



Using Microsoft Entra ID as an Identity Provider (IdP) for Parallels Browser Isolation

- Parallels Browser Isolation

Configuring Microsoft Entra ID as an Identity Provider (IdP)

App Registration

1. Navigate to <https://portal.azure.com/#home>.
2. In the top Search Bar, search "App Registration".
3. On App registration, click on "New registration".
4. Provide the following values:
 - ◆ Name
 - ◆ Supported Account Type
 - ◆ Redirect URI
 - ◆ Select "Web" from the drop-down.
 - ◆ Value - <https://pbi.parallels.com/rbi/oidc/signin/callback>
5. Now Move to the Left Navigation Pane to do the following on each tab.

Certificates and Secrets

1. Navigate to the **Secret** tab.
2. Click on "New client secret".
3. Add a "Description" and set the expiration time.
4. Finally, click "Add".

Token configuration

1. "Add group claim", select group types, and click "Add".
2. Select an appropriate group type.
3. Customize token property.
4. Add Optional Claim.
5. Token Type = ID.
6. Select Claim and preferred_username in the checkbox.

API Permission

1. Add permission", then on "APIs my organization uses", then on "Microsoft Graph"
2. Click on "Delegate permission",
3. Select permission "group",
4. Select "Group".
5. Read "All"
6. Click on "Add permission"
7. Click on "Grant admin consent", then "Yes"

Owners

1. Goto Owners and Click "Add Owners"
2. Add the list of users who would be using the Parallels Browser Isolation

3. Go to the Overview section and have the following values at hand for the Next Steps on IdP Configuration on Parallels Browser Isolation
4. Discovery URL - Goto Endpoints and Copy OpenID Connect metadata document value (Format `https://login.microsoftonline.com/{tenantid}/v2.0/.well-known/openid-configuration`)
5. Client ID - Application (client) ID
6. Client Secret - Client Credentials (Also can be fetched from certificated) - Copy the Secret Value (Which is hidden)

Parallels Browser Isolation My Account

1. Goto **Dashboard** and Navigate to Parallels browser Isolation.
2. Click on **Initial Config** to navigate to the Parallels Browser Isolation Owner Portal.
3. Copy and paste the above values into the configuration section of the Admin Portal on Parallels Browser Isolation. *Note: The initial owner of the Parallels Browser Isolation will complete this step.*

Please refer to the image below:



Overview



Configuration



Admin Management

Configuration

Domain Configuration

Parallels Browser Isolation connects to your domain in order to centralize control and secure web browsing, enhances security by isolating web content in a remote environment, utilizing your domain for effective adm

Domain

pbi.parallelslab.com

Unique domain name used to identify the environment and select the OpenID Connect configuration.

IdP Configuration

Parallels Browser Isolation requires connection to an identity provider (IdP). An identity provider (IdP) functions as a digital guest list for cloud applications, managing and storing user identities. It verifies identities through various methods, such as username-password combinations, and provides user identity lists for service providers like Sign-On (SSO) to authenticate.

Discovery URL

https://login.microsoftonline.com/[Tenant ID]/v2.0/.well-known/openid-confi

Enter the URL of the discovery document of the OpenID Connect provider with which you want to connect.

Client ID

Client ID

Your client ID for connecting with identity provider.

Client secret

Client Secret

Your client secret for connecting with identity provider.

Username claim name

preferred_username

Key in the OpenId id_token which holds the username claim name.

Groups claim name

groups

Key in the OpenId id_token which holds the groups claim name.