Entra: HYPR Enterprise Passkey in CC

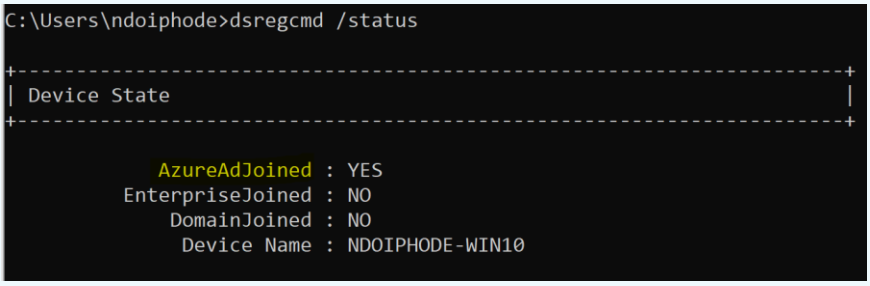
HYPR Enterprise Passkey (a.k.a. the FIDO2 Mobile Authenticator pattern) enables your HYPR Mobile App-enabled device to act as a FIDO2 security key when authenticating through Microsoft Entra. Once implemented, Entra will see any affected mobile devices as hard token passkeys.

HYPR Enterprise Passkey can be integrated with several different workstation setups, depending on your environment:

- *Non-domain-joined*: Windows workstation is not joined to any domain and is owned by the user; the user can login via a Microsoft account or an account local to the machine
- *On-premises Active Directory*: Windows workstation is joined to an on-premises Active Directory and is owned by the user; the user can login to any workstation which is joined to same domain using the user credentials on the domain controller
- *Entra Domain-joined*: Windows workstation is joined directly to the Entra cloud; the user can login to any workstation joined to Entra AD using the user account in Entra
- *Hybrid Entra Domain-joined*: Windows workstation is joined to both the on-premises Active Directory and to the Entra cloud; the user can login using the user credentials on the domain controller.

- Use the following command to check the status of a Windows workstation:

```
dsregcmd /status
```



Only AzureAdJoined is set to Yes because the workstation is only joined to AzureAD

Incase of HYBRID workstation, DomainJoined will be set to Yes as well

Feature Flags

Following Feature Flags are required to be enabled for the rpApp:

Mandatory to be enabled (No Wifi or BLE)

✅AZURE_IDP_INTEGRATION

✅AZURE_NATIVE_LOGIN

✅FIDO2_MOBILE_AUTHENTICATOR

✅RP_APP_WORKSTATION_ENABLED

✅AZURE_PROVISION_API

What You'll Need

Server/Tenant

- Make sure you have the **Entra tenant** available and an account that exists on the *.onmicrosoft.com domain with **Global Admin Access**
    - Enable FIDO2 Security Keys in the Entra tenant as referenced here or here
- You should have an **Intune account** on the *.onmicrosoft.com domain with **Global Admin Access** with Intune licenses
    - Enable the FIDO2 Security Key Credential Provider in Intune:
        - Enabling for new workstation joins
        - Enabling for existing workstation joins
        - Microsoft documentation

Workstation

- Currently the workstation/VM OS must be **Windows**, as macOS is not yet supported
- Entra **domain-joined** or hybrid-joined VMs or physical laptops with which to test

- Ensure the Windows Workstation OS patch level requirements are met
- HYPR Passwordless client must be installed on the affected workstation(s)
- Workstation support for FIDO2 security keys will vary depending on how the workstation is joined:
    - Microsoft does not support FIDO2 security keys for authentication to Active Directory workstations
    - Microsoft supports FIDO2 security keys for authentication to Hybrid Entra AD joined workstations
    - Microsoft supports FIDO2 security keys for authentication to Entra AD joined workstations
- Hybrid workstations only:
    - Ensure Domain Controller patch level requirements are met
    - Ensure AES256_HMAC_SHA1 is enabled [required]
    - Configure Active Directory and Entra to support Entra AD Kerberos
    - Additional steps to support administrative accounts.
        - By default, these accounts can't use security keys

Setting Up the Entra AD Tenant

Using Powershell script

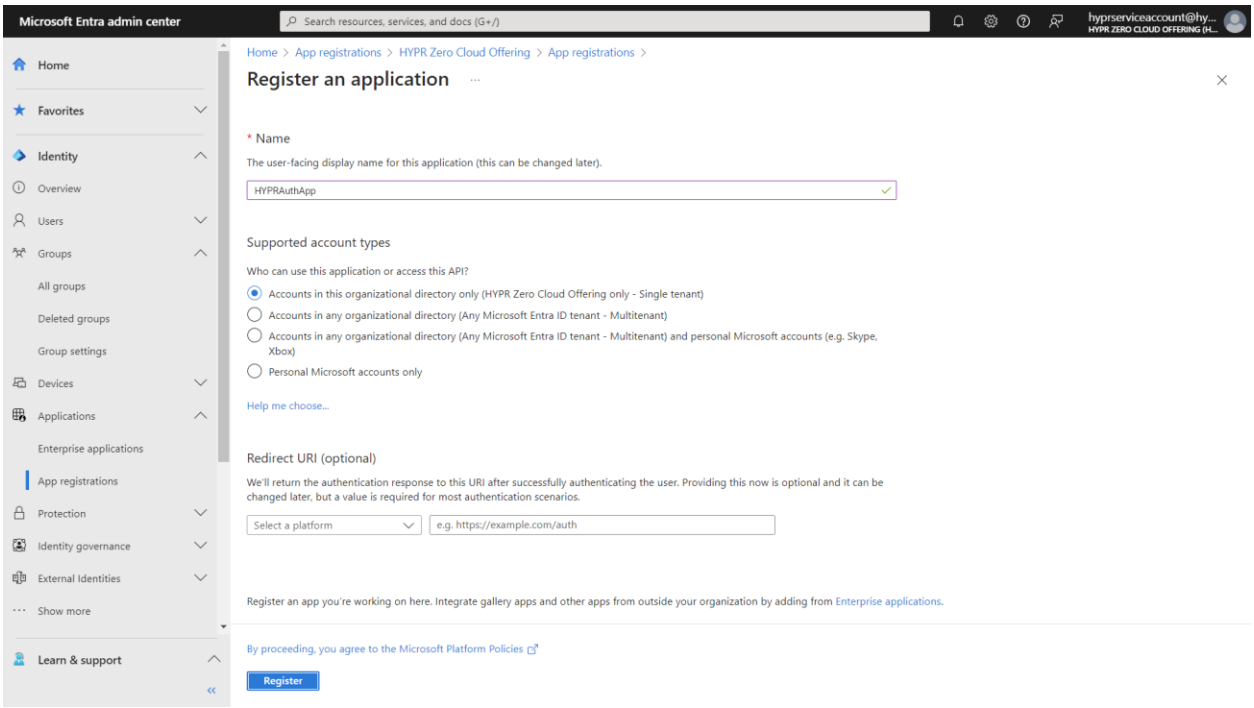
EPK App registration first iteration.ps1

