

# 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
```

```
C:\Users\ndoiphode>dsregcmd /status

+-----+
| Device State |
+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DomainJoined : NO
Device Name : NDOIPHODE-WIN10
```

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



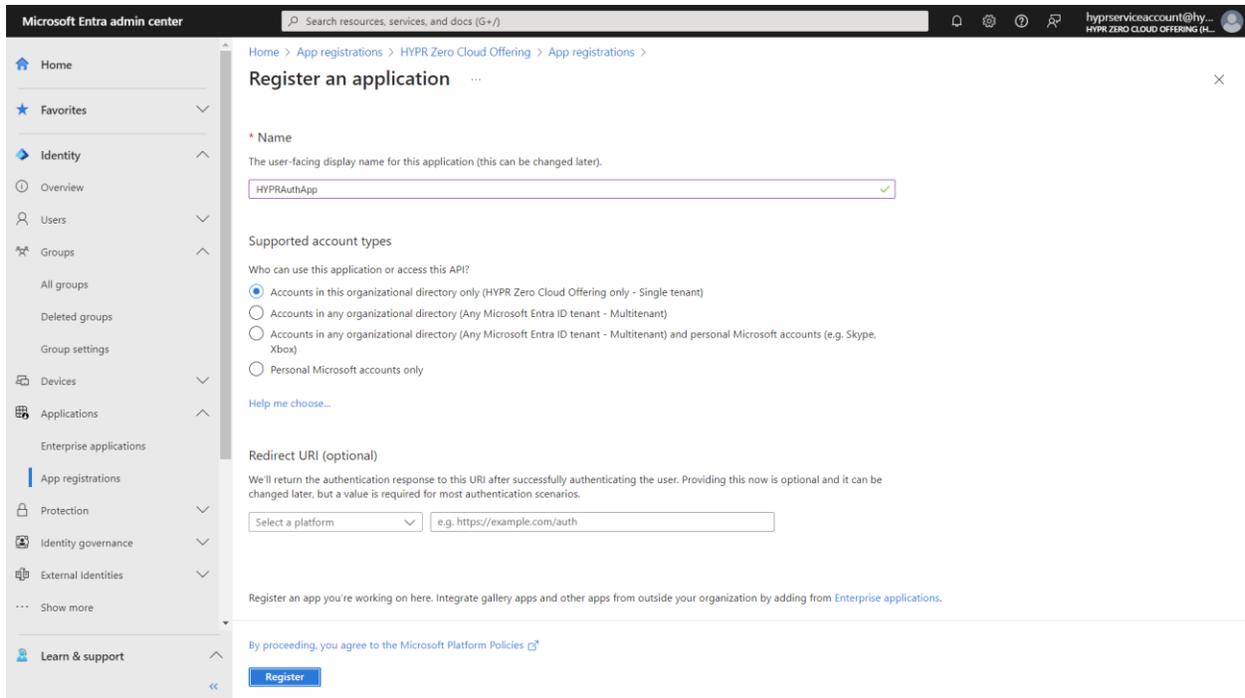
EPK App registration  
first iteration.ps1

**Note: Change the app name to match required by HYPR**

**OR via User interface**

### Register Application

