# Azure SSO Configuration Guide

This document guides an Azure administrator through the steps necessary to set up Single Sign On (SSO) functionality via Azure with Brivo. For information and support using Azure with Brivo outside the scope detailed in this guide, please contact Microsoft.

## I Configuration

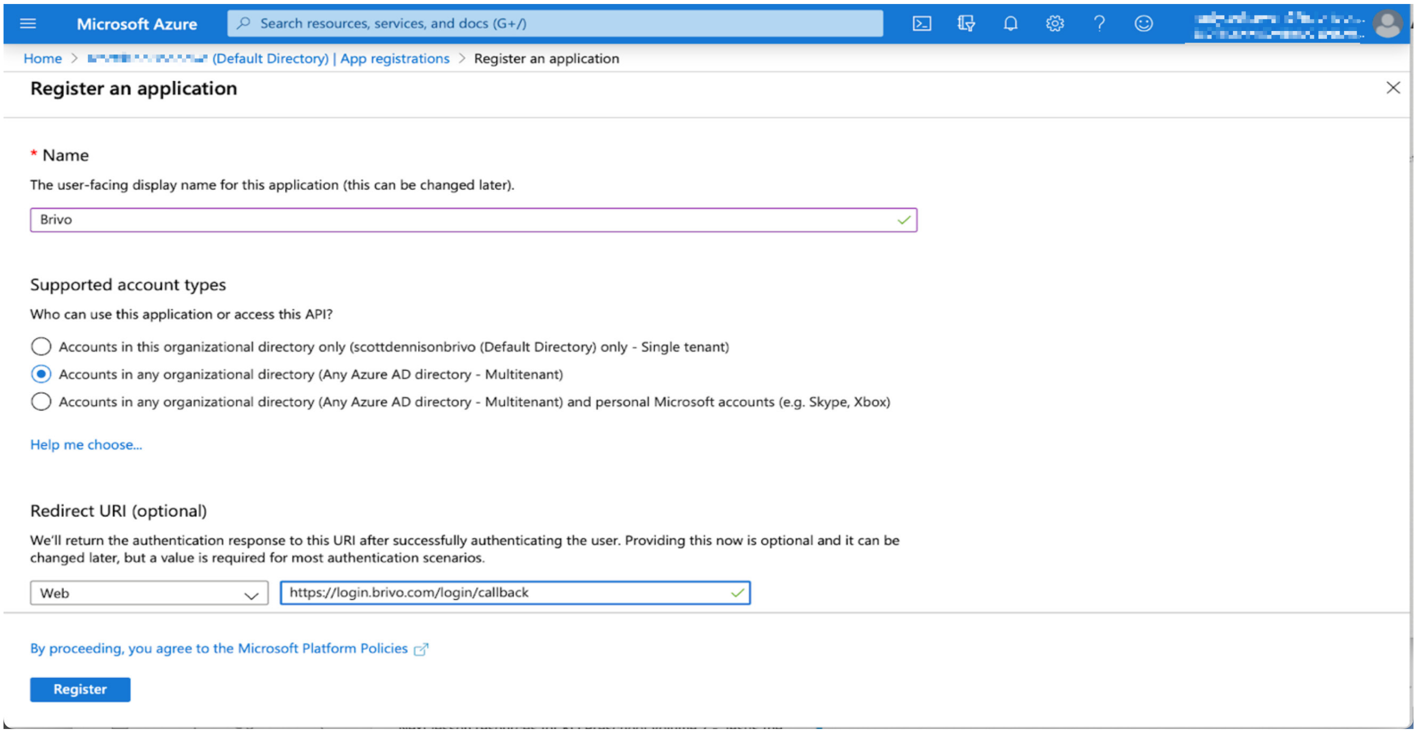
# Configuration

Brivo will need the following information to establish the Azure SSO connection:

- Microsoft Azure AD domain name
- Application (client) ID (Step 1) - See page 2 of this guide
- Application secret (Step 2) - See page 3 of this guide

## Configuring Azure for Single Sign On (SSO)

1. Login to Microsoft Azure.
2. Register the new application for Brivo.
    a. Select **App Registrations** from the left-hand navigation menu.
    b. Select **New Registration** from the action menu at the top of the page.
    c. Register a new application with the following configuration:
        i. **Name**: Brivo
        ii. **Supported account types**: Accounts in any organization directory (Any Azure AD directory - Multitenant)
        iii. **Redirect URL**: Web / https://login.brivo.com/login/callback
    d. Copy the new application's **Application (client) ID** and provide it to Brivo via the instructions on page 5.