Note: Change the app name to match required by HYPR

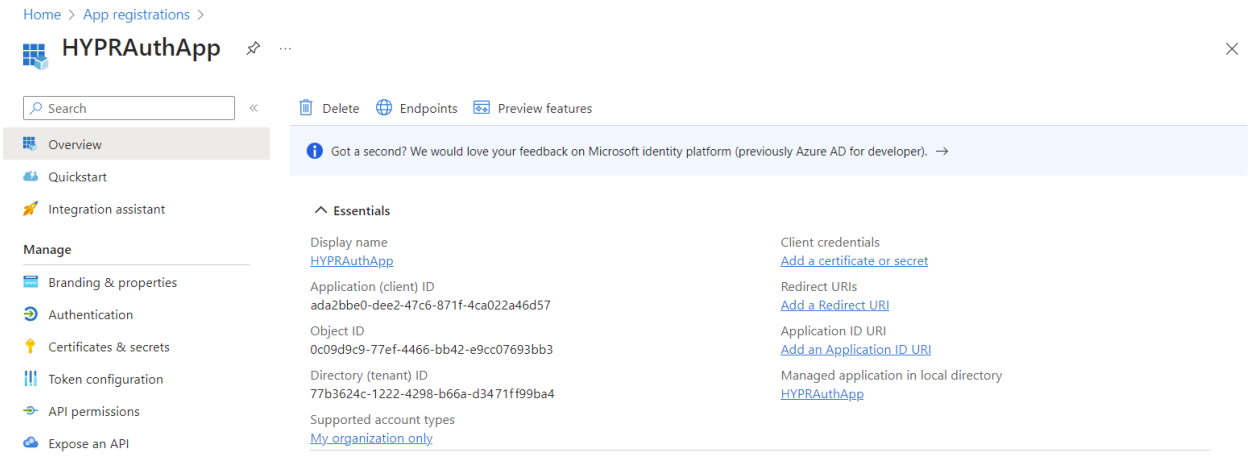
OR via User interface

Register Application

1. From the Home screen, select **Entra Active Directory > App registrations > New registration**.

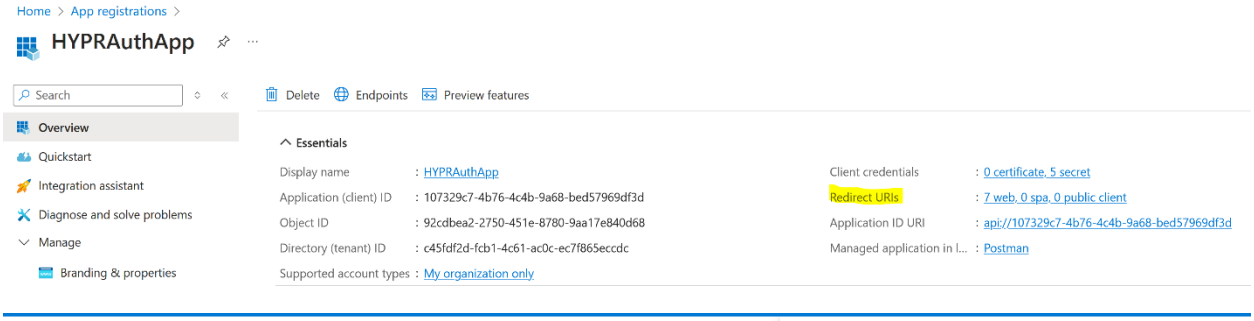


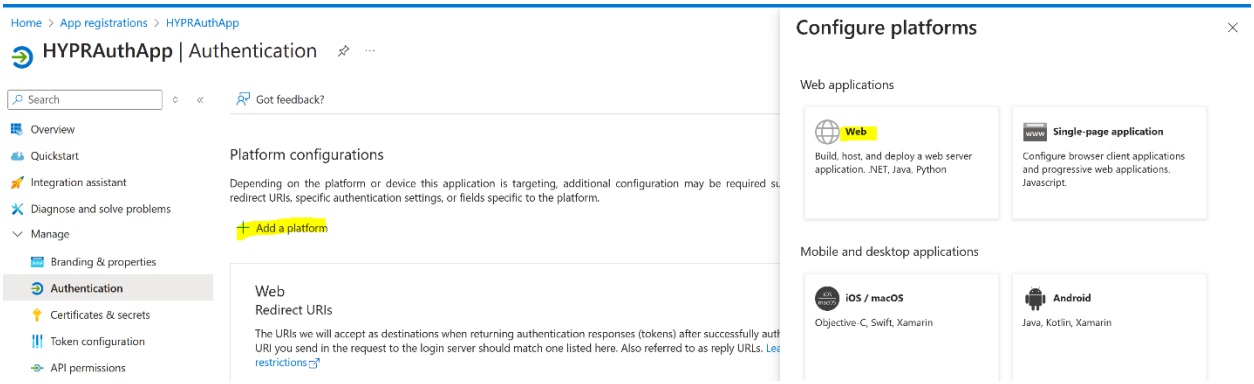
2. On the *Register an application* dialog:
    - Enter the application name: **HYPRAuthApp**
    - Select **Accounts in this organizational directory only**
    - Click **Register** when done
3. Save the clientId and tenantId. You will need these later for PowerShell and HYPR's UX configuration.

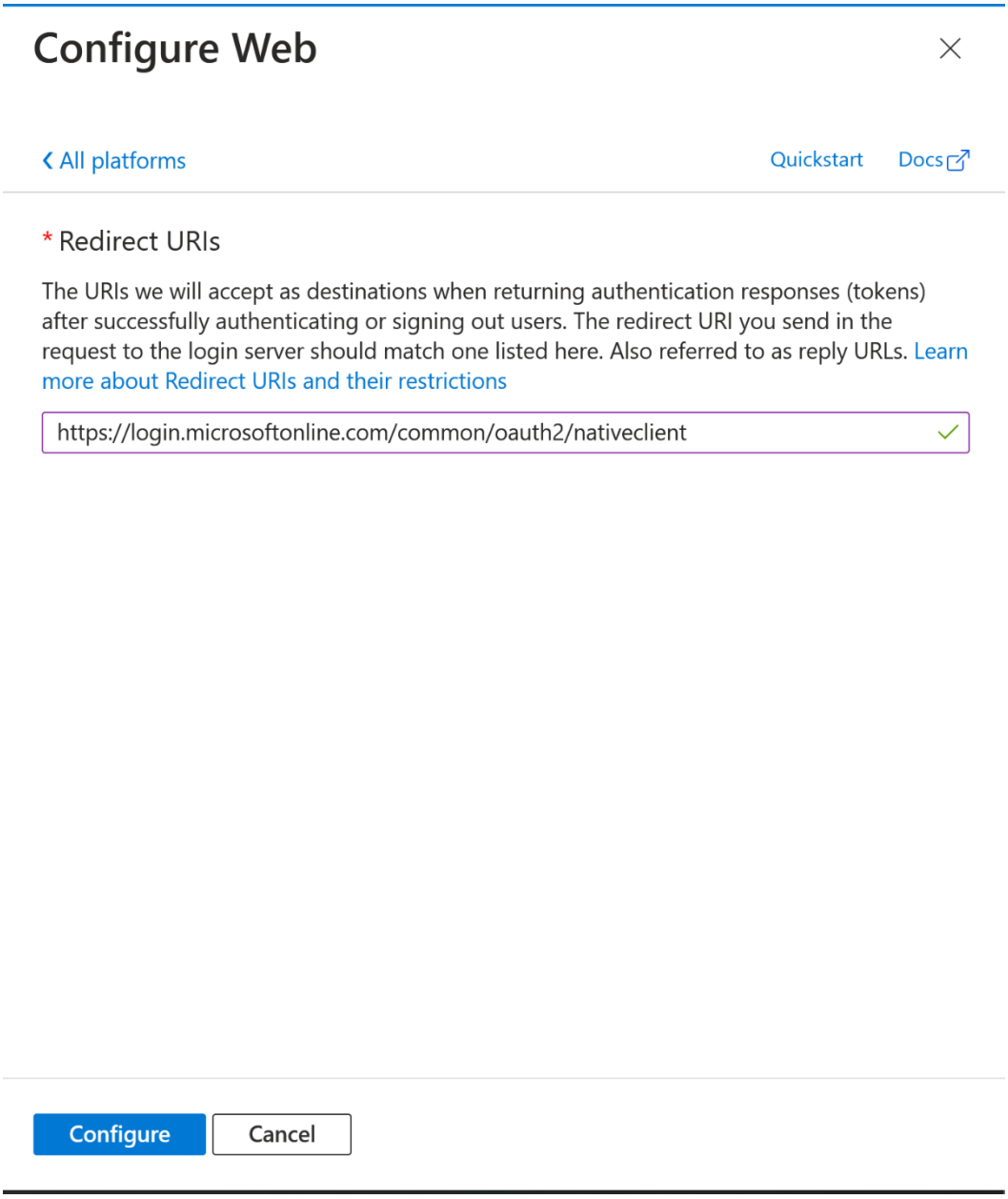


Configure a Web Redirect URI

Entra ID --> App Registrations --> “HYPR app” --> redirect URI --> *“https://login.microsoftonline.com/common/oauth2/nativeclient”*

