

SSO with Passtab using Microsoft Ad Azure

These are your setup steps inside the Microsoft AD Azure Console in preparation for Passtab SSO:

Note: please replace "yoursite" with your detail ie: purplepark.passtab.com

- **SP Entity ID / Issuer:** <https://yoursite.passtab.com>
- **Redirect URL:** <https://yoursite.passtab.com/?q=samlassertion>
- **Logout URL:** <https://yoursite.passtab.com/user/logout>

Before we begin, please complete these items below:

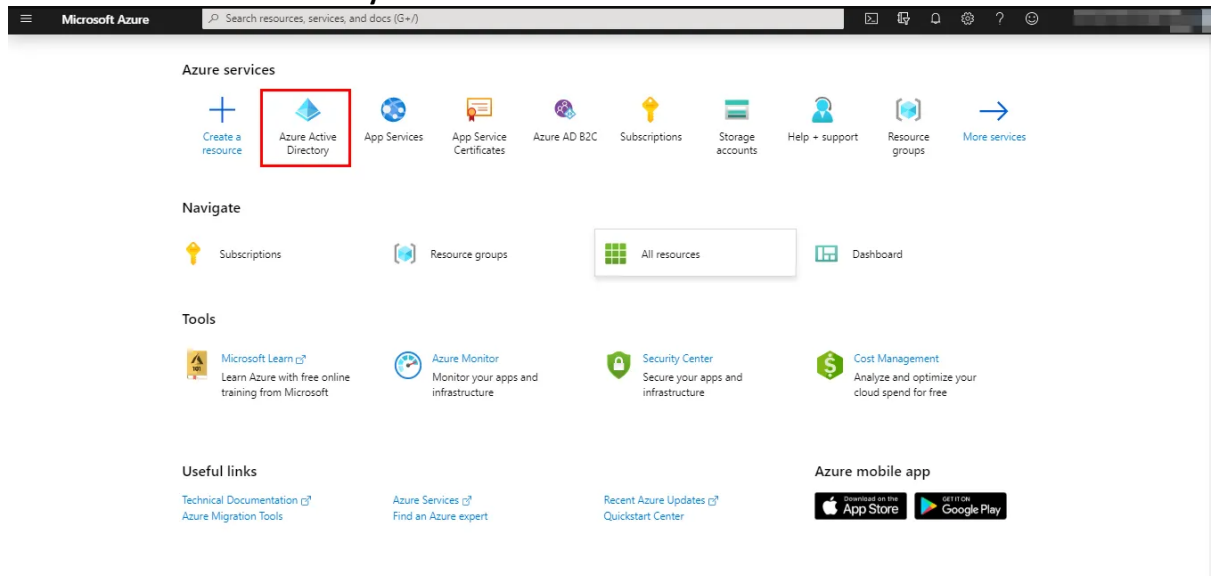
Please complete these steps: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

