

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.

+ Add II Advanced options ∨	Home > Subscriptions > Subscriptions							×
Subscription name 🐍 Subscription ID 🗘 My role 🗘 Current cost Secure Score ৃ Parent management group 🎲 Status 🎲	+ Add 👔 Advanced options	bscriptions : Filtered (1 of 1) My role == al	Status == all	च Add filter				
	Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Secure Score ↑↓	Parent management group $\uparrow \downarrow$	Status ↑↓	

- 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.

Home >		
Microsoft Entra ID	registrations 🖈 🚥	×
Overview Preview features Diagnose and solve problems	New registration Endpoints Troubleshooting Refresh Download Preview features Refresh Cot feedback? Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory (JADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Latar more	×
Manage	All applications Owned applications Deleted applications	
A Groups	P Start typing a display name or application (client) ID to filter these r	
External Identities		
Roles and administrators	This account isn't listed as an owner of any applications in this directory.	
Administrative units	View all applications in the directory	
🚸 Delegated admin partners		
Enterprise applications		
Devices		
III, App registrations		
Identity Governance		
Application proxy		
Custom security attributes		

- 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 regi	strations >
Register an applic	ation
* Name	
The user-facing display name for t	this application (this can be changed later).
Supported account types	
Who can use this application or ac	ccess this API?
 Accounts in this organization. 	al directory only (StickSecure only - Single tenant)
Accounts in any organization	al directory (Any Microsoft Entra ID tenant - Multitenant)
 Accounts in any organization Xbox) 	al directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype,
O Personal Microsoft accounts	only
Liele me cheese	
ALARD SPECIFICATION OF TAXABLE	
Redirect URI (optional)	
We'll return the authentication res	sponse to this URI after successfully authenticating the user. Providing this now is optional and it can be red for most authentication scenarios
changed later, but a value is requi	red for most address to the second
Select a platform	e.g. https://example.com/auth
Register an app you're working or	here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.
	for a finite provide a fi
by proceeding, you agree to the N	uicrozori kiariolui kolliciez (3)
Register	

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

Home > App registrations	o ication 🖉 ···		×
₽ Search «	🔋 Delete 🜐 Endpoints 💀 Preview features		
Uverview	A Eccentiale		
📣 Quickstart 💉 Integration assistant	Display name	Client credentials : <u>Add a certificate or secret</u> Referent LIR: <u>add a Refinert LIR</u>	
Manage	Object ID : diffuere buss sets ochr poperstored	Application ID URI : Add an Application ID URI	
 Branding & properties Authentication 	Directory (tenant) ID : r2101	Managed application in I : benajmin-test-application	
Certificates & secrets Token configuration	Welcome to the new and improved App registrations. Looking to learn how it's changed from the second sec	om App registrations (Legacy)? Learn more	×
 API permissions Expose an API 	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory updates but we will no longer provide feature updates. Applications will need to be upgrace	Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security led to Microsoft Authentication Library (MSAL) and Microsoft Graph. <u>Learn more</u>	×
 App roles Owners 	Get Started Documentation		
 Roles and administrators Manifest 	Build your applicatio	n with the Microsoft identity platform	



9. Click Certificates and Secrets

10. Click **New client secret** and enter a **Description** (e.g. Steampipe Scanner)

Home > App registrations >	> -test-application	Add a client secret		×
🔶 -test-applie	cation Certificates & secrets 👒 🐇			
· · · · · · · · · · · · · · · · · · ·		Description	Enter a description for this client secret	
♀ Search «	요구 Got feedback?	Expires	Recommended: 180 days (6 months)	\sim
Overview				
📣 Quickstart	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a we scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.			
🚀 Integration assistant				
Manage	Application registration certificates secrets and federated credentials can be found in the tabs below.			
📰 Branding & properties				
Authentication	Certificates (0) Client secrets (0) Federated credentials (0)			
📍 Certificates & secrets	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application			
Token configuration	A seciel string that the application uses to prove its rulentity when requesting a token. Also can be releved to as application p			
API permissions	+ New client secret			
Expose an API	Description Expires Value 🛈 Se			
10 App roles	No client secrets have been created for this application.			
A Owners				
Roles and administrators				
Manifest				

- 11. Click **Add** to create the new Client secret.
- 12. Copy/Paste the **Value** from the created Client secret into notepad. **Note**: You will not be able to retrieve this value after navigating away from the page.