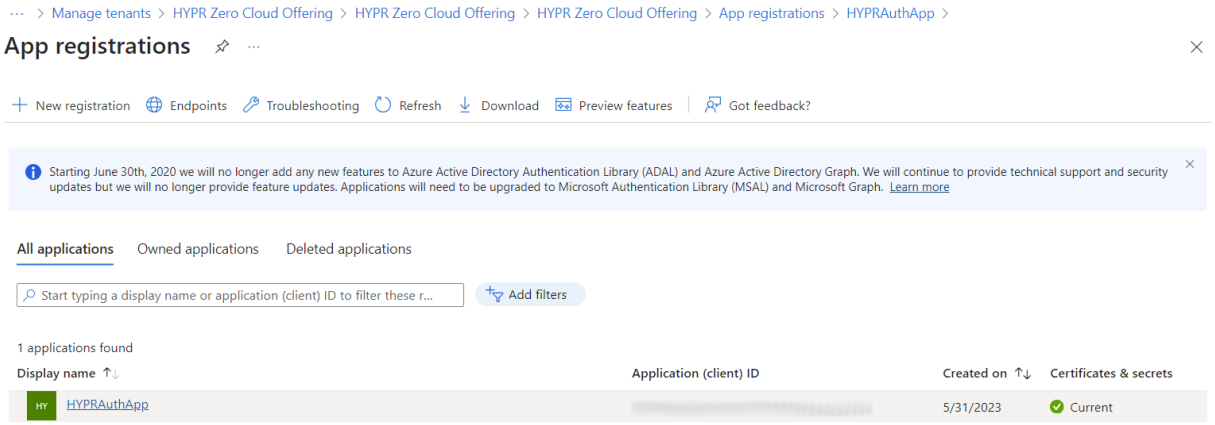




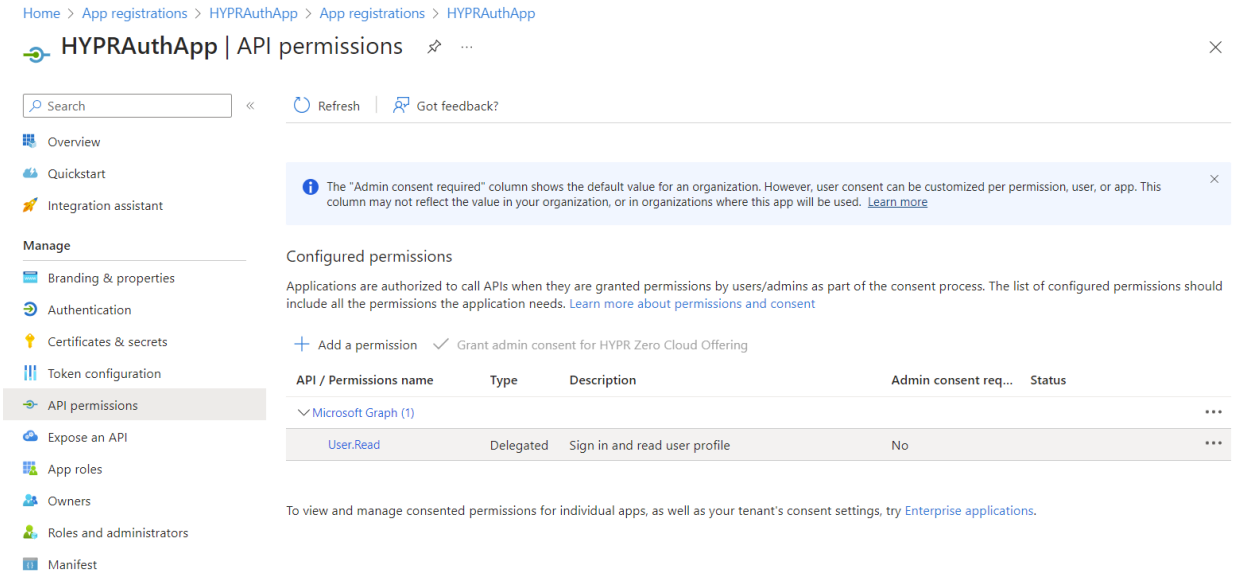

Configure Web
All platforms
Quickstart
Docs
* Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions
https://login.microsoftonline.com/common/oauth2/nativeclient
Configure
Cancel

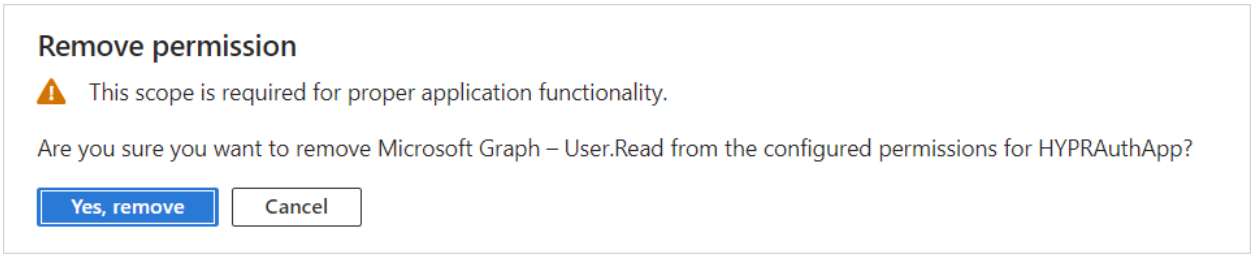
Grant Required API Permissions

1. From the Entra Active Directory screen, select **App registrations** and **select the app you just made**.

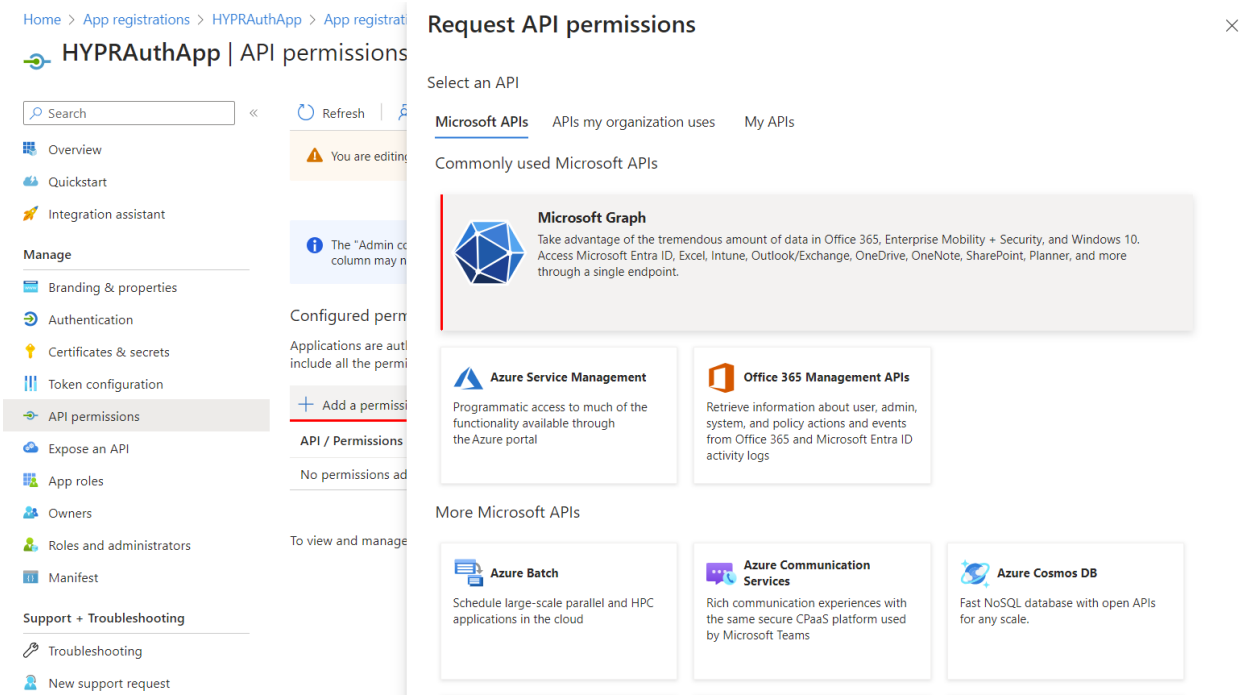


2. While that app is selected, click **API permissions**.
3. By default, the application will already have Microsoft Graph's *User.Read* permission. This isn't required, so **remove it** by clicking the **...** icon and choosing **Remove permission**. Click **Yes, remove** to confirm when prompted.