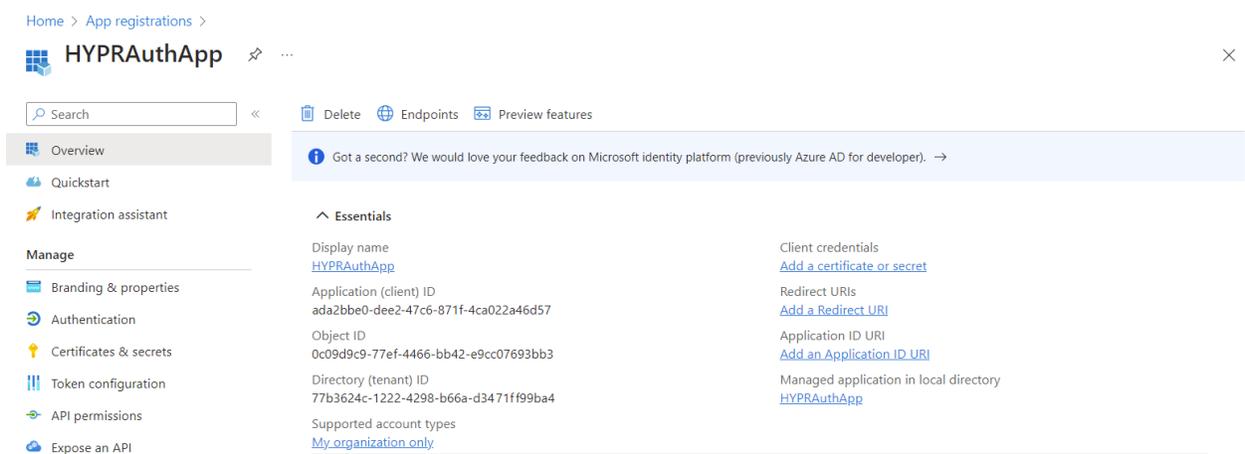
1. From the Home screen, select **Entra Active Directory > App registrations > New registration**.



## 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"

Home > App registrations > HYPRAuthApp

Search [ ] Delete Endpoints Preview features

**Overview**

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties

**Essentials**

Display name	: HYPRAuthApp	Client credentials	: 0 certificate, 5 secret
Application (client) ID	: 107329c7-4b76-4c4b-9a68-bed57969df3d	Redirect URIs	: 7 web, 0 spa, 0 public client
Object ID	: 92cdbea2-2750-451e-8780-9aa17e840d68	Application ID URI	: api://107329c7-4b76-4c4b-9a68-bed57969df3d
Directory (tenant) ID	: c45fdf2d-fcb1-4c61-ac0c-ec7f865eccdc	Managed application in L...	: Postman
Supported account types	: My organization only		

Home > App registrations > HYPRAuthApp

HYPRAuthApp | Authentication

Search [ ] Got feedback?

**Overview**

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication**
    - Certificates & secrets
    - Token configuration
    - API permissions

**Platform configurations**

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

[Add a platform](#)

**Web**

**Redirect URIs**

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating. The URIs you send in the request to the login server should match one listed here. Also referred to as reply URIs. [Learn more](#)

**Configure platforms**

Web applications

- Web**  
Build, host, and deploy a web server application. .NET, Java, Python
- Single-page application**  
Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications

- iOS / macOS**  
Objective-C, Swift, Xamarin
- Android**  
Java, Kotlin, Xamarin

---

# 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](#)



---

[Configure](#)

[Cancel](#)

---

## Grant Required API Permissions

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

... > Manage tenants > HYPR Zero Cloud Offering > HYPR Zero Cloud Offering > HYPR Zero Cloud Offering > App registrations > HYPRAuthApp >

### App registrations

+ New registration | Endpoints | Troubleshooting | Refresh | Download | Preview features | Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications | Owned applications | Deleted applications

Start typing a display name or application (client) ID to filter these r... | Add filters

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
HYPRAuthApp	...	5/31/2023	Current

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.

Search

Refresh | Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

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](#)

+ Add a permission  Grant admin consent for HYPR Zero Cloud Offering

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

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

### Remove permission

This scope is required for proper application functionality.

Are you sure you want to remove Microsoft Graph – User.Read from the configured permissions for HYPRAuthApp?

Yes, remove

Cancel

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

Search

Refresh | Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

### Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs



#### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



#### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal



#### Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs

More Microsoft APIs



#### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud



#### Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams



#### Azure Cosmos DB

Fast NoSQL database with open APIs for any scale.

