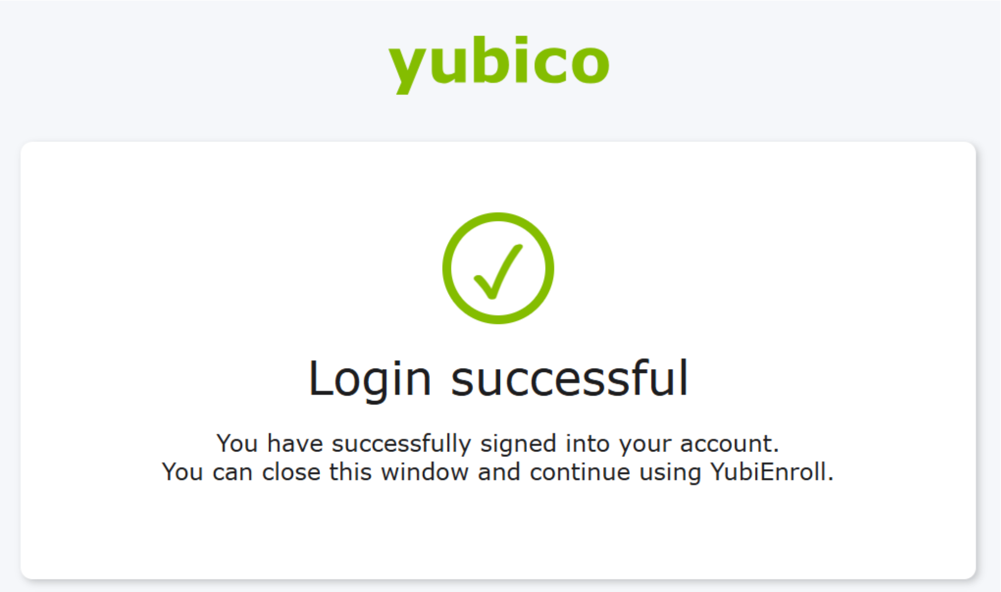
For more information about the `yubienroll profiles` command, see *YubiEnroll Commands*.

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*.

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.



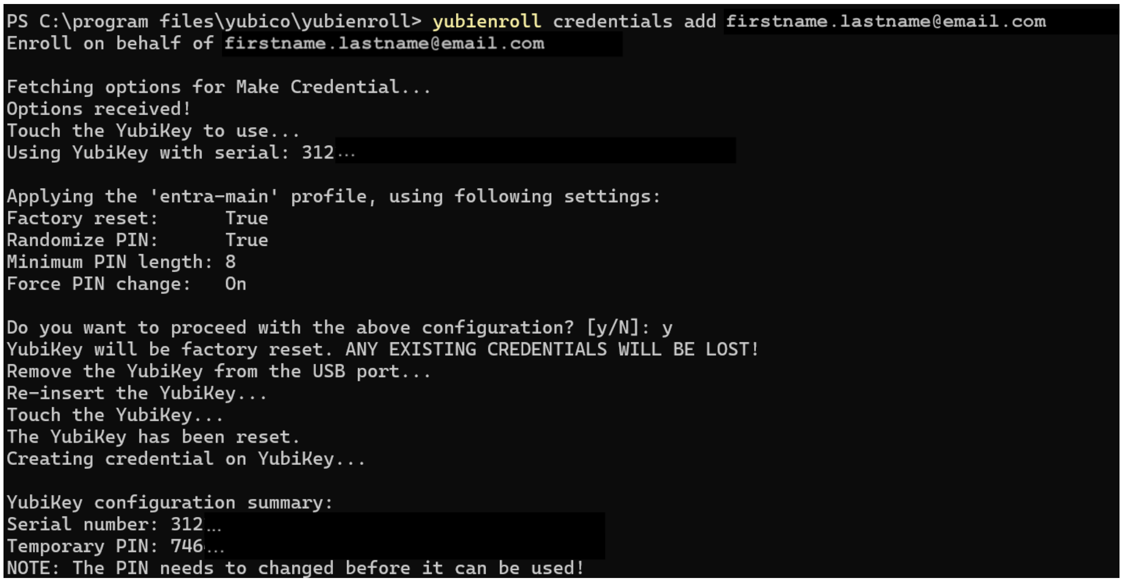
yubico

Login successful

You have successfully signed into your account.
You can close this window and continue using YubiEnroll.