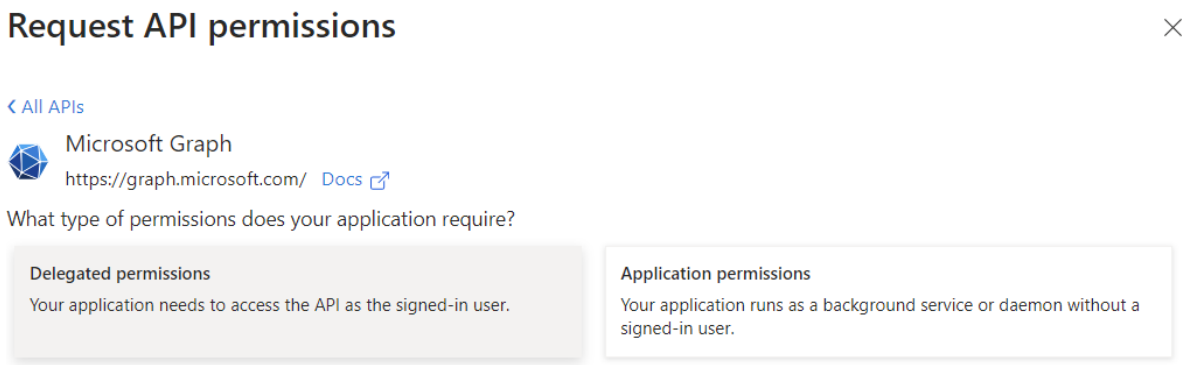




4. Click **Add a permission**, and on the tiled choices, select **Microsoft Graph**.



5. Select **Delegated permissions**.

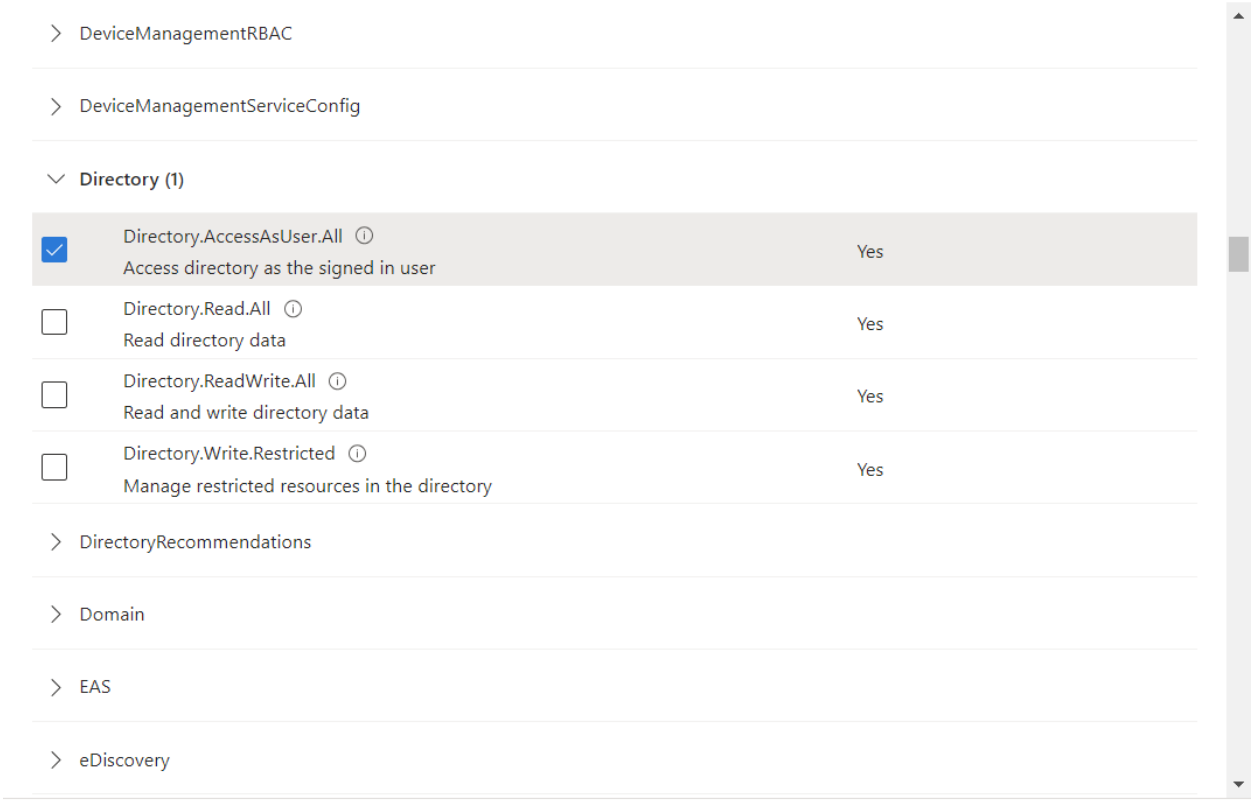


Delegated by Default

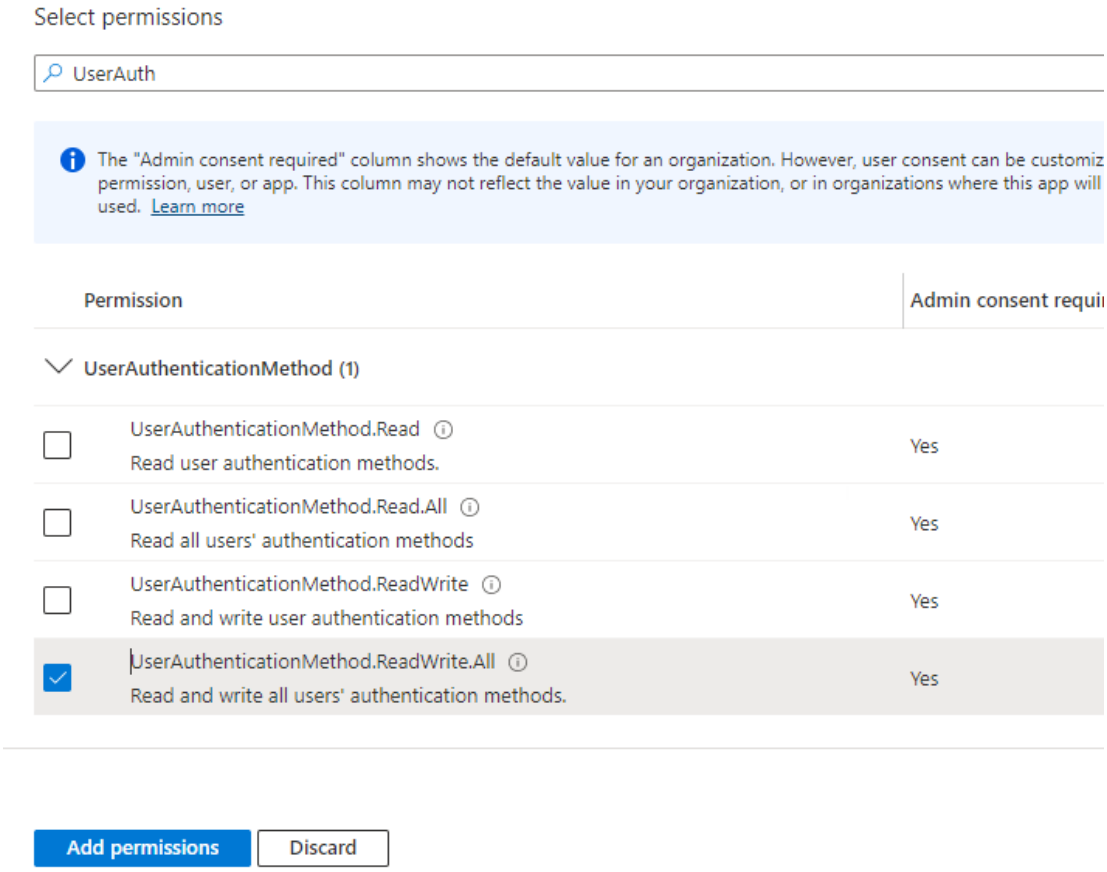
Sometimes Entra will not display the option for Delegated or Application permissions, and will immediately assume Delegated as the choice. As no Application permissions are required, this works in your favor. However, after you grant Admin Consent later in the process, you will be able to verify the permission type.