[redacted]

Home > [redacted] (Default Directory) | App registrations > Register an application

Register an application

* Name

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

Brivo

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (scottdennisonbrivo (Default Directory) 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.

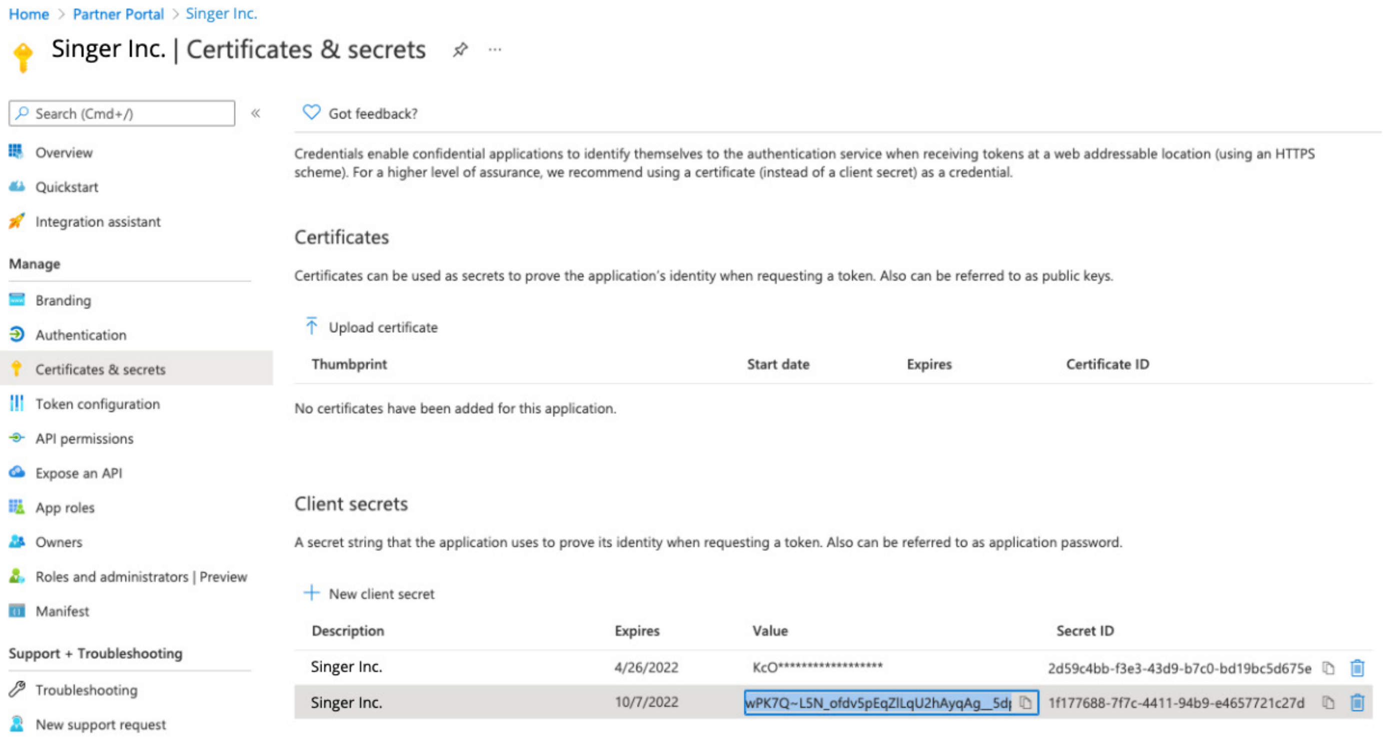
Web | https://login.brivo.com/login/callback

By proceeding, you agree to the Microsoft Platform Policies

3. Generate a new client secret for the Brivo application.

   a. Select **Certificates & secrets** from the navigation menu.

   b. Select **New client secret** and enter the desired settings.



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.

Certificates

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

| Thumbprint | Start date | Expires | Certificate ID |
|---|---|---|---|

No certificates have been added for this application.

