



Cranium Deployment Guide

Azure ML and Azure OpenAI

September 2023

Overview

This document walks through the step-by-step process of setting up and deploying a Cranium Integration to your organization's Azure Machine Learning and Azure OpenAI instances. Support is available for any questions or issues, either by emailing support@cranium.ai, or submitting a ticket on support.cranium.ai.

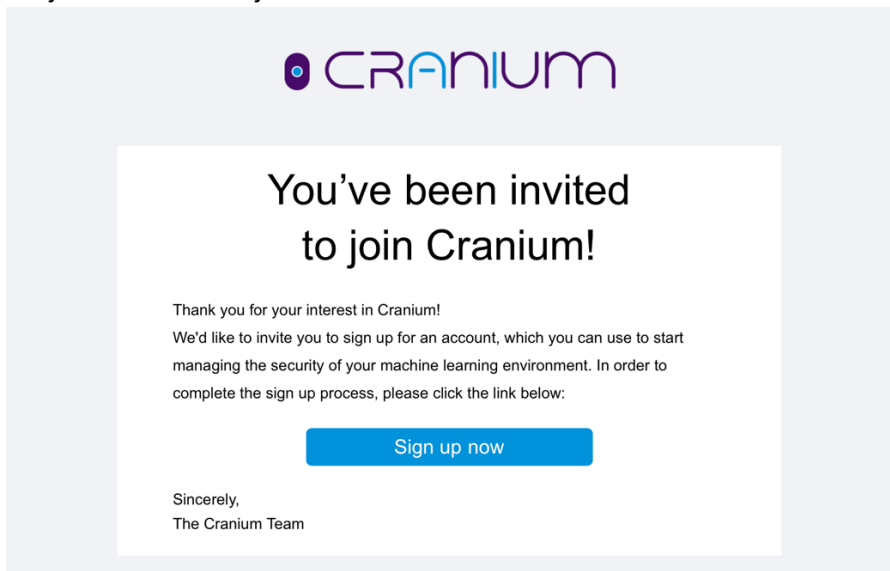
Included in this guide:

- Pre-Requisites
- Deployment Steps
- Getting Started with Cranium
- Architecture Diagram
- Asset Information Received from Connector
- Analysis Information Received from Connector

Pre-Requisites

Prior to integration, please review the following items and contact support if any items are missing.

1. Confirm that an email was sent to you or someone on your team from noreply@cranium.net with the subject "Invitation to join Cranium".

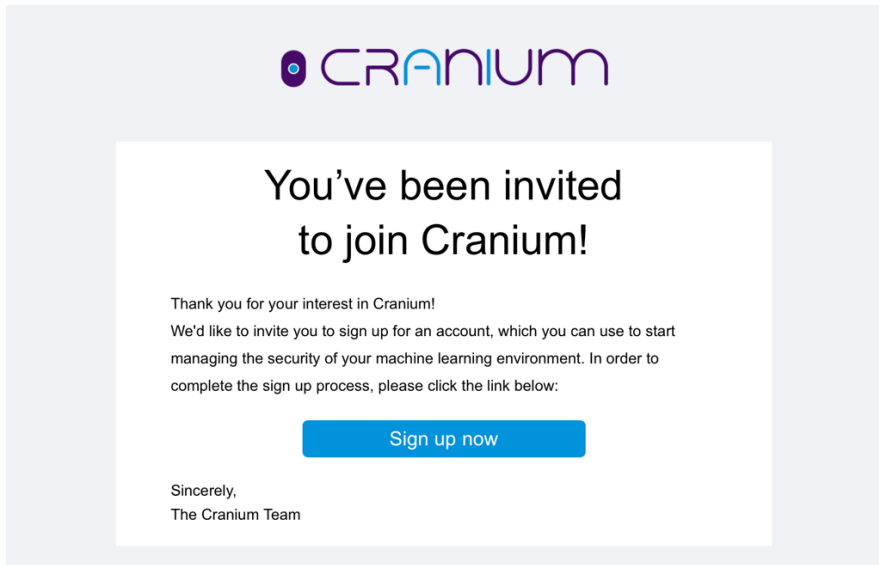


2. Azure admin privileges are needed to grant the proper API app permissions in Step 2.5 of the Cranium integration deployment.
 - a. If an Azure admin is not available at the time of the scheduled integration, Step 2 can be completed prior to the rest of the integration.
 - b. Note that the secret value created for the new App registration will need to be available at the time of deployment for Step 4.
3. Owner privileges are needed in Azure for the specific resource group, Azure OpenAI service, subscription, or management group that will be connected to the Cranium Connector.