5. Select **Delegated permissions**.

## Request API permissions



[< All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

### 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



> DeviceManagementRBAC

> DeviceManagementServiceConfig

▼ Directory (1)

<input checked="" type="checkbox"/>	Directory.AccessAsUser.All ⓘ Access directory as the signed in user	Yes
<input type="checkbox"/>	Directory.Read.All ⓘ Read directory data	Yes
<input type="checkbox"/>	Directory.ReadWrite.All ⓘ Read and write directory data	Yes
<input type="checkbox"/>	Directory.Write.Restricted ⓘ Manage restricted resources in the directory	Yes

> DirectoryRecommendations

> Domain

> EAS

> eDiscovery

Add permissions

Discard

## Select permissions

UserAuth

**i** 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](#)

Permission	Admin consent required
✓ UserAuthenticationMethod (1)	
<input type="checkbox"/> UserAuthenticationMethod.Read ⓘ Read user authentication methods.	Yes
<input type="checkbox"/> UserAuthenticationMethod.Read.All ⓘ Read all users' authentication methods	Yes
<input type="checkbox"/> UserAuthenticationMethod.ReadWrite ⓘ Read and write user authentication methods	Yes
<input checked="" type="checkbox"/> UserAuthenticationMethod.ReadWrite.All ⓘ Read and write all users' authentication methods.	Yes

Add permissions

Discard

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

Refresh | Got feedback?

 You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

 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 for all 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](#)

+ Add a permission  Grant admin consent for hydrZeroP2

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2) <span>...</span>				
<a href="#">Directory.AccessAsUser.All</a>	Delegated	Access directory as the signed in user	Yes	 Not granted for hydrZer... <span>...</span>
<a href="#">UserAuthenticationMethod.Reac</a>	Delegated	Read and write all users' authentication methods.	Yes	 Not granted for hydrZer... <span>...</span>

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

Refresh | Got feedback?

### Grant admin consent confirmation

Do you want to grant admin consent for the requested permissions for all accounts in hydrZeroP2? This will update any existing admin consent records this application already has.

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](#)

+ Add a permission  Grant admin consent for hydrZeroP2

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2) <span>...</span>				
<a href="#">Directory.AccessAsUser.All</a>	Delegated	Access directory as the signed in user	Yes	 Not granted for hydrZer... <span>...</span>
<a href="#">UserAuthenticationMethod.Reac</a>	Delegated	Read and write all users' authentication methods.	Yes	 Not granted for hydrZer... <span>...</span>

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

\*\*\*\*Updated Permissions 10.1

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](#)

+ Add a permission    ✓ Grant admin consent for HYPR CORP