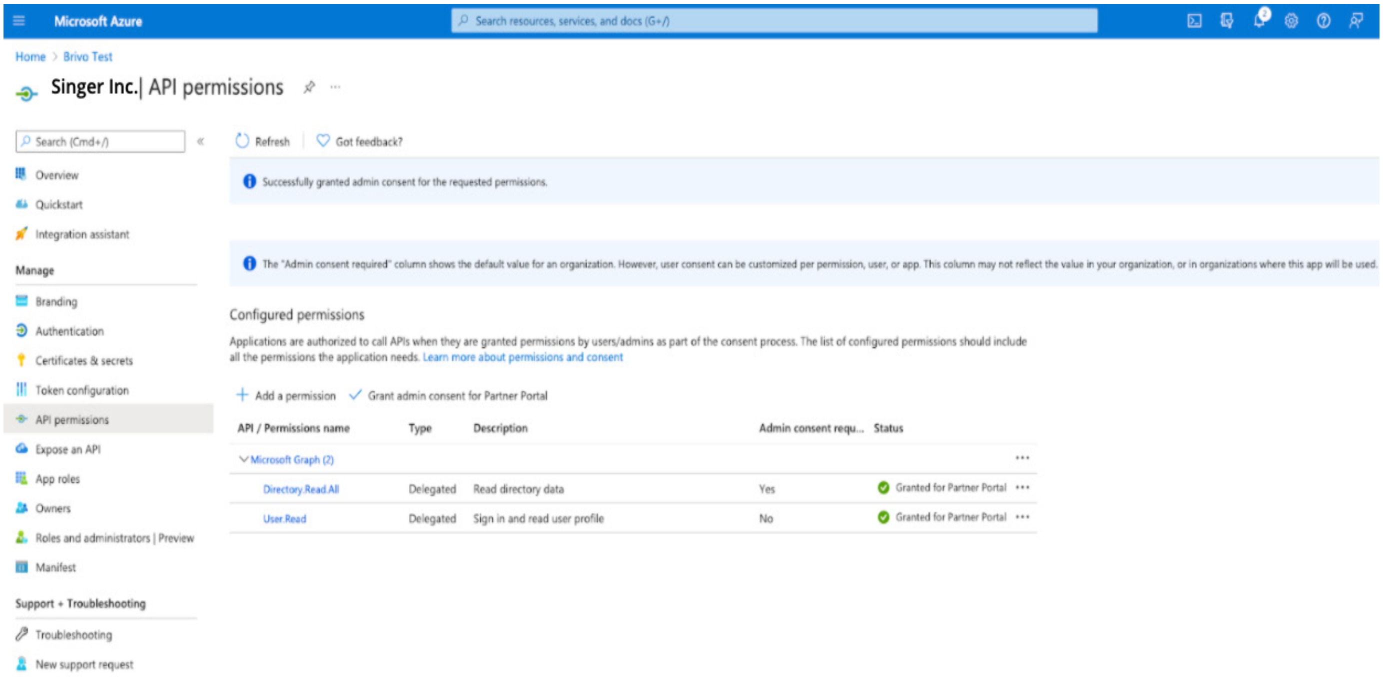
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| Description | Expires | Value | Secret ID |
|---|---|---|---|
| Singer Inc. | 4/26/2022 | KcO****************** | 2d59c4bb-f3e3-43d9-b7c0-bd19bc5d675e |
| Singer Inc. | 10/7/2022 | wPK7Q~L5N_ofdv5pEqZILqU2hAyqAg__5d| | 1f177688-7f7c-4411-94b9-e4657721c27d |

   c. Copy the security **Value** and provide it to Brivo via the instructions on page 5.

4. Add Directory.Read.All and User.Read API permissions to the application to allow Brivo to access Azure user data.
    a. Select **API permissions** from the left-hand navigation menu.
    b. Select **Add a permission**.
    c. Select **Microsoft Graph**.
    d. Select **Delegated permissions**.
    e. Under the Directory category, select **Read.All**.
    f. Under the User category, select **Read**.



Successfully granted admin consent for the requested permissions.

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.