6. Scroll down and locate **Directory.AccessAsUser.All***. Add it, then continue scrolling to find and add **UserAuthenticationMethod.ReadWrite.All**.

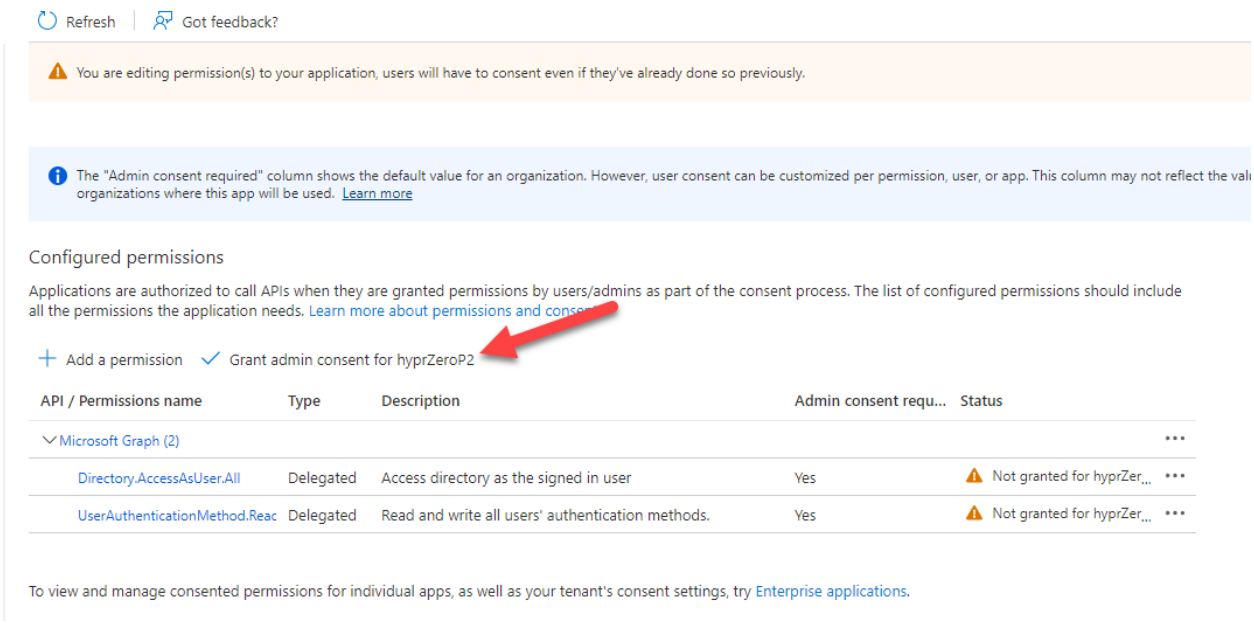
Request API permissions

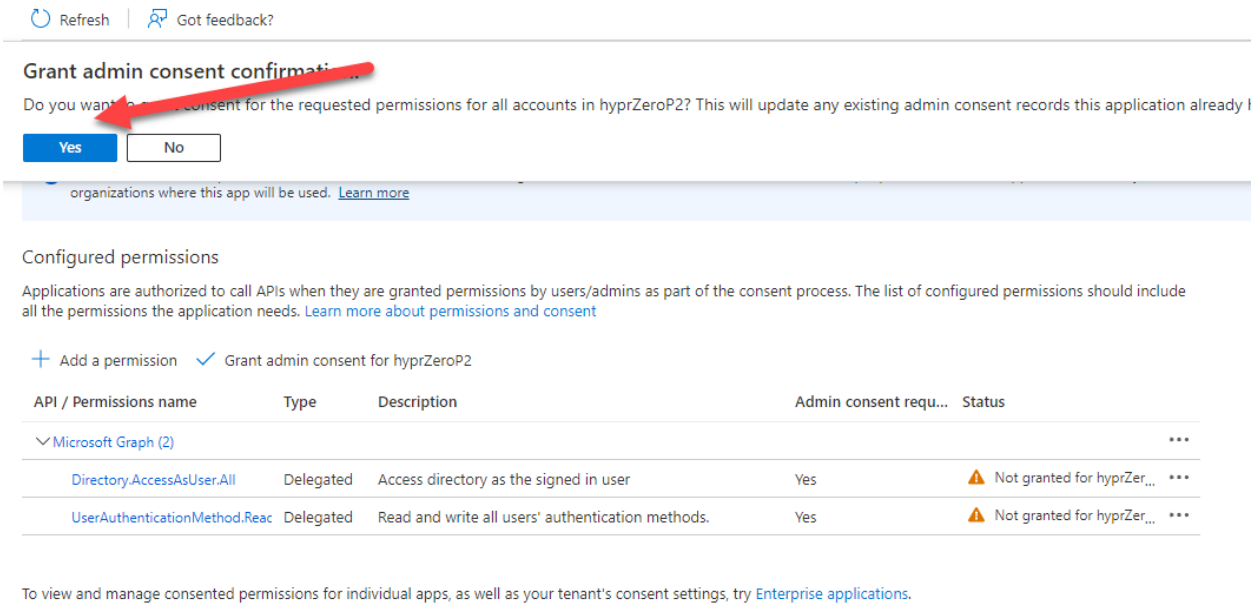


Add permissions | Discard

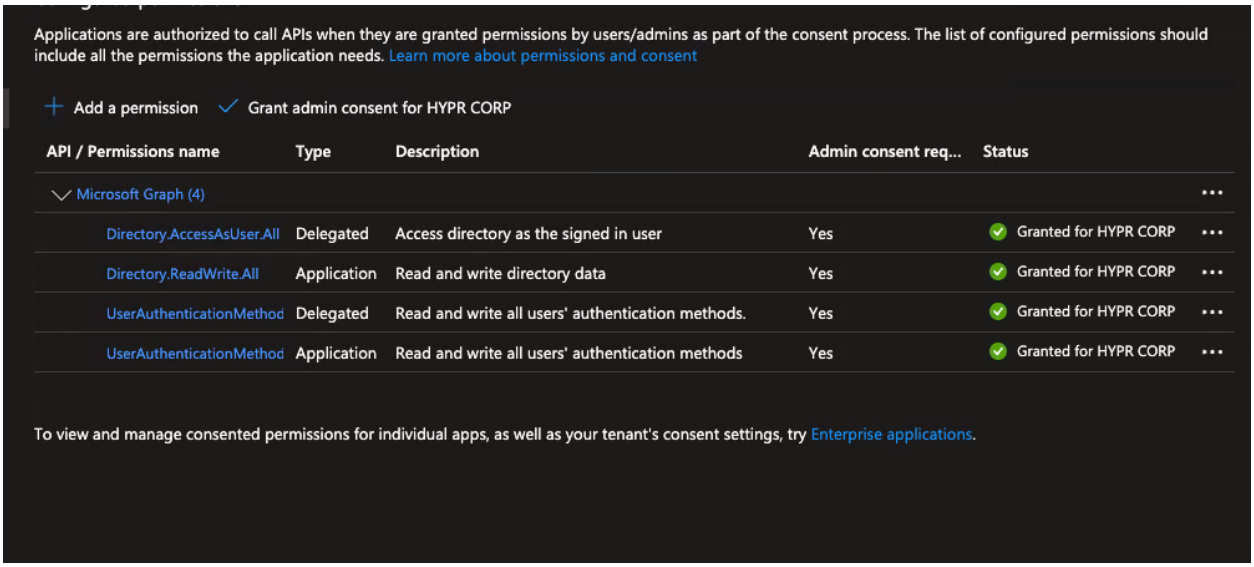


7. Click **Add Permissions** when done.
8. You must now **Grant admin consent** for the permissions to take effect.





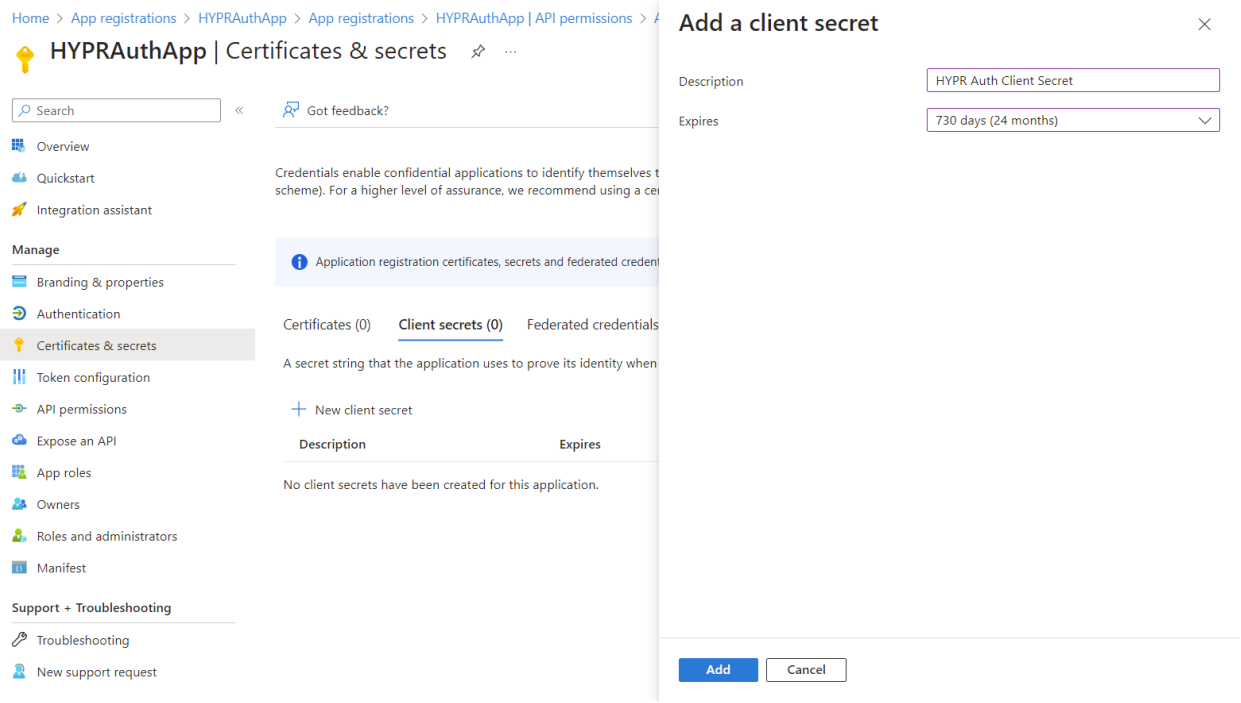
****Updated Permissions 10.1



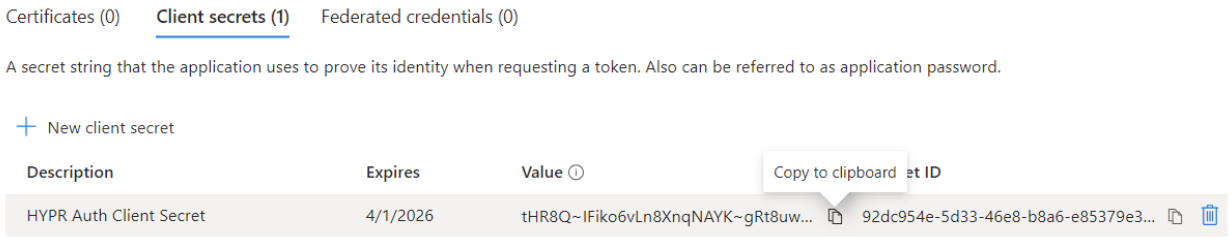
Creating a Client Secret