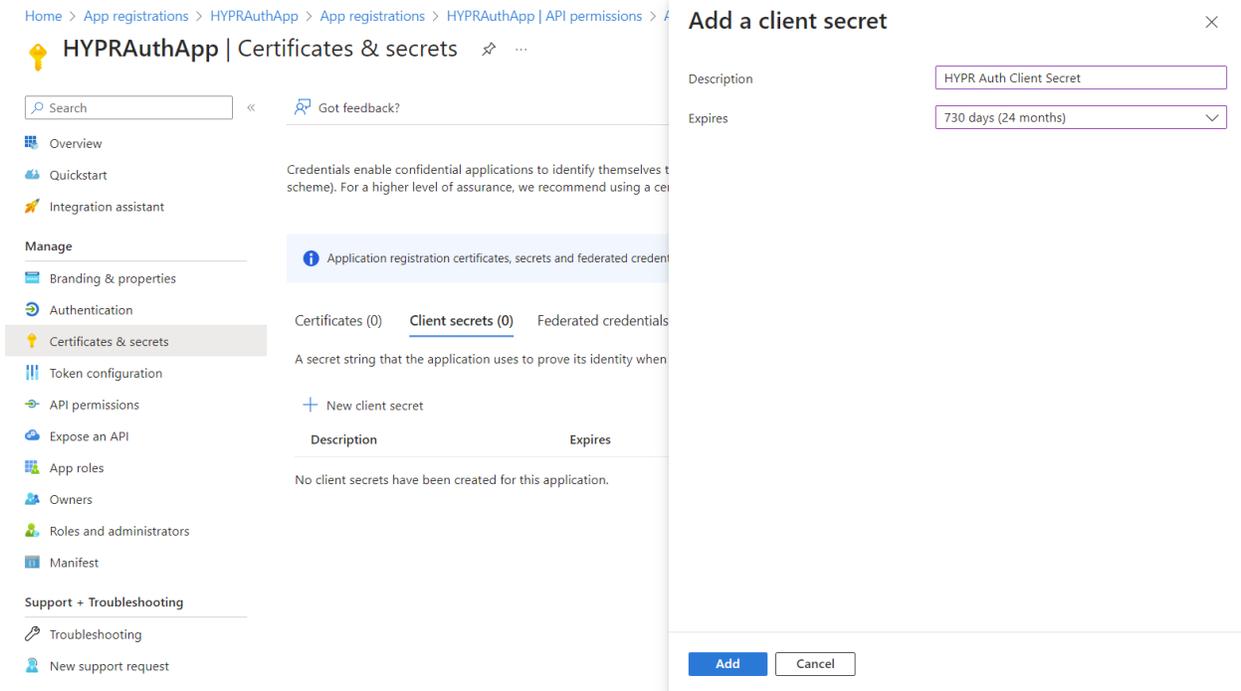
API / Permissions name	Type	Description	Admin consent req...	Status
∨ Microsoft Graph (4) <span style="float: right;">...</span>				
<a href="#">Directory.AccessAsUser.All</a>	Delegated	Access directory as the signed in user	Yes	✓ Granted for HYPR CORP <span style="float: right;">...</span>
<a href="#">Directory.ReadWrite.All</a>	Application	Read and write directory data	Yes	✓ Granted for HYPR CORP <span style="float: right;">...</span>
<a href="#">UserAuthenticationMethod</a>	Delegated	Read and write all users' authentication methods.	Yes	✓ Granted for HYPR CORP <span style="float: right;">...</span>
<a href="#">UserAuthenticationMethod</a>	Application	Read and write all users' authentication methods	Yes	✓ Granted for HYPR CORP <span style="float: right;">...</span>

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

## 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

Search x << Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

**Certificates (0)** Client secrets (5) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
No certificates have been added for this application.				

## Enable Security Keys in the Entra Tenant

1. **Login** to [entra.microsoft.com](https://entra.microsoft.com) as a global admin account.
2. Navigate to **Entra Active Directory > Security > Authentication methods**.  
Click **FIDO2 security key**.

Home > HYPR Zero Cloud Offering | Security > Security | Authentication methods >

**Authentication methods | Policies** ...

HYPR Zero Cloud Offering - Microsoft Entra ID Security

Search x << Got feedback?

**Manage**

- Policies**
- Password protection
- Registration campaign
- Authentication strengths
- Settings

**Monitoring**

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)

**Manage migration** On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. [Learn more](#)

[Manage migration](#)

Method	Target	Enabled
<b>FIDO2 security key</b>	All users	Yes
Microsoft Authenticator		No
SMS		No
Temporary Access Pass		No
Hardware OATH tokens (Preview)		No
Third-party software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No

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**.

## FIDO2 security key settings ...



FIDO2 security keys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more.](#)  
FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target Configure

Enable

Include Exclude

Target  All users  Select groups

Name	Type	Registration
All users	Group	Optional

Save

Discard

- 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*.

## FIDO2 security key settings ...

FIDO2 security keys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more.](#)  
FIDO2 keys are not usable in the Self-Service Password Reset flow.

Enable and Target Configure

### GENERAL

Allow self-service set up  Yes  No

Enforce attestation  Yes  No

### KEY RESTRICTION POLICY

Enforce key restrictions  Yes  No

Restrict specific keys  Allow  Block

[Add AAGUID](#)

No AAGUIDs have been added.