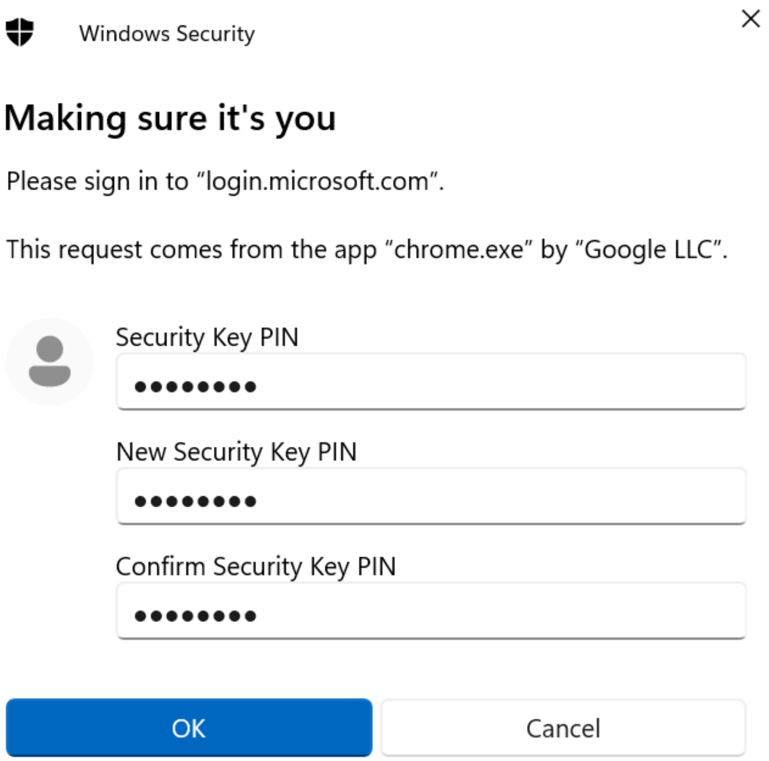
5. Insert or present the YubiKey you want to enroll.
6. Run the command `yubienroll credentials add firstname.lastname@email.com` where “firstname.lastname@email.com” is the end users’ account identifier in this example.

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 code to be used is displayed.



```
PS C:\program files\yubico\yubienroll> yubienroll credentials add firstname.lastname@email.com
Enroll on behalf of firstname.lastname@email.com

Fetching options for Make Credential...
Options received!
Touch the YubiKey to use...
Using YubiKey with serial: 312… [redacted]

Applying the 'entra-main' profile, using following settings:
Factory reset:      True
Randomize PIN:      True
Minimum PIN length: 8
Force PIN change:   On

Do you want to proceed with the above configuration? [y/N]: y
YubiKey will be factory reset. ANY EXISTING CREDENTIALS WILL BE LOST!
Remove the YubiKey from the USB port...
Re-insert the YubiKey...
Touch the YubiKey...
The YubiKey has been reset.
Creating credential on YubiKey...

YubiKey configuration summary:
Serial number: 312… [redacted]
Temporary PIN: 746…
NOTE: The PIN needs to changed before it can be used!
```

11. Provide the YubiKey and the temporary PIN code to the end user.
12. To authenticate with identity provider (Microsoft Entra in this example), the end user presents the provided YubiKey and the temporary PIN code. If the "Force PIN change" was set to "On", the end user is prompted to change the PIN code upon first log in.



Making sure it's you

Please sign in to “login.microsoft.com”.

This request comes from the app “chrome.exe” by “Google LLC”.

Security Key PIN: ●●●●●●●●

New Security Key PIN: ●●●●●●●●

Confirm Security Key PIN: ●●●●●●●●

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*.