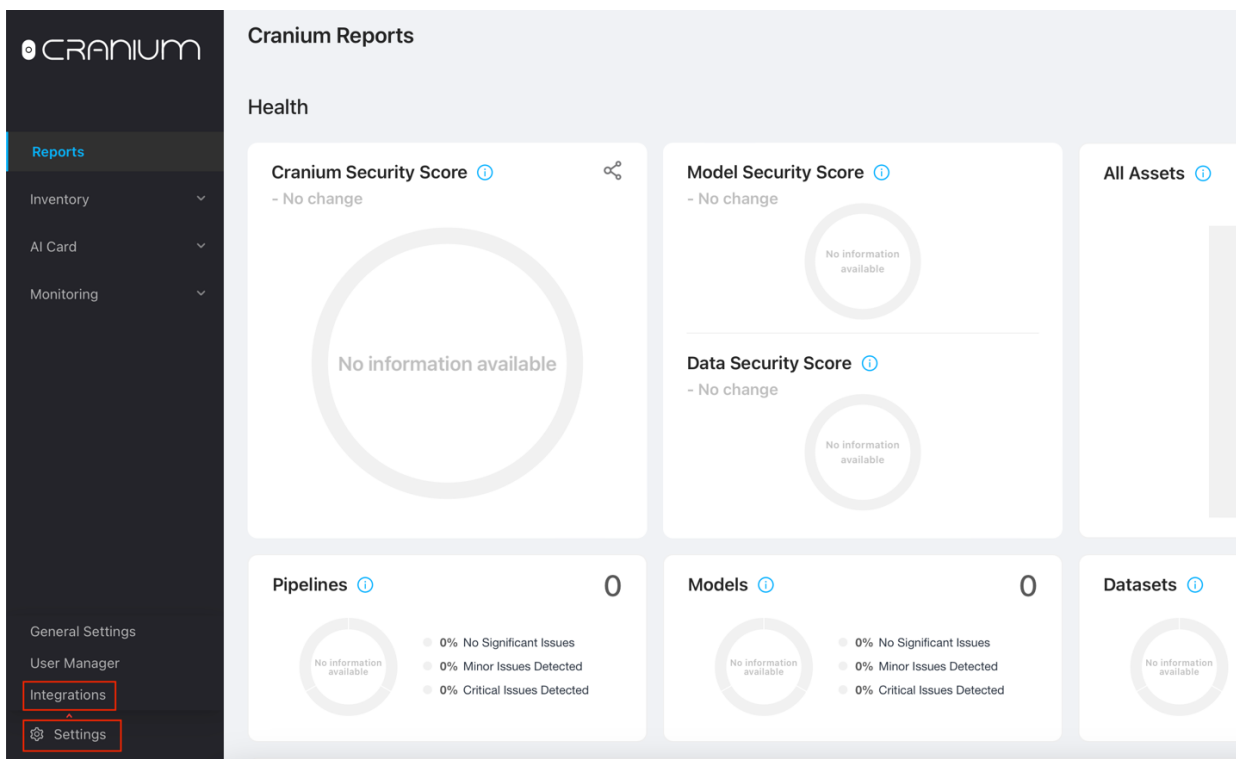
Deployment Steps

Step 1: Create an Azure ML Integration in Cranium and save the integration token

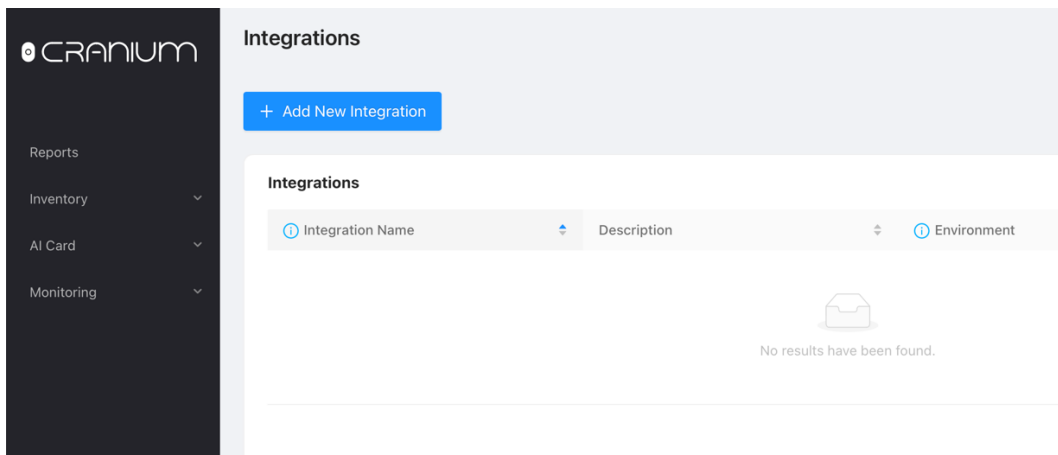
1. Login to Cranium by clicking the “Sign up now” button from your “Invitation to join Cranium” email



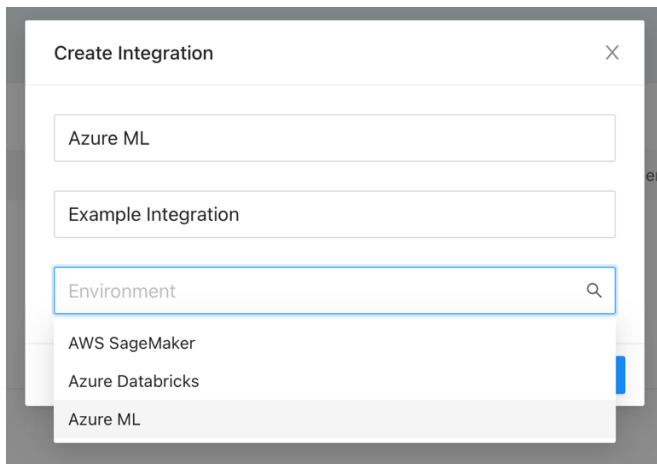
2. Complete the sign up instructions
3. Go to Settings > Integrations in the bottom left corner of the page



4. Click “Add New Integration”



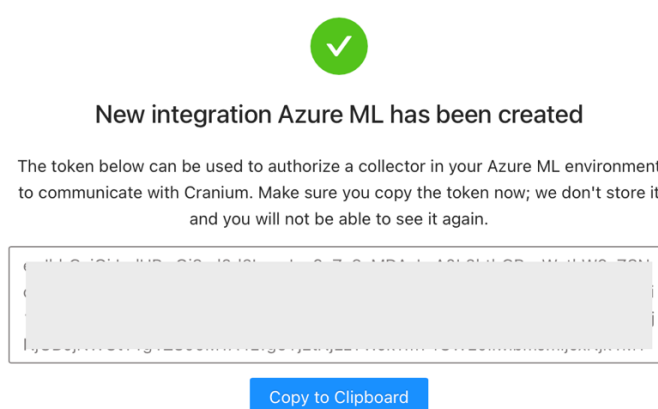
5. Give it any name and description you'd like and select “Azure ML” as the environment. (“Azure OpenAI” will be added as an option in an upcoming release)



- Note that this Environment label does not impact anything about the way the integration works and is only used as a helpful identifier