The custom domain you need to verify is: <https://yoursite.passtab.com>

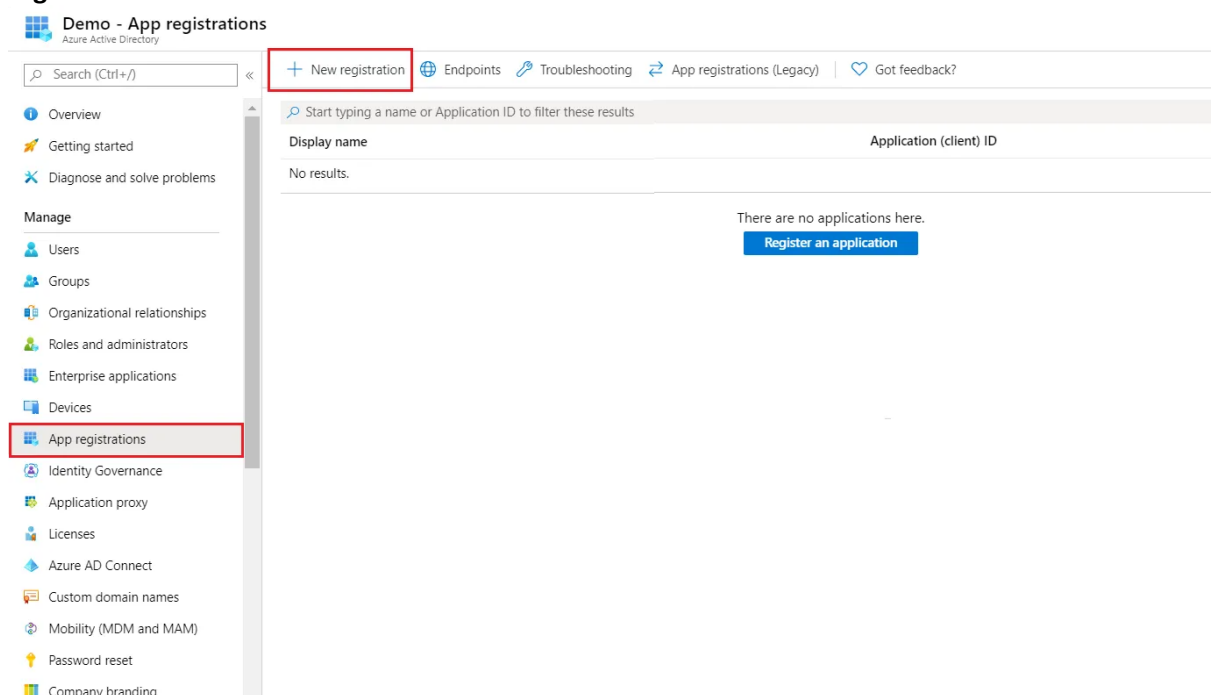
- a. Then email your Passtab contact person the TXT record.
- b. Please wait while we update our DNS with this record. This may take 1-2 days. We'll email you to advise completion.
- c. Once point b. is completed and you have been emailed, please verify the domain (instructions here: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain#verify-your-custom-domain-name>)
- d. Please email your Passtab contact that point c. is complete. We will remove the DNS record. You can proceed immediately to step 1, on the next page.

Step 1: Configuring Azure AD as Identity Provider (IdP)

- Navigate to your Azure AD portal.
- Click on **Azure Active Directory** from **Azure services**.



- In the left-hand navigation pane, click the **App registrations** service, and click **New registration**.



- Assign a Name and Redirect URI to application. Select **Web app** as **Application type** and click on **Register** button.

Home > Demo - App registrations > Register an application

Register an application

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

test

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Demo only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[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.

Web

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- You'll see the app on App Registration window. Click on **Authentication** option which will open Authentication window and then click on **Add a Platform** button under this window. Now, add **Redirect URI** and **Logout URL** and click on **Configure** button.

Home > Demo - App registrations > test - Authentication

test - Authentication

Search (Ctrl+F)

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previous)
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Save Discard Switch to the old experience Got feedback?

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

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Demo only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Advanced settings

Default client type

Treat application as a public client.
Required for the use of the following flows where a redirect URI is not used:

Yes No

Configure Web

< All platforms Quickstart Docs

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about redirect URIs and the restrictions](#)

Enter the redirect URI of the application

The value must not be empty.