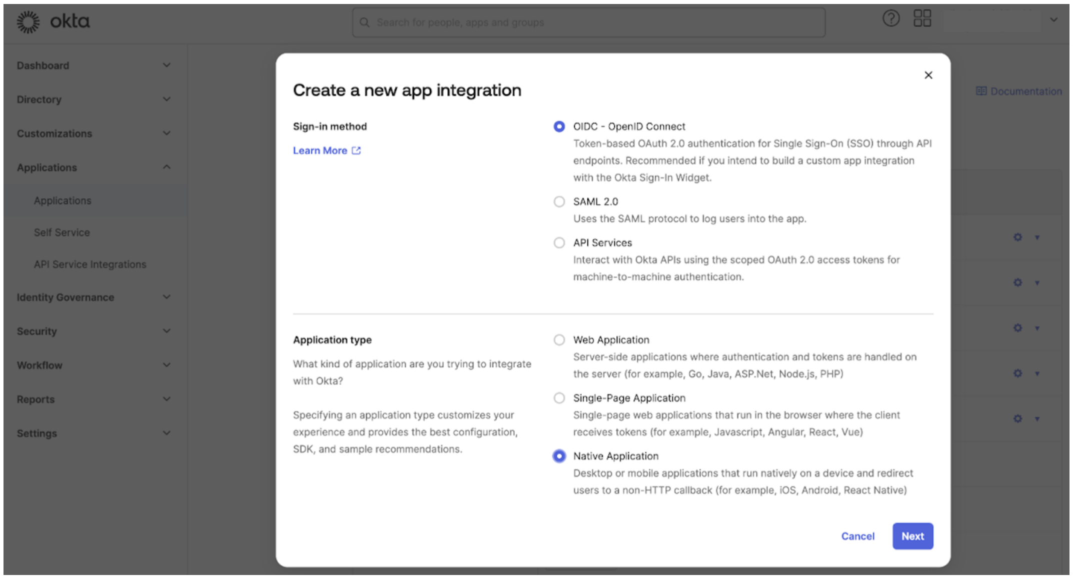
5.2 Registering the YubiEnroll App

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.



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
Uses the SAML protocol to log users into the app.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

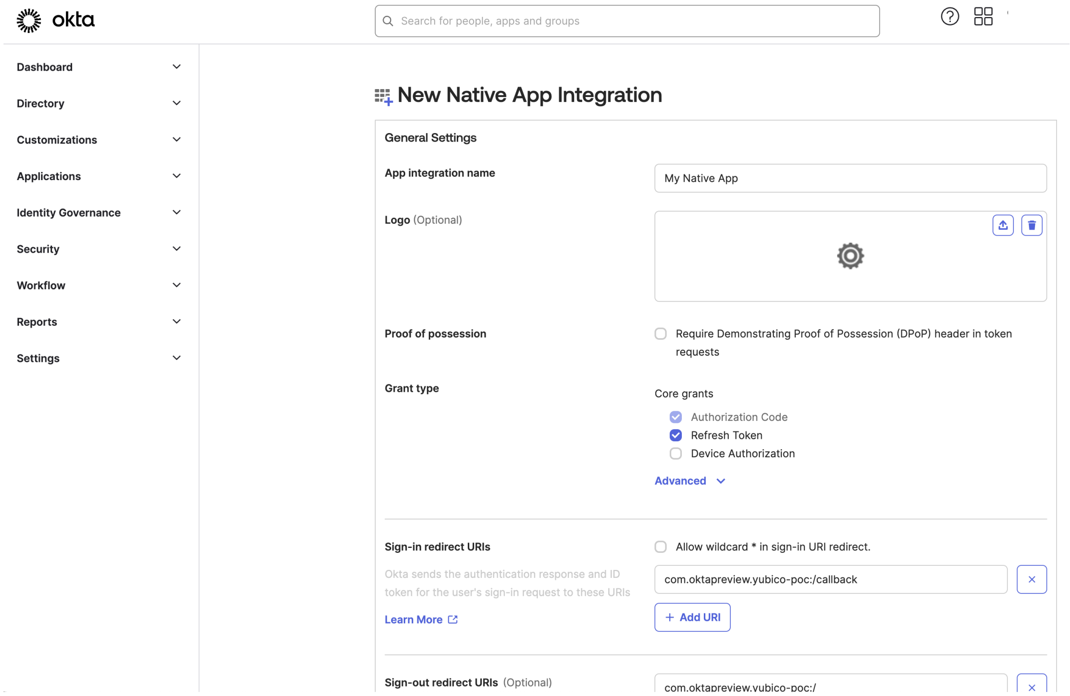
Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

○ Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

● Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

- 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.