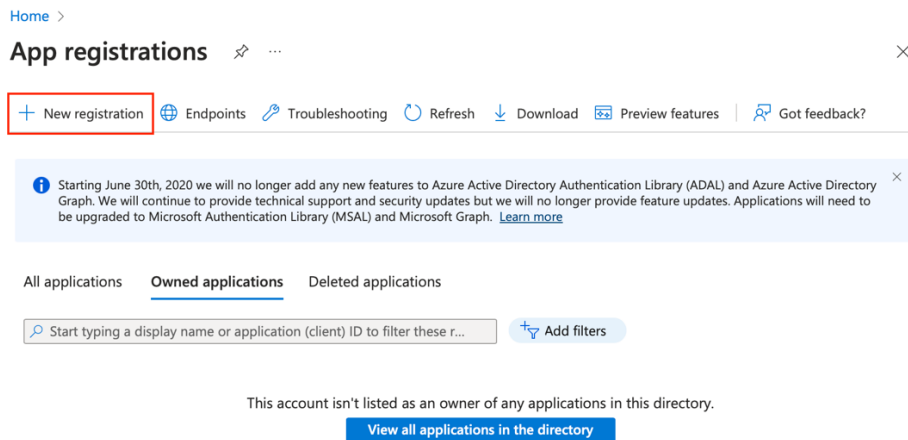
6. Click “Save” and “Copy to Clipboard” on the next screen

- **IMPORTANT**: Save the copied token value somewhere to be used in Step 4

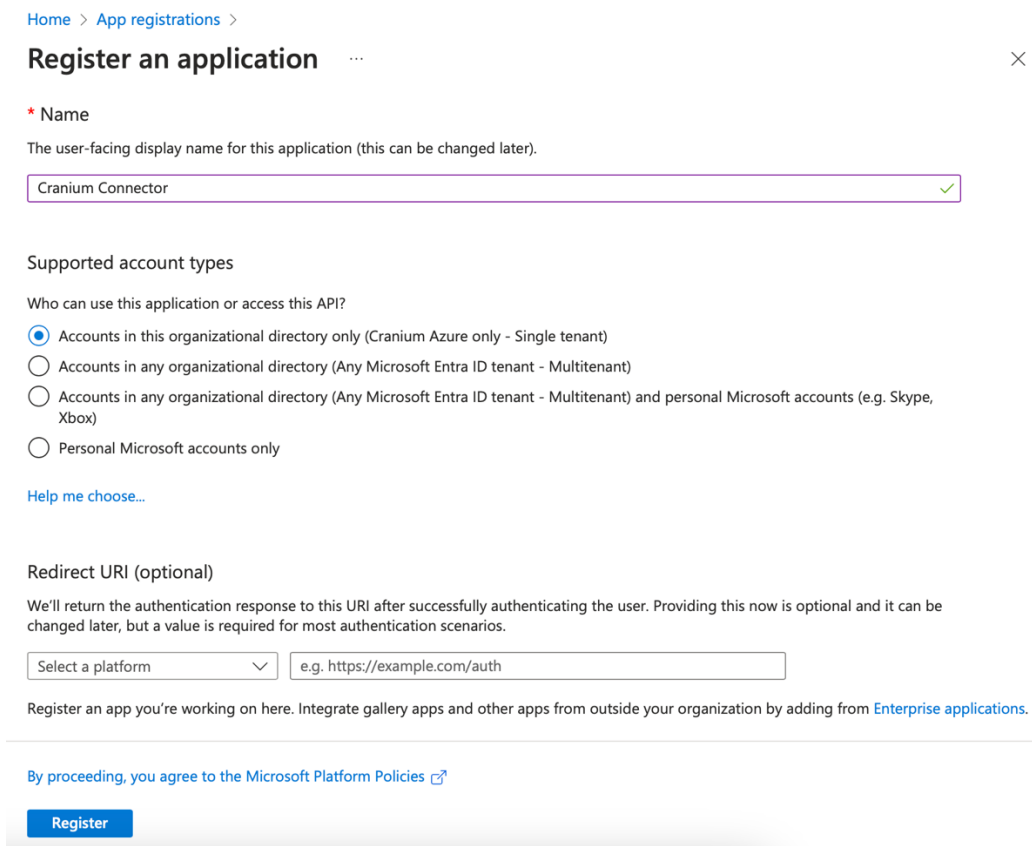


Step 2: Register a new app in Azure with Graph Application “User.Read.All” permissions and create a new secret and save the secret value

