



stick

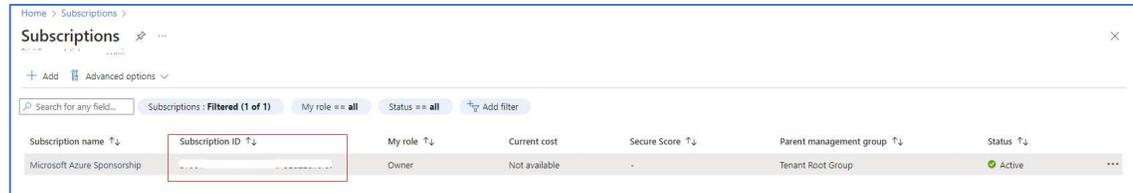
Stick

Your friendly compliance and security platform.

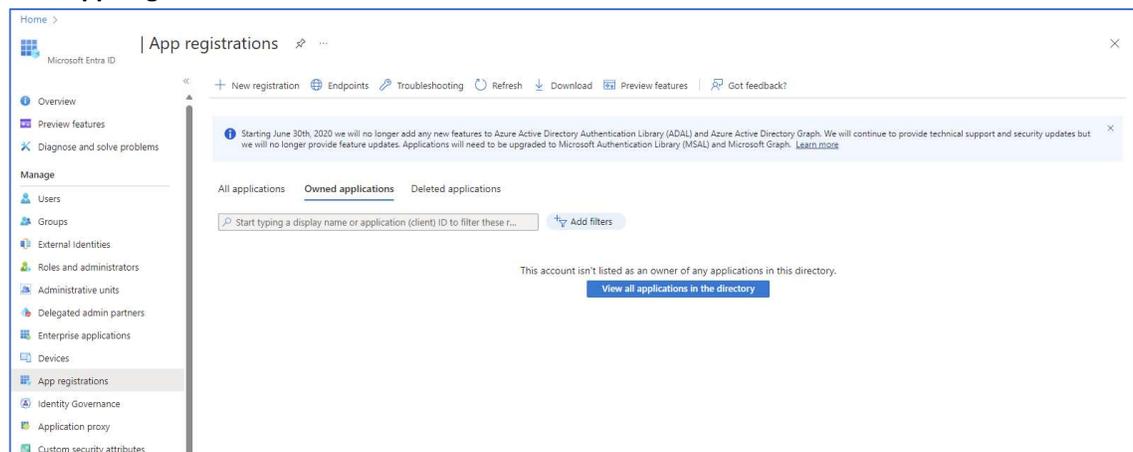
Azure Integration

Azure Integration

1. Login to the Azure Portal and access the **Subscriptions** panel. Make note of the Subscription ID that includes the resources for scanning.



2. Copy/Paste the **Subscription ID** into notepad. This value is required for Azure scanning.
3. Return to the portal home page and click **Microsoft Entra ID**.
4. Click **App Registrations**.



5. Click **New registration**.
6. Enter a name to best identify the App Registration to its purpose. Leave all other settings as their default.

Home > | App registrations >

Register an application

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

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

Accounts in this organizational directory only (StickSecure only - Single tenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[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.

Select a platform

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

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

7. Click **Register** to create the App Registration.
8. On the summary page copy/paste the **Application (client) ID** and **Directory (tenant) ID** to notepad.

Home > | App registrations >

-test-application

Search Delete Endpoints Preview features

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

Essentials

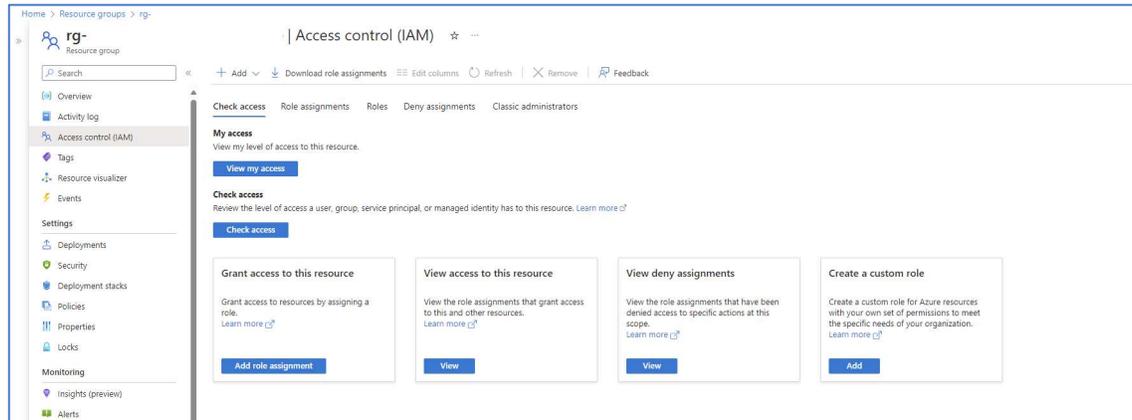
Display name	:		Client credentials	:	Add a certificate or secret
Application (client) ID	:	<input type="text" value="72121212-1212-1212-1212-121212121212"/>	Redirect URIs	:	Add a Redirect URI
Object ID	:	<input type="text" value="72121212-1212-1212-1212-121212121212"/>	Application ID URI	:	Add an Application ID URI
Directory (tenant) ID	:	<input type="text" value="72121212-1212-1212-1212-121212121212"/>	Managed application in L...	:	benjamin-test-application