You'll need to provide a client secret when you set up the integration in the HYPR Control Center. Generate the client secret in Entra as follows:

1. From the Entra Active Directory screen, select **App registrations** and choose your app.
2. Select **Certificates & secrets**, then click **New client secret**.



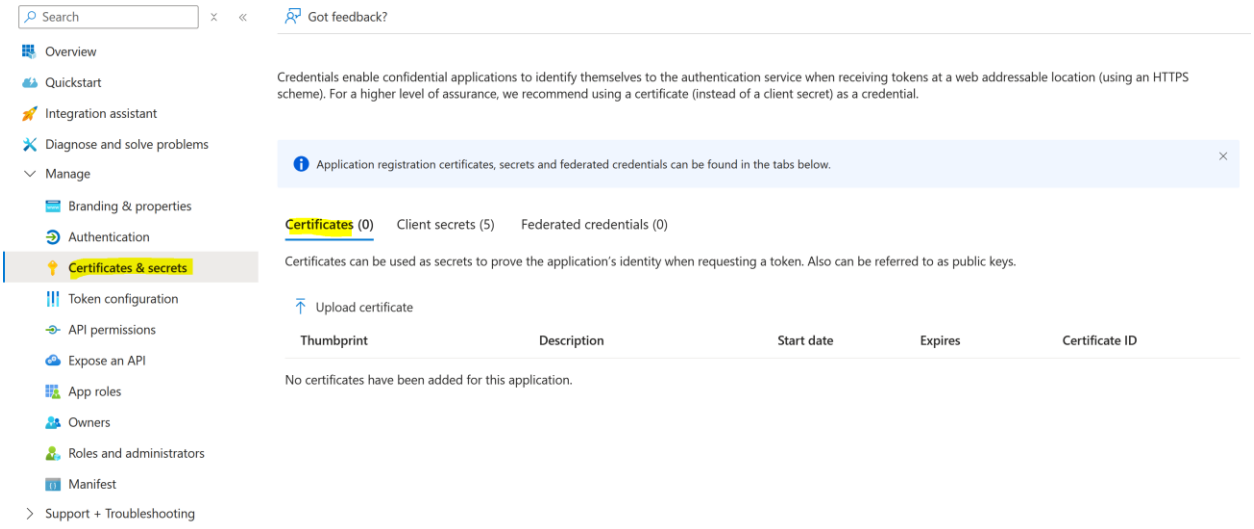
3. Enter a **Description** and an **Expires** date. Click **Add** when finished. Entra returns to the *Certificates and Secrets* list.
4. **Make a note of the client secret value** now so you can use it later.



One Time Only

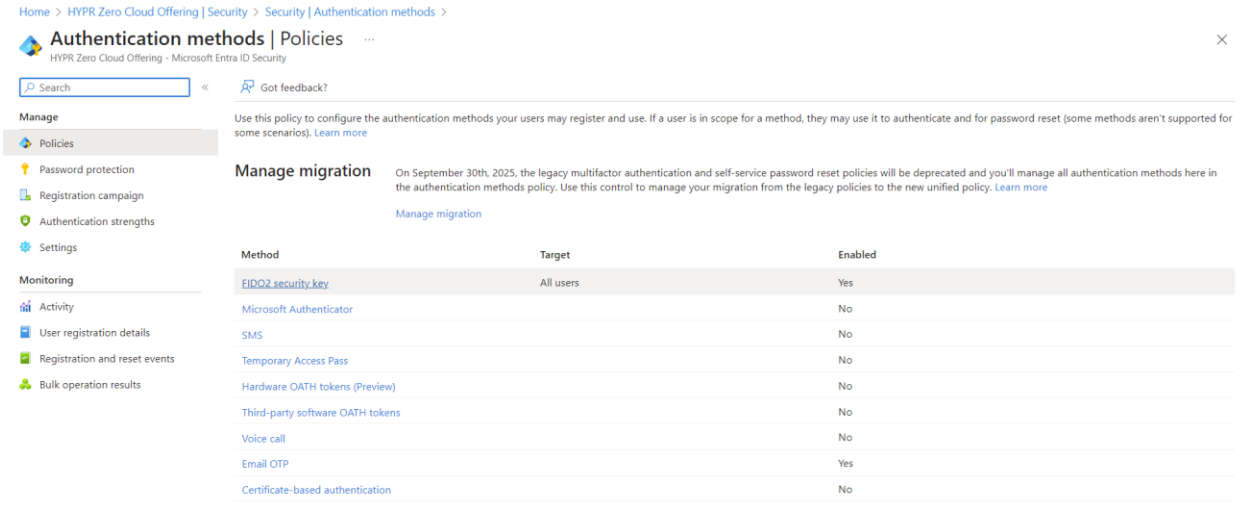
If you return to this screen later, Entra will mask the value and you won't be able to copy it.