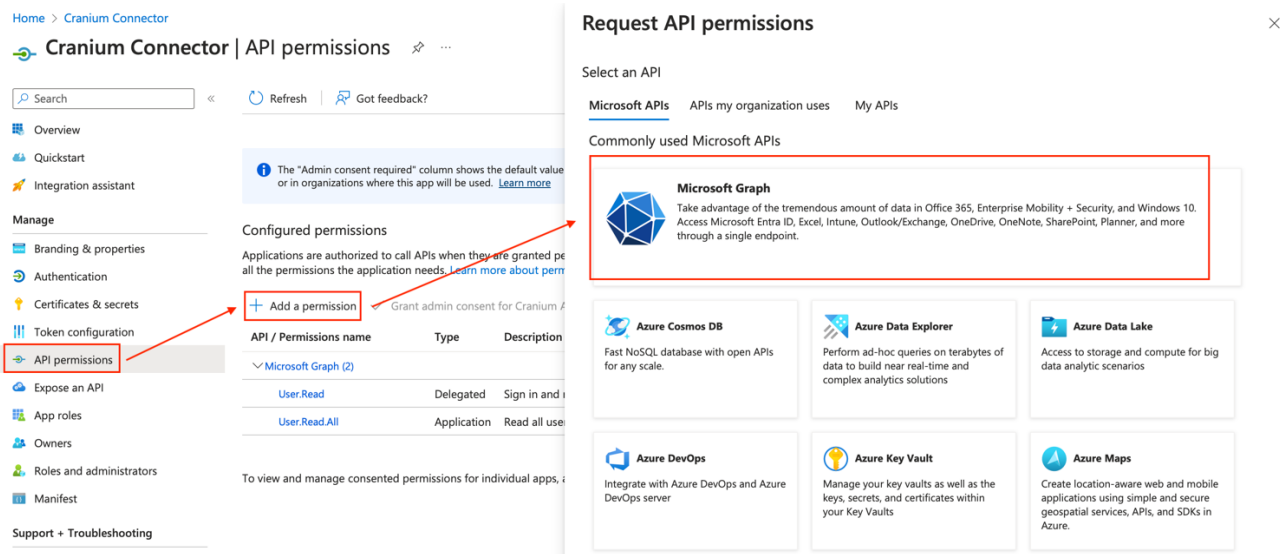
1. Go to the “App registrations” page and click “New Registration”



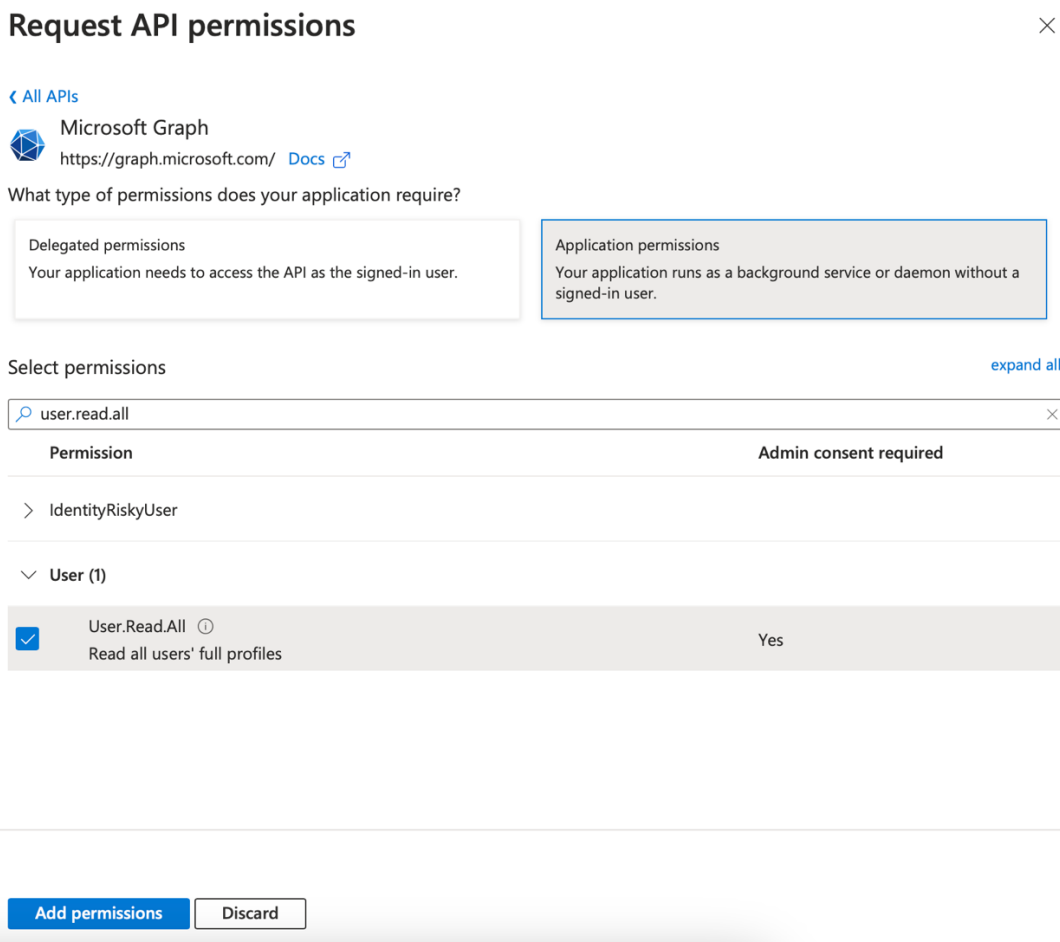
2. Give it any name you'd like, leave the defaults, and click “Register”



