broadvoice

b-hive Setting Up Azure AD With Broadvoice

User Guide

Table of Contents

Introduction

Broadvoice has implemented Single Sign-On with Azure Active Directory. SSO signs users into the b-hive portal using their company Azure Active Directory domain credentials when they are on their corporate devices connected to the corporate network.

This feature provides users easy access to cloud-based applications without needing any additional on-premises components. This guide will instruct administrators on how to set up Azure AD with Broadvoice

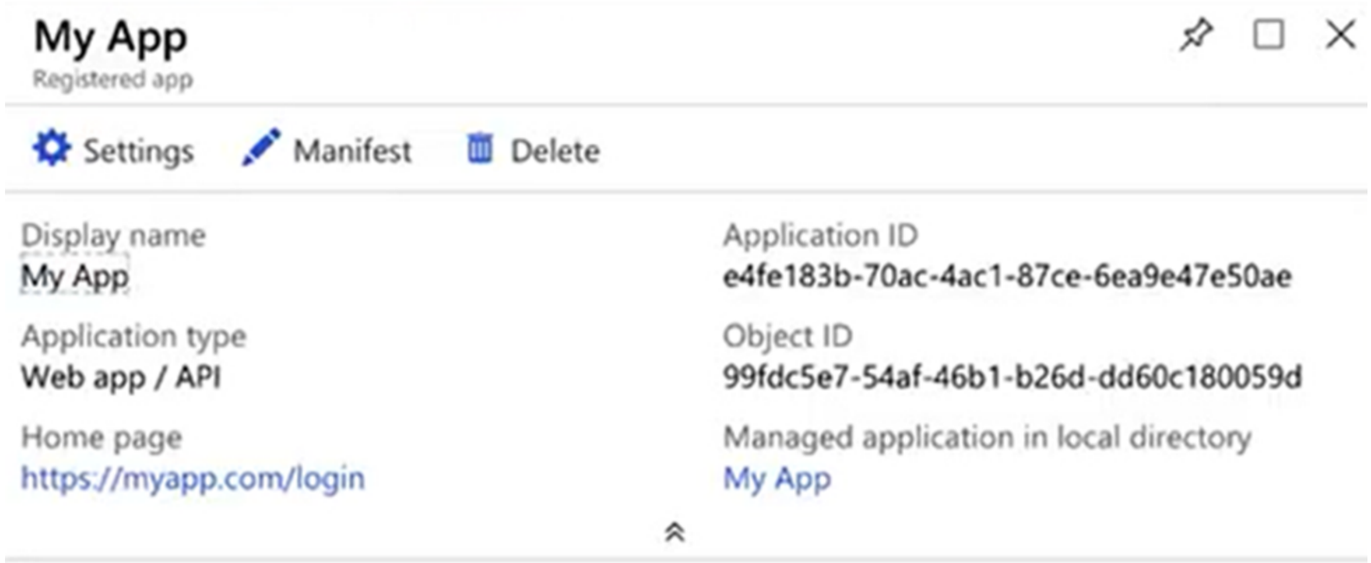
Configuration

Create an Application Registration

Open Azure Active Directory and click App Registrations
Click on New Application Registration

- Name Field: (Create a name ex. Broadvoice)
- Application Type: Web app / API
- Sign-on URL: https://login.broadvoice.com/login/callback