New Native App Integration

General Settings

App integration name: My Native App

Logo (Optional)

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

Grant type

Core grants
☑ Authorization Code
☑ Refresh Token
□ Device Authorization

Sign-in redirect URIs: □ Allow wildcard * in sign-in URI redirect.
Okta sends the authentication response and ID token for the user's sign-in request to these URIs
Learn More
com.oktapreview.yubico-poc:/callback

Sign-out redirect URIs (Optional): com.oktapreview.yubico-poc:/

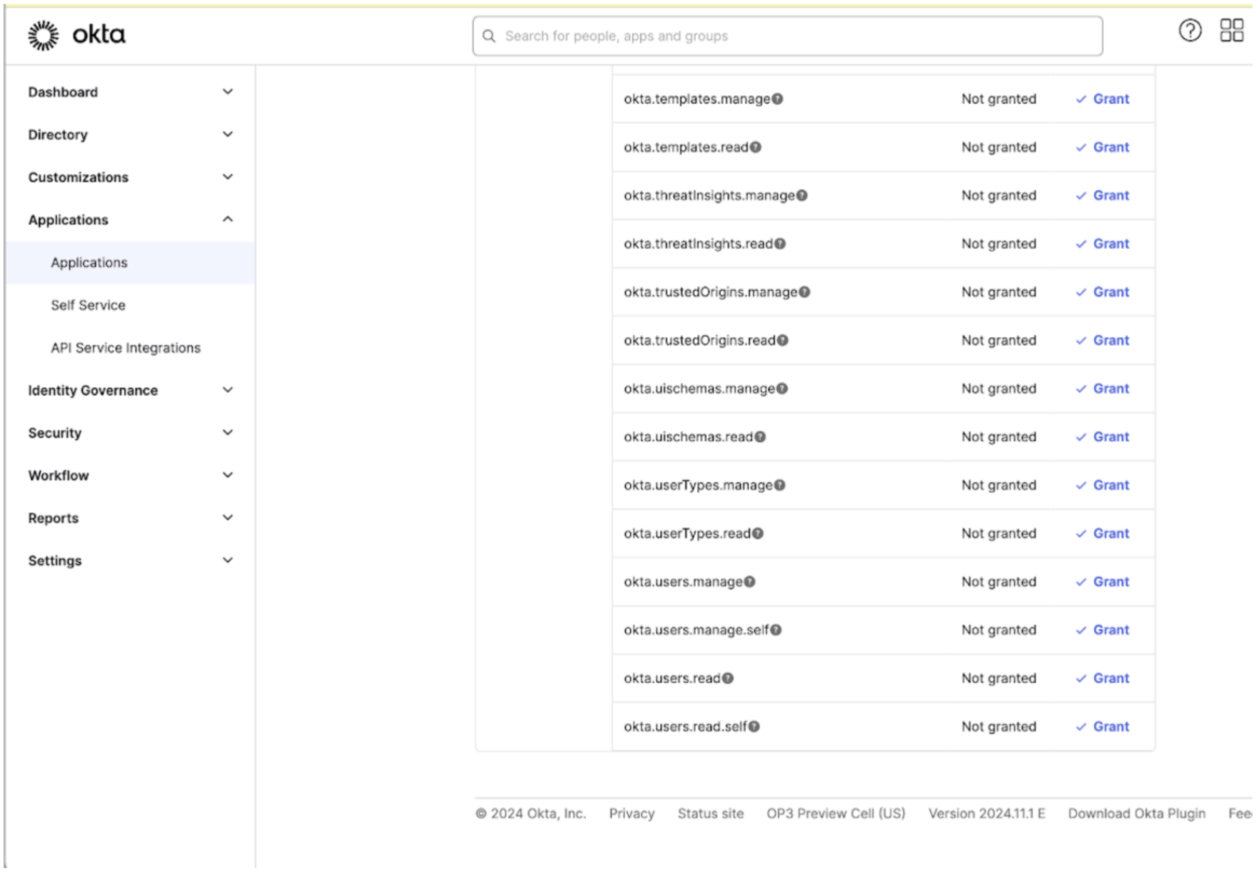
For more details on how to register the YubiEnroll app, see Create an OAuth 2.0 app in Okta (Okta documentation).

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.



okta.templates.manage	Not granted	✓ Grant
okta.templates.read	Not granted	✓ Grant
okta.threatInsights.manage	Not granted	✓ Grant
okta.threatInsights.read	Not granted	✓ Grant
okta.trustedOrigins.manage	Not granted	✓ Grant
okta.trustedOrigins.read	Not granted	✓ Grant
okta.uischemas.manage	Not granted	✓ Grant
okta.uischemas.read	Not granted	✓ Grant
okta.userTypes.manage	Not granted	✓ Grant
okta.userTypes.read	Not granted	✓ Grant
okta.users.manage	Not granted	✓ Grant
okta.users.manage.self	Not granted	✓ Grant
okta.users.read	Not granted	✓ Grant
okta.users.read.self	Not granted	✓ Grant

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*.