5. OR Use Certificates

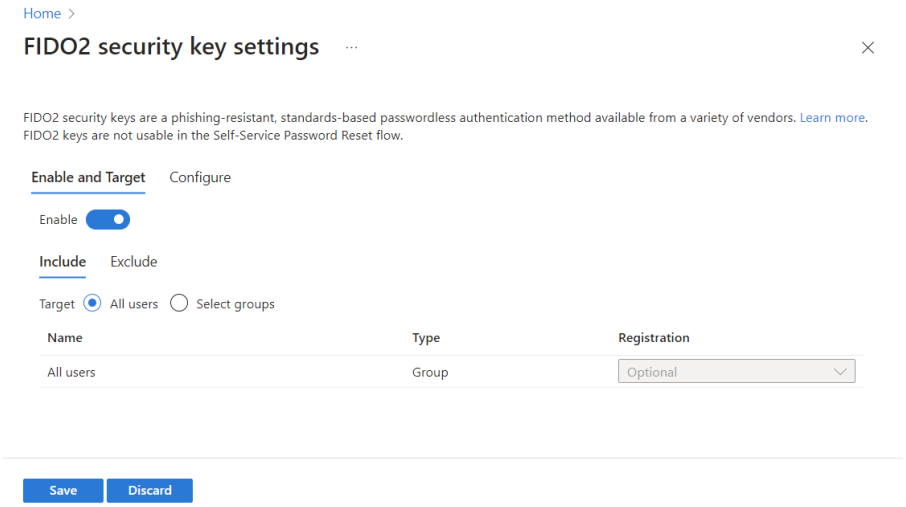


Enable Security Keys in the Entra Tenant

1. **Login** to entra.microsoft.com as a global admin account.
2. Navigate to **Entra Active Directory > Security > Authentication methods**. Click **FIDO2 security key**.



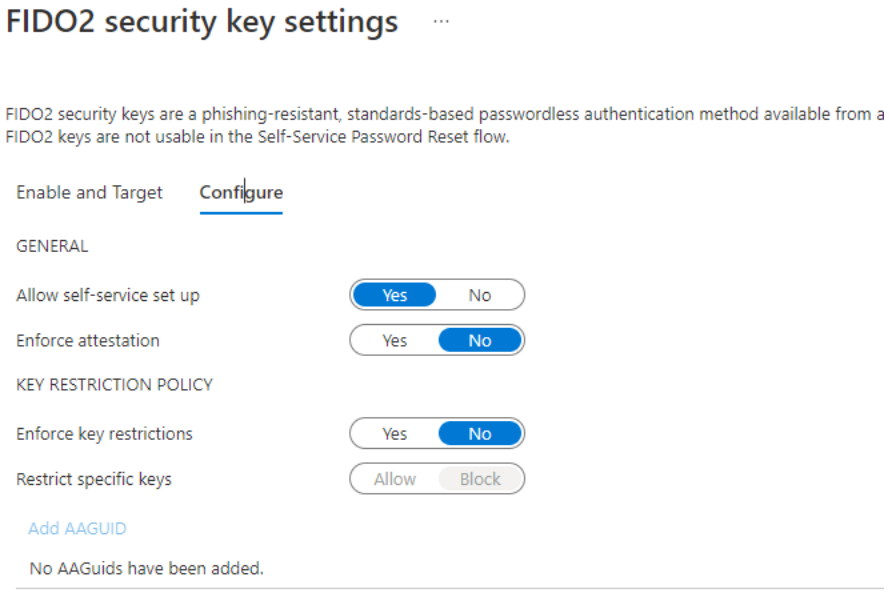
3. *FIDO2 security key settings* defaults to the *Enable and Target* tab. Here you can enable security keys and define allowed users. **Include All users** and leave the registration as **Optional**.



4. On the *Configure* tab, make sure the **settings are as depicted below**. This is the only configuration we will support at this time.

Enforced Attestation

Microsoft uses the *Enforce attestation* feature to ensure the FIDO2 authenticator is certified by the FIDO Alliance and approved by Microsoft's team. HYPR's AAGUID was added as an approved FIDO2 Authenticator on March 2023. HYPR supports this setting as either *True* or *False*.



Enable Security Keys in Intune

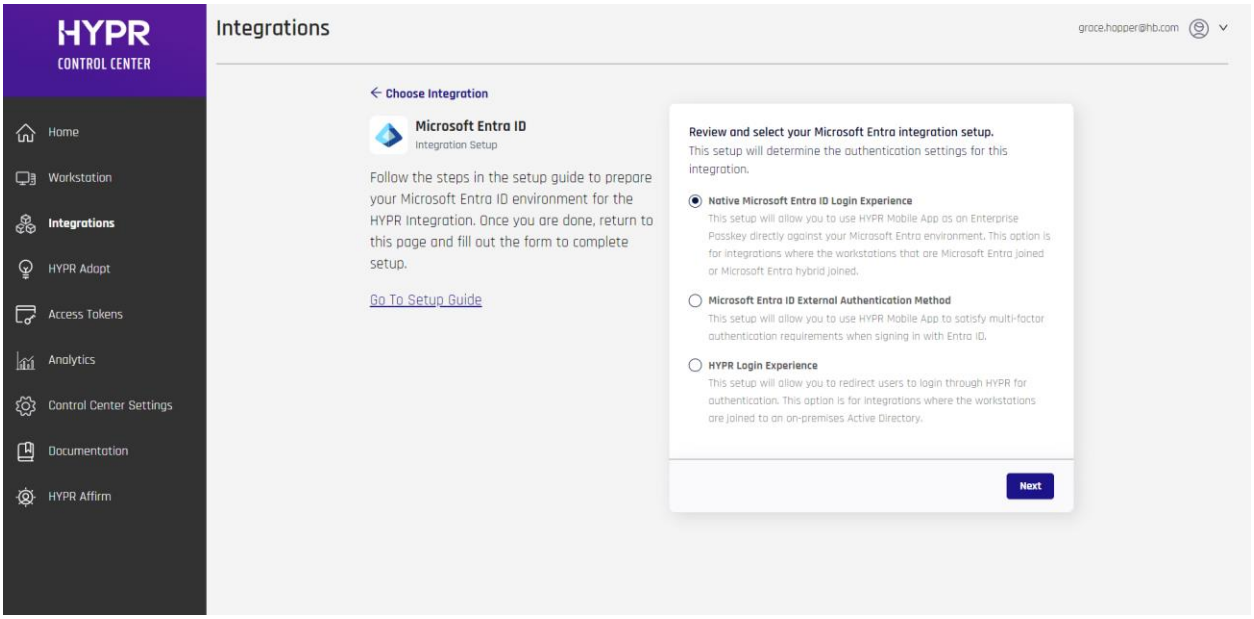
Once security keys are enabled in Entra, you must set a policy in Intune (i.e., Endpoint Manger) which will allow for security key login on Windows OS. Follow Microsoft's instructions on setting up Intune policies for security key-enabled logins.

Setting Up the HYPR Tenant

When up and running, make sure HYPR has enabled the necessary features to support HYPR Enterprise Passkeys.

To install a new Enterprise Passkeys integration in Control Center:

1. On a new tenant, navigate to **Integrations > Add New Integrations > Microsoft Entra ID**.
2. You will be prompted to select your login experience. For the FIDO2 Mobile Authenticator, select **Native Microsoft Entra Login Experience**, and click **Next**.