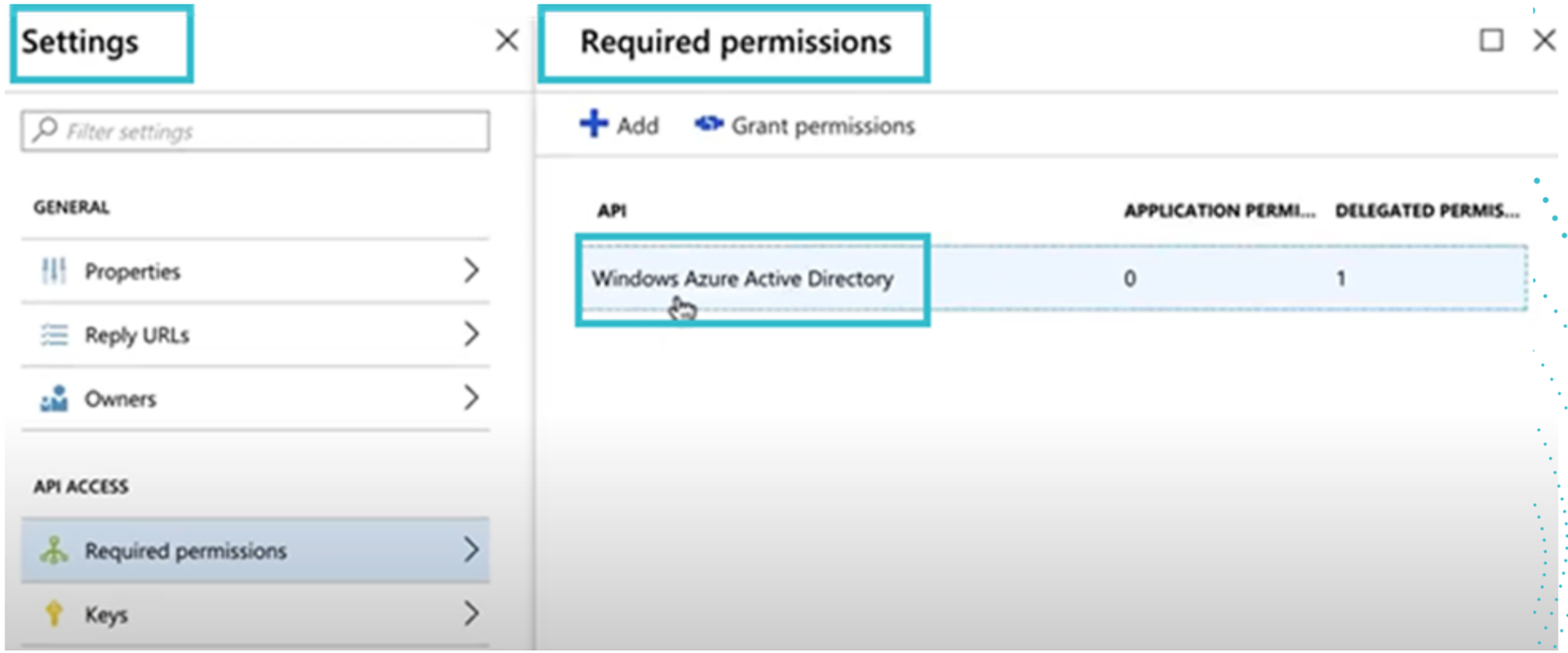
You should now have a Registered Application



Configuration

Grant Permission to The Application

- Click on Settings and go to Required permissions under API Access
- Under Required Permissions, choose Windows Azure Active Directory



Note: From the checkbox options, grant Sign in and read user profile and Read directory data.

Configuration

Create a Key to Use as The Client's Secret

- Under Settings, choose Keys under API Access
- Under Passwords, enter a Description and Expiry Time. (Expiry time can be Never).
- Choose Save, the key value will appear. Copy that value It will not be visible again after you leave the keys page.

Set Reply URLs

- You should see the URL we specified at the start: https://login.broadvoice.com/login/callback
- Add the following URL - https://broadvoice.us.auth0.com/login/callback.

Fill Out The Following Information

From your Azure AD setup, provide the following information:

- Application ID: This is the application ID received when the app was registered in step 1.
- Client Secret: This is the Secret Value copied from step 3.
- Azure AD Domain: This is in the Overview in the Azure Portal.
  Ex: authdomain.onmicrosoft.com
- Email Domains: If you have alternate or additional email domains that use this Azure AD Domain. Ex: myapp.com

Grant Auth0 The Necessary Permissions

- Broadvoice is not an administrator on your Azure AD system, we will get a link to be used to authorize the connection.
- Once configured, you will receive a URL to verify and authorize the connection with Broadvoice.

FAQs

How does it work?

If enabled, users will be directed to your Azure AD for authentication as long as your email address matches your Azure AD email address.

What systems can I integrate with Enterprise SSO?

Currently, Boradvoice supports Azure Active Directory.