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://myapp.com/logout

Implicit grant

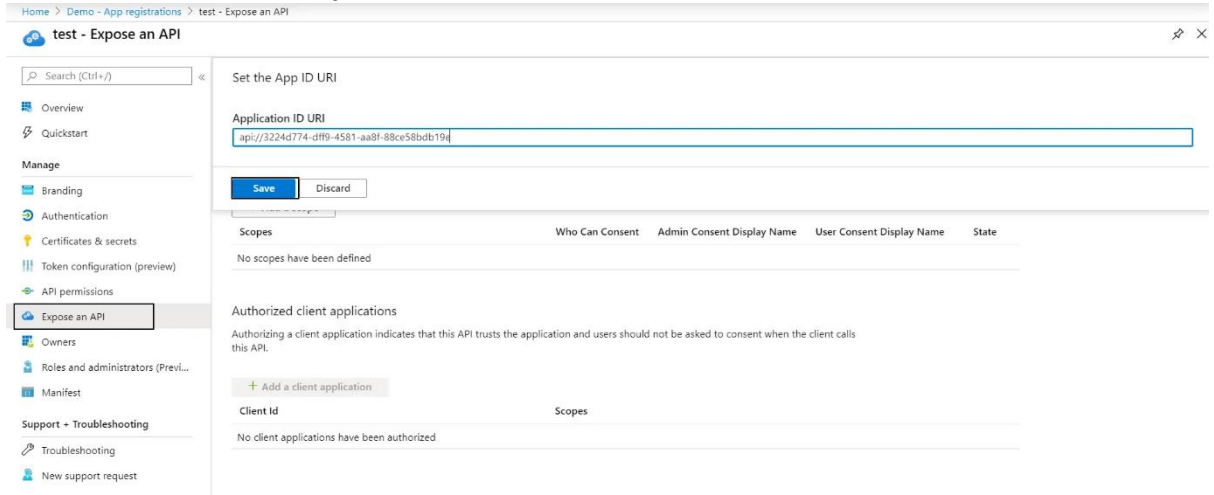
Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens
☐ ID tokens

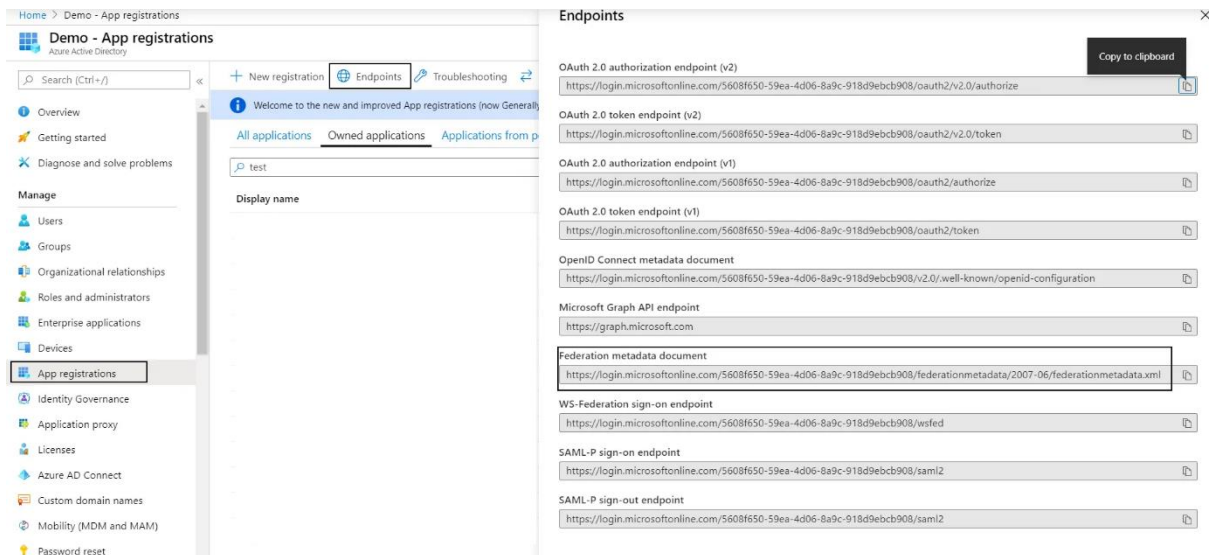
Configure **Cancel**

- Click on **Expose an API** display on the left side of Dashboard. Here change **Application ID URI** value with the **SP-Entity ID / Issuer** and save.



Step 2: Configure Application

- Click on App registrations display on the left side of Dashboard.
- Click on Endpoints on App Registration window and copy Federation Metadata Document endpoint. You can also save the metadata document by going to this endpoint. Once saved, email this metadata document back to your Passtab contact.



Step 3: Test Azure AD user

- Please set up a “test” user in your Azure AD account (if you have one already, you won’t need to do this)
- Send the details for this test user (username and password) to your contact at Passtab. This will enable us to test the SSO from our end to ensure it’s working correctly before we confirm completion.