CHAPTER

SIX

YUBIENROLL WITH MICROSOFT ENTRA

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

6.1 Configuration Steps

The configuration steps involve the following:

- *Registering the YubiEnroll application in Microsoft Entra*.
- *Configuring the YubiEnroll permissions in Microsoft Entra*.
- *Adding the Microsoft Entra 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 Registering the YubiEnroll App

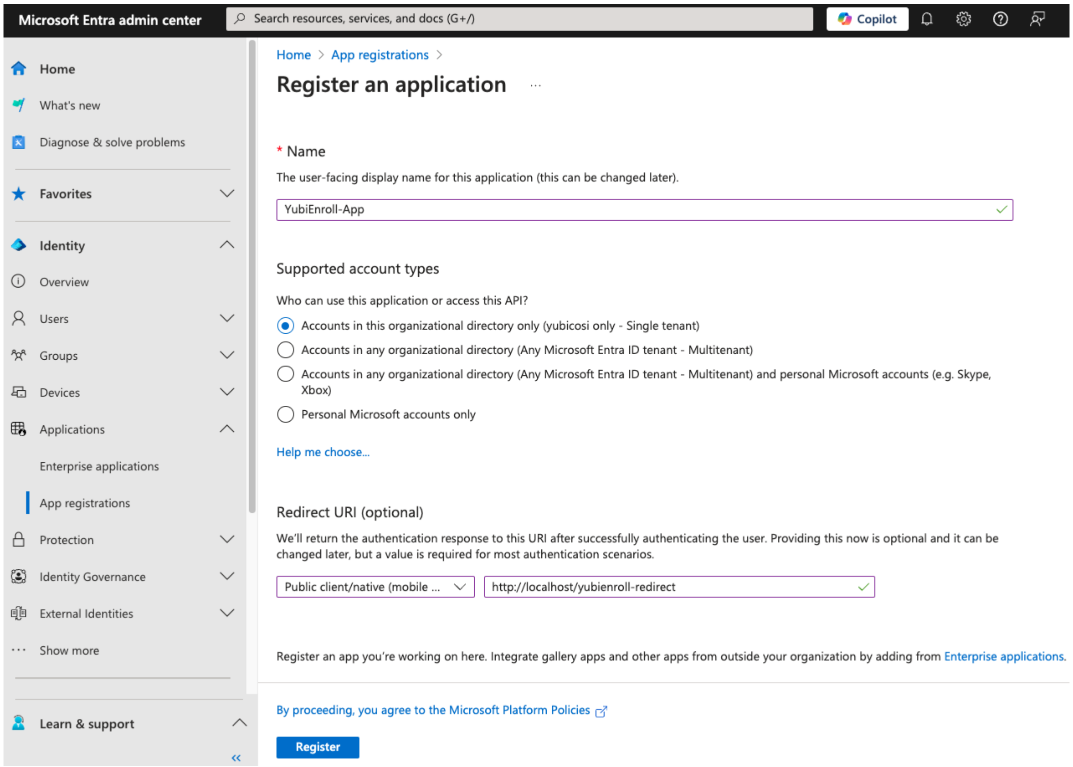
When configuring the Microsoft Entra provider in YubiEnroll, the following parameter values are needed:

- client_id
- tenant_id
- redirect_uri

These parameter values are created when registering the YubiEnroll (OAuth) application in Microsoft Entra. To register the YubiEnroll app, 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 supports ephemeral ports.



Register an application

* Name

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

YubiEnroll-App

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (yubicosi only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | http://localhost/yubienroll-redirect