Supported account types : [My organization only](#)

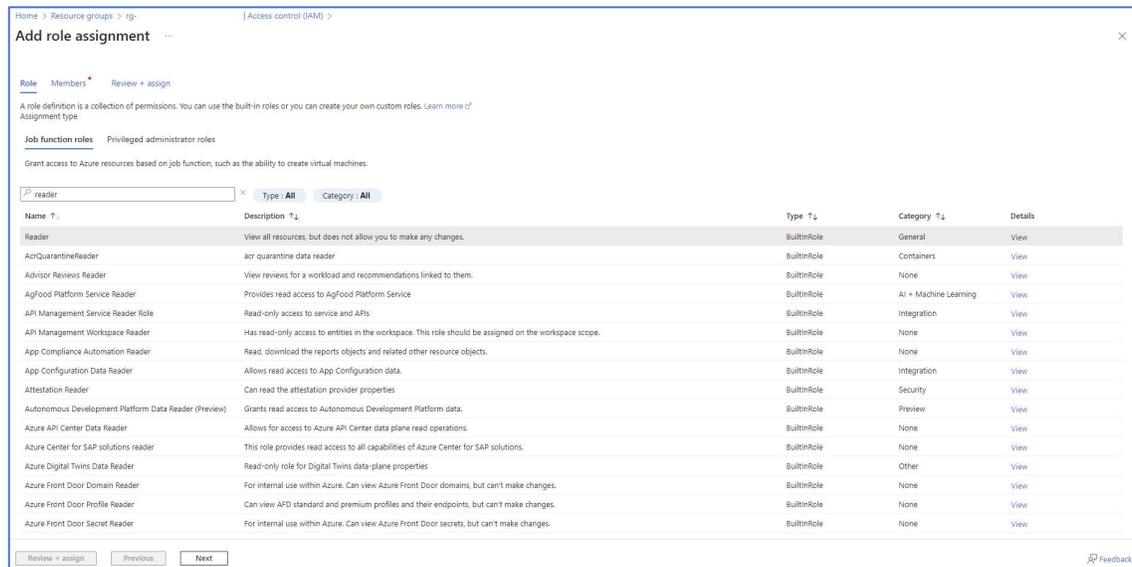
Get Started | [Documentation](#)

Build your application with the Microsoft identity platform

1. In the Azure Portal select a Resource Group to assign the App Registration profile to.
2. Click the **Access control (IAM)** link in the left panel.

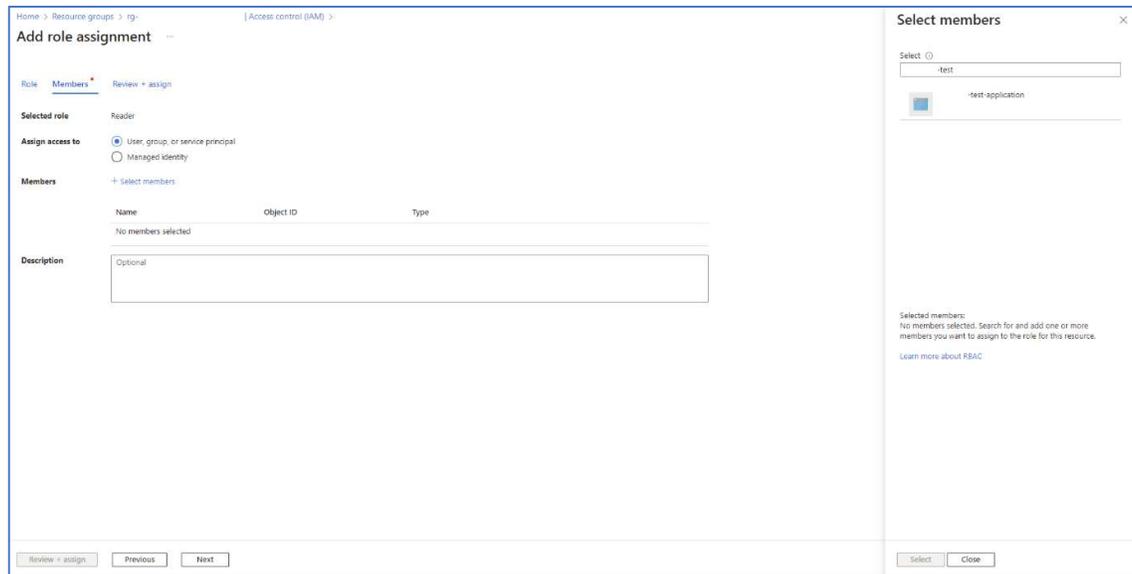


3. Click Add -> Add Role Assignment
4. Enter **Reader** in the search panel and select **Reader** from the available Job function roles.



5. Click **Next**
6. On the **Members** tab set **Assign** access value to User, group, or service principal and click **Select members**.

7. In the Select members panel search for the name of the application created above and add them to the members.



8. Click **Select**
9. Click **Review + assign**
10. This process has now set up the created Application Registration to have read permissions to the selected resource.

The copy/pasted details from above are to be used when registering a new Azure or MS 365 profile in Stick Secure. Those values are:

Subscription ID, Tenant ID, Client ID, Client Secret