Configured permissions

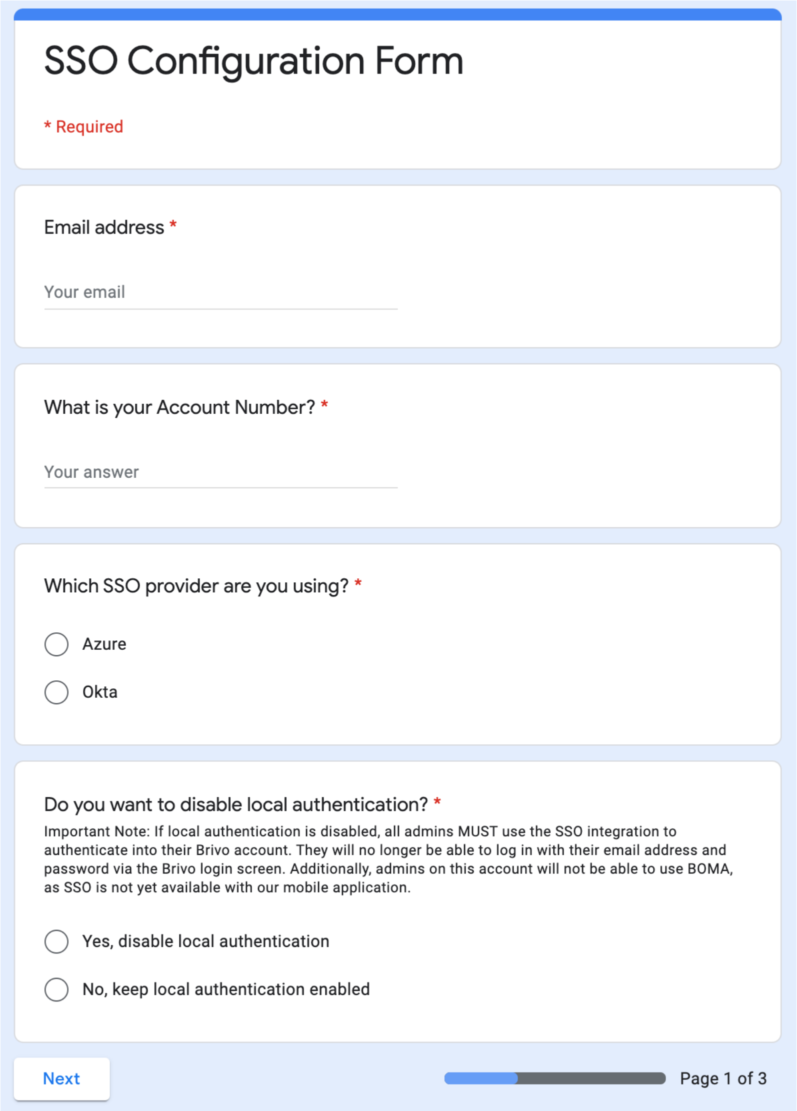
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (2) | | | | |
| Directory.Read.All | Delegated | Read directory data | Yes | Granted for Partner Portal |
| User.Read | Delegated | Sign in and read user profile | No | Granted for Partner Portal |

5. Open a browser window and go to https://forms.gle/qCbShAPGmhHTzyreA (an online fillable form).

6. Enter your **Email Address**, your **Brivo account number**, select **Azure**, select **Local Auth enabled or disabled,** and click **Next**.

**Important Note:** If Local Auth is disabled, all administrators MUST use the SSO integration to authenticate into their Brivo account. They will no longer be able to log in with their email address and password via the Brivo login screen. Additionally, administrators on this account will not be able to use Brivo Access app, as SSO is not yet available with our mobile application.