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

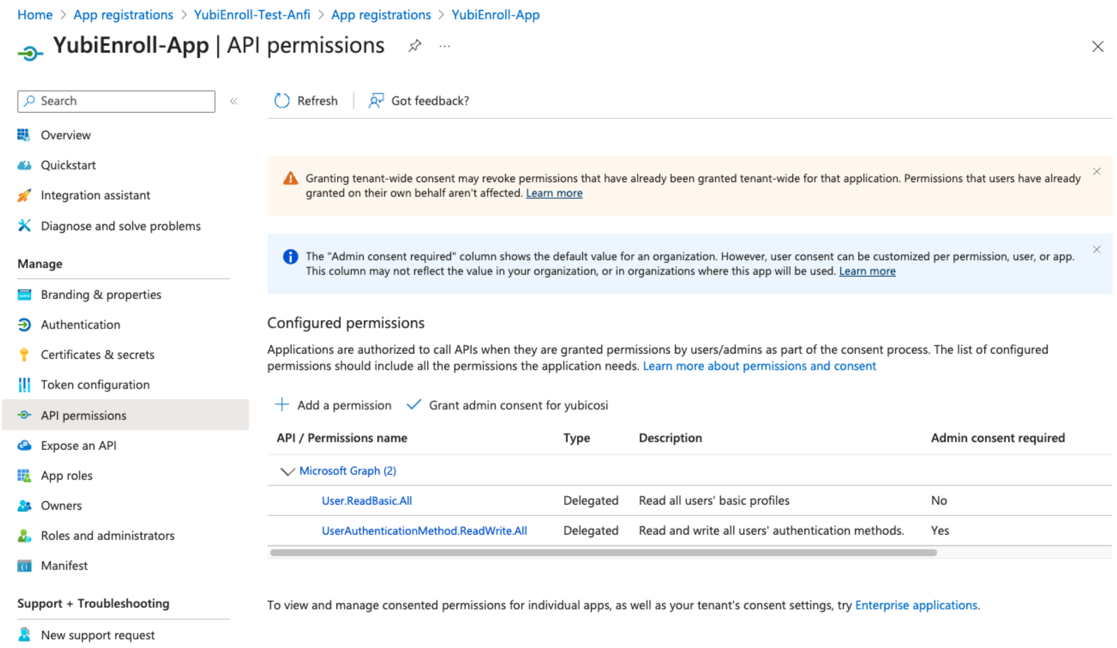
By proceeding, you agree to the Microsoft Platform Policies

Register

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

6.3 Configuring Permissions

The permissions required by YubiEnroll in Microsoft Entra are **Microsoft Graph Delegated permissions** “User.ReadBasic.All” and “UserAuthenticationMethod.ReadWrite”. To add these, open the YubiEnroll app in Microsoft Entra, select **API permissions** in the left menu, and click **Add a permission**.



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

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

Configured permissions

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

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

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

For more information on how to configure app permissions, see Overview of Microsoft Graph permission (Microsoft documentation).

For a user to be able to grant consent to these permissions, the user must be assigned a supported Microsoft Entra Role. One of the following least privileged roles are supported for this operation:

- Authentication Administrator
- Privileged Authentication Administrator

6.4 Adding the Microsoft Entra Provider

Before you can run YubiEnroll with Microsoft Entra, 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, 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*.

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|T`	Enable logging at given verbosity level.
`--log-file FILE`	Write logs to a specified FILE.
`-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`	Logout from the active provider.
`profiles`	Manage enrollment profiles.
`providers`	Manage authentication settings for identity providers.
`status`	Show which provider is active and its authentication status.
`users`	Search for users.

7.2 yubienroll login

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

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

Commands

Command	Description
`login`	Authenticate with an identity provider.

7.3 yubienroll logout

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

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`	Logout from the active provider.

7.4 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 a user.
`delete`	Delete a FIDO credential for a user.
`list`	List FIDO credentials for a user.

7.4.1 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 code length or force PIN code 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 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`	Delete a FIDO credential for a user.
`--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.
`--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.
`-h, --help`	Show this message and exit.

7.4.2 yubienroll credentials delete

```
yubienroll credentials delete [OPTIONS] CREDENTIAL_ID
```

Delete credentials available in the identity provider for an end user.

Examples

- Delete credentials in the identity provider for the end user with `credential_ID` “123XYZ”.

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

7.4.3 yubienroll credentials list

```
yubienroll credentials list [OPTIONS]
```

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

Examples

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

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

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 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.

7.6 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
```

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 full provider configuration.

7.7 yubienroll status

```
yubienroll status
```

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.

7.8 yubienroll users

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

When enrolling an end user, you will need the user identifiers “ID” and “Username”. Often “Username” is the same as the email address in the identity provider, but it does not have to be.

You can search for users in the identity provider using the `yubienroll users <query>` command where “query” can be for example the name of the end user. The user identifier “ID” and “Username” will be returned which is used in the enrollment.

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.