## Enable Security Keys in Intune

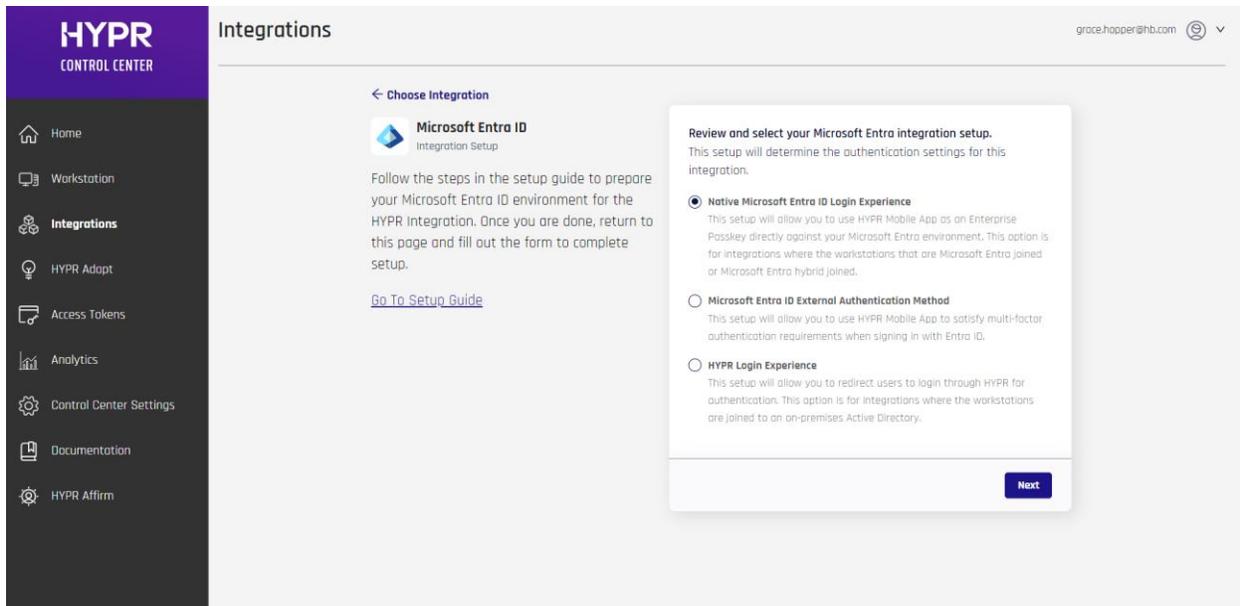
Once security keys are enabled in Entra, you must set a policy in Intune (i.e., Endpoint Manger) which will allow for security key login on Windows OS. Follow Microsoft's instructions on setting up Intune policies for security key-enabled logins.

## 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:**



## 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**.

**Integration Added!** 🎉

---

**You can now enroll your organization for HYPR passwordless authentication.**

Get started by enrolling yourself and registering a device for authentication (Link will open a new tab)

[Maybe Later](#) [Enroll Myself](#)

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

The screenshot shows a management console interface with four tabs: 'User Management', 'Audit Trail', 'Login Settings' (which is selected and underlined), and 'Integration Settings'. The main content area is titled 'Desktop Client' and contains the following text: 'Download our desktop client application to try out Passwordless Desktop MFA on your workstation.' Below this is a section for 'Restrict domains' with a toggle switch that is currently turned off. The text below the toggle reads: 'When enabled, only the domains provided below will allowed to register or authenticate.' A 'Save' button is located to the right of this text. At the bottom of the main content area, there is a callout box with the title 'Windows Desktop Client' (highlighted in yellow) and the text: 'Download client for Microsoft Entra joined or Microsoft Entra hybrid joined workstations which are running Windows OS'. Below this callout is a large blue button labeled 'Download Desktop Client' with a downward arrow icon. At the bottom left of the console, there is a button labeled 'Installation Guides'.

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