3. You are presented a form which contains the HYPR Application Name and all of the Entra-related data needed for HYPR to connect to the Entra tenant. These are the items created/captured above; **complete the fields as follows**:

Microsoft Entra ID
Identity Provider

User Management | Audit Trail | Login Settings | **Integration Settings**

Integration Settings

Integration Status

● **ENABLED**

This integration is enabled. If disabled, all users with a Microsoft Entra ID account in your organization will not be able to authenticate with HYPR.

Native Microsoft Entra Login Experience

This setup will allow you to use HYPR Mobile App as an Enterprise Passkey directly against your Microsoft Entra environment. This option is for integrations where the workstations that are Microsoft Entra joined or Microsoft Entra hybrid joined. For more information view docs.

Disable

Application Name

HYPR Native Passkeys

The web account name as it will appear in mobile device and PUSH notifications

Tenant ID

c45fdf2d-fcb1-4c61-ac0c-ec7f865eccdc

The global tenant ID defined by Microsoft Entra ID

Client ID

107329c7-4b76-4c4b-9a68-bed57969df3d

The custom HYPR application's client ID (also referred to as Application ID in Microsoft Entra ID)

Client Secret

••••••••••••••••••••

The Client secret which was generated for the Client ID provided above

Client Certificate

Client Certificate

Provide the PEM-encoded certificate to authenticate requests using the certificate-based method.

Client Private Key

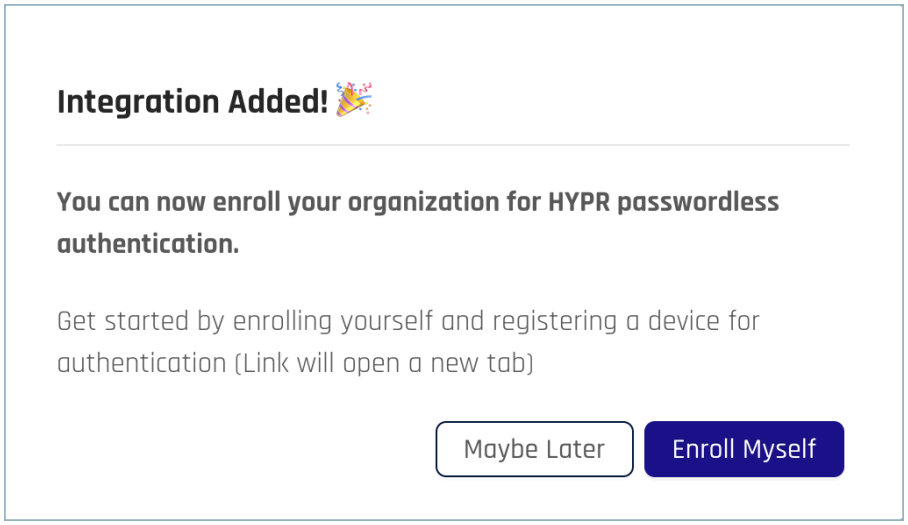
Client Private Key

Provide the PEM-encoded private key to authenticate requests using the certificate-based method.

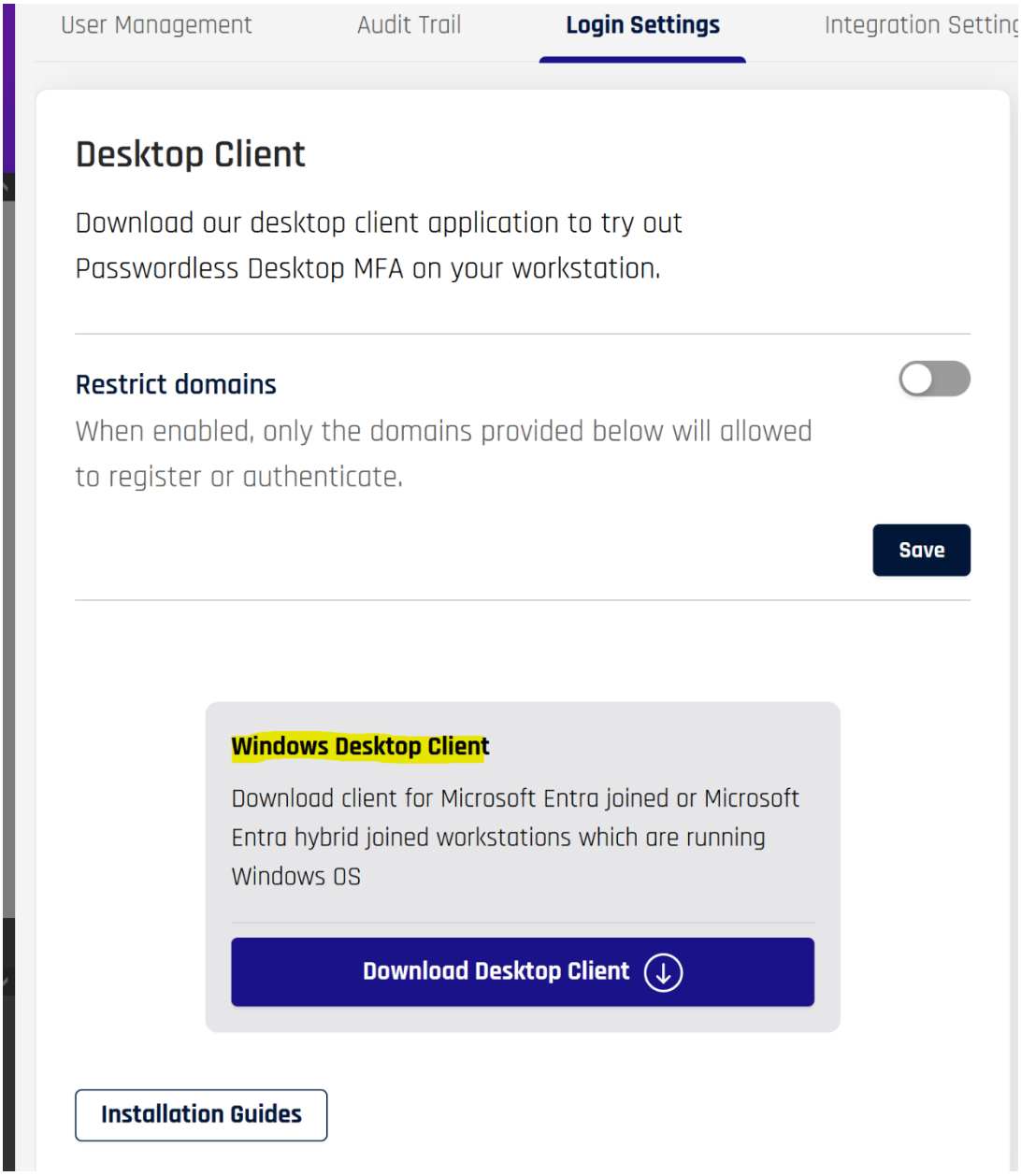
Update Integration

- *Application Name*: Only alphanumeric, spaces, dash, underscores, or trailing - or _ are allowed; this is the same validation rule for all HYPR RP Application names (rpAppId); the namespace is limited to 23 characters
- *Tenant ID*: The ID of the tenant
- *Client ID*: The ID of the client/application in Entra AD
- *Client Secret*: The secret associated with the client/application **OR**
- *Client Certificate*
- *Client private Key*

4. When you are finished, click **Add Integration**; if *Add Integration* is successful, it confirms all of the parameters provided were validated and HYPR can now connect to Entra, You will be presented a popup box. Click **Maybe Later**.



5. Navigate to the Login Settings Tab and download the Windows Desktop Client



Note: Starting 10.1, there is no toggle switch for Fido Gateway, BLE and Wi-Fi in the Login Settings Tab

Additional:

Enabling FIDO2 Passwordless Security Key on Windows

FIDO2 security key sign-in to Windows - Microsoft Entra ID | Microsoft Learn

Three ways of enabling security key sign-in on Windows 10 & Windows 11 | by Jonas Markström | Medium

*Registration

1 EPK registration.mp4

*Authentication

2 authentication.mp4

*Offline PIN Login

3 offline pin EPK.mp4

*Web login

4 browser EPK login.mp4