O Cearch	// Cat faadhaak?					
>> Search	K Got reedback?					
 Overview Quickstart 	Got a second to give us some fee	=dback? \rightarrow				×
ntegration assistant Manage	Credentials enable confidential applica scheme). For a higher level of assuran	ations to identify themselves to ce, we recommend using a cer	o the authentication service when receiving tokens a tificate (instead of a client secret) as a credential.	a web addressable location (using an HTTPS	
Branding & properties						
Authentication	Application registration certificate	es, secrets and federated credent	ials can be found in the tabs below.			×
📍 Certificates & secrets						
Token configuration	Certificates (0) Client secrets ((1) Federated credentials	(0)			
API permissions	A secret string that the application u		requesting a token. Also can be referred to as applic	tion password.		
Expose an API						
App roles	+ New client secret		-			
Moners 2	Description	Expires	Value ①	Secret ID		
	1j	8/12/2024			D	İ
Roles and administrators						
 Roles and administrators Manifest 						
 Roles and administrators Manifest Support + Troubleshooting 						
Koles and administrators Manifest Support + Troubleshooting						

The created App Registration should now be granted access to the resources intended for scanning by Steampipe. The below are details on attaching at the resource group level. This allows the Steampipe query engine read access to all resources container within the selected resource group.



- 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.

Home > Resource groups > rg-				
» Resource group	Access control ((IAM) ☆ …		
✓ Search «	+ Add \lor \downarrow Download role assignments	🗉 Edit columns 🕛 Refresh 🗙 Remove 🌶	Feedback	
Overview Activity log	Check access Role assignments Roles	Deny assignments Classic administrators		
१०, Access control (IAM)	My access			
 Tags Resource visualizer Events 	View my level of access to this resource. View my access Check access Review the level of access a user, group, service prin	ncipal, or managed identity has to this resource. Learn n	ore a'	
Settings	Check access			
📩 Deployments				
 Security Deployment stacks 	Grant access to this resource	View access to this resource	View deny assignments	Create a custom role
 Policies Properties Locks 	Grant access to resources by assigning a role. Learn more 🖻	View the role assignments that grant access to this and other resources. Learn more P	View the role assignments that have been denied access to specific actions at this scope. Learn more and	Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization. Learn more [2]
Monitoring	Add role assignment	View	View	Add
Insights (preview)				
Alerts				

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

Home > Resource groups > rg-	Access control (IAM) >			
Add role assignment				>
3				
Role Members Review + assign				
A role definition is a collection of permissions. You can use the Assignment type	built-in roles or you can create your own custom roles. Learn more d'			
Job function roles Privileged administrator roles				
Grant access to Azure resources based on job function, such a	as the ability to create virtual machines			
₽ reader	X Type : All Category : All			
Name 🛧	Description 14	Туре ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.	BuiltInRole	None	View
AgFood Platform Service Reader	Provides read access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
API Management Service Reader Role	Read-only access to service and APIs	BuiltInRole	Integration	View
API Management Workspace Reader	Has read-only access to entities in the workspace. This role should be assigned on the workspace scope.	BuiltInRole	None	View
App Compliance Automation Reader	Read, download the reports objects and related other resource objects.	BuiltInRole	None	View
App Configuration Data Reader	Allows read access to App Configuration data.	BuiltInRole	Integration	View
Attestation Reader	Can read the attestation provider properties	BuiltInRole	Security	View
Autonomous Development Platform Data Reader (Preview)	Grants read access to Autonomous Development Platform data.	BuiltInRole	Preview	View
Azure API Center Data Reader	Allows for access to Azure API Center data plane read operations.	BuiltInRole	None	View
Azure Center for SAP solutions reader	This role provides read access to all capabilities of Azure Center for SAP solutions.	BuiltInRole	None	View
Azure Digital Twins Data Reader	Read-only role for Digital Twins data-plane properties	BuiltInRole	Other	View
Azure Front Door Domain Reader	For internal use within Azure. Can view Azure Front Door domains, but can't make changes.	BuiltInRole	None	View
Azure Front Door Profile Reader	Can view AFD standard and premium profiles and their endpoints, but can't make changes.	BuiltInRole	None	View
Azure Front Door Secret Reader	For internal use within Azure. Can view Azure Front Door secrets, but can't make changes.	BuiltInRole	None	View
Review + assign Previous Next				R Feedba

- 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.

Home > Resource grou	s > rg- Access control (IAM) >	Select members ×
Add role assig	nment	
Role Members	Review + assign	Select () -test -test -test
Selected role	Reader	-
Assign access to	User, group, or service principal	
	Managed identity	
Members	+ Select members	
	Name Object ID Type	
	No members selected	
Description	Optional	
		Selected members: No nembers selected. Search for and add one or more members you want to assign to the role for this resource. Learn more about REAC
Review + assign	Previous Next	Select Close

- 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