SSO Configuration Form

* Required

Email address *

Your email

What is your Account Number? *

Your answer

Which SSO provider are you using? *

○ Azure

○ Okta

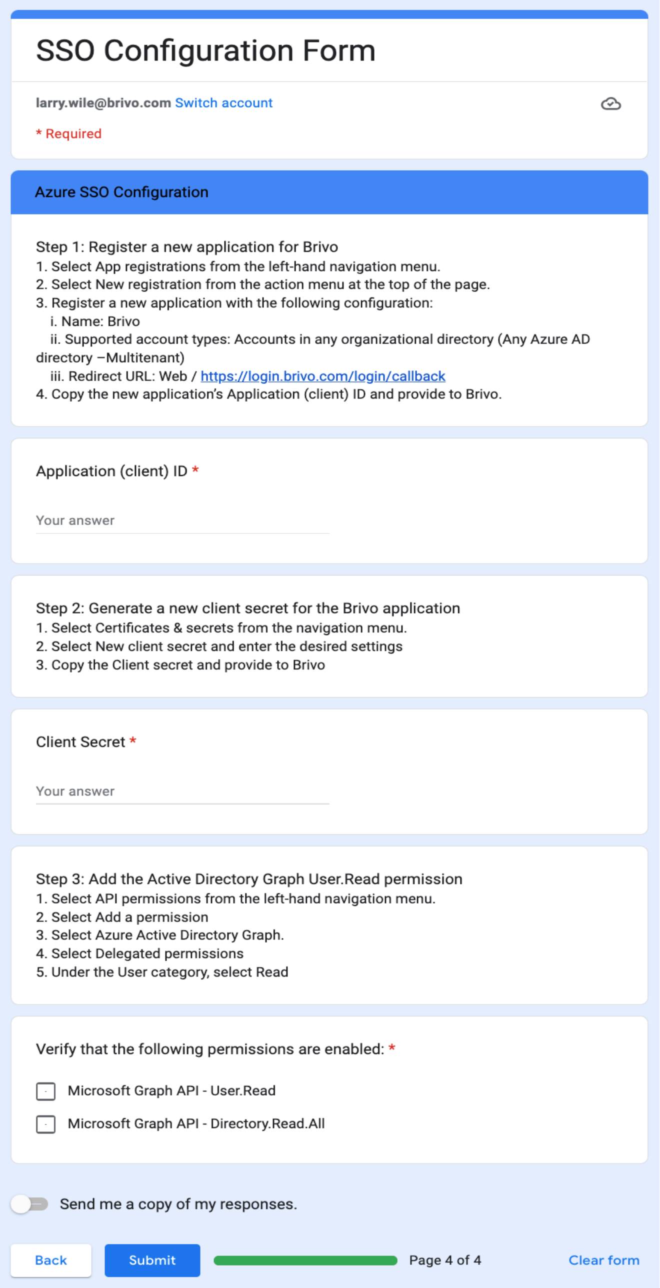
Do you want to disable local authentication? *

Important Note: If local authentication is disabled, all admins MUST use the SSO integration to authenticate into their Brivo account. They will no longer be able to log in with their email address and password via the Brivo login screen. Additionally, admins on this account will not be able to use BOMA, as SSO is not yet available with our mobile application.

○ Yes, disable local authentication

○ No, keep local authentication enabled

7. Enter the Application (client) ID from page 2 in the **Application (client) ID** field, and the Client Secret from page 3 in the **Client Secret** field. Verify that the correct permissions are enabled by checking the box **Active Directory Graph - User Read**. If you wish to have a copy of these responses sent to your email address, switch the **Send me a copy of my responses** toggle and then click **Submit**.



SSO Configuration Form

larry.wile@brivo.com Switch account

* Required

Azure SSO Configuration

Step 1: Register a new application for Brivo
1. Select App registrations from the left-hand navigation menu.
2. Select New registration from the action menu at the top of the page.
3. Register a new application with the following configuration:
   i. Name: Brivo
   ii. Supported account types: Accounts in any organizational directory (Any Azure AD directory –Multitenant)
   iii. Redirect URL: Web / https://login.brivo.com/login/callback
4. Copy the new application's Application (client) ID and provide to Brivo.

Application (client) ID *

Your answer

Step 2: Generate a new client secret for the Brivo application
1. Select Certificates & secrets from the navigation menu.
2. Select New client secret and enter the desired settings
3. Copy the Client secret and provide to Brivo

Client Secret *

Your answer

Step 3: Add the Active Directory Graph User.Read permission
1. Select API permissions from the left-hand navigation menu.
2. Select Add a permission
3. Select Azure Active Directory Graph.
4. Select Delegated permissions
5. Under the User category, select Read

Verify that the following permissions are enabled: *

□ Microsoft Graph API - User.Read

□ Microsoft Graph API - Directory.Read.All

Send me a copy of my responses.

8. All other steps concerning Azure SSO Configuration are handled by Brivo directly.

## Revision List

| Date | Version | Description |
|---|---|---|
| June 18, 2020 | 1.0 | Initial Draft |
| April 26, 2021 | 1.1 | Updates to content |
| October 27, 2021 | 1.2 | Updates to content |
| August 24, 2022 | 1.3 | Removed Onair references |
| | | |