- In "API permissions", click "Add a permission", and select "Microsoft Graph"



- Select "Application permissions", find and select "User.Read.All" Permission and click "Add permissions"



Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

user.read.all

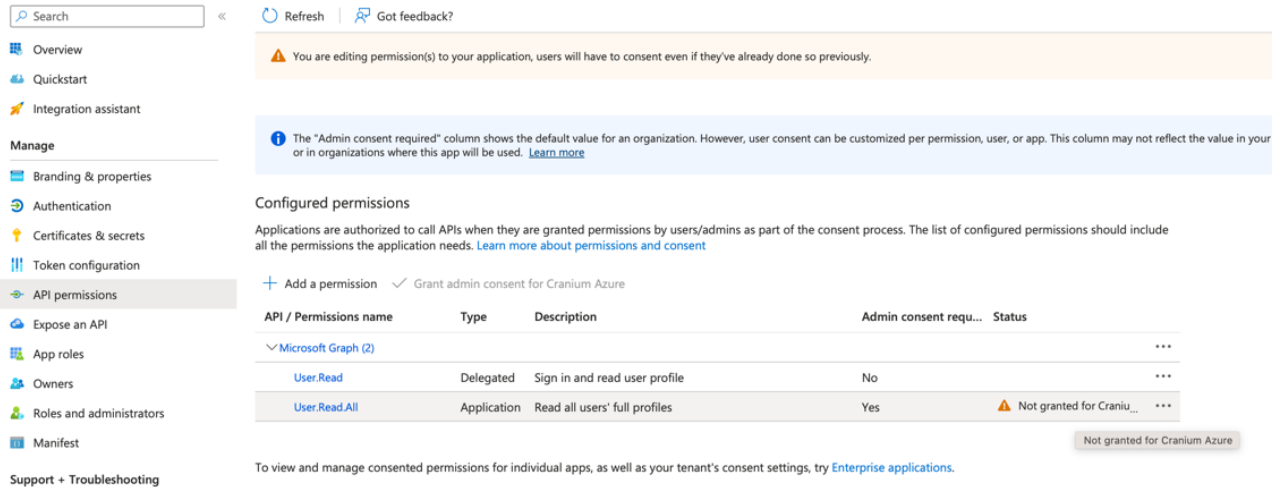
Permission	Admin consent required
> IdentityRiskyUser	
< User (1)	
☒ User.Read.All ⓘ Read all users' full profiles	Yes

[Add permissions](#) [Discard](#)

5. If this permission was created without admin privileges, then a warning will appear on the top of the screen and an admin will need to access the newly created Cranium Connector to grant access

Home > App registrations > Cranium Connector

Cranium Connector | API permissions



Search

Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 or in organizations where this app will be used. [Learn more](#)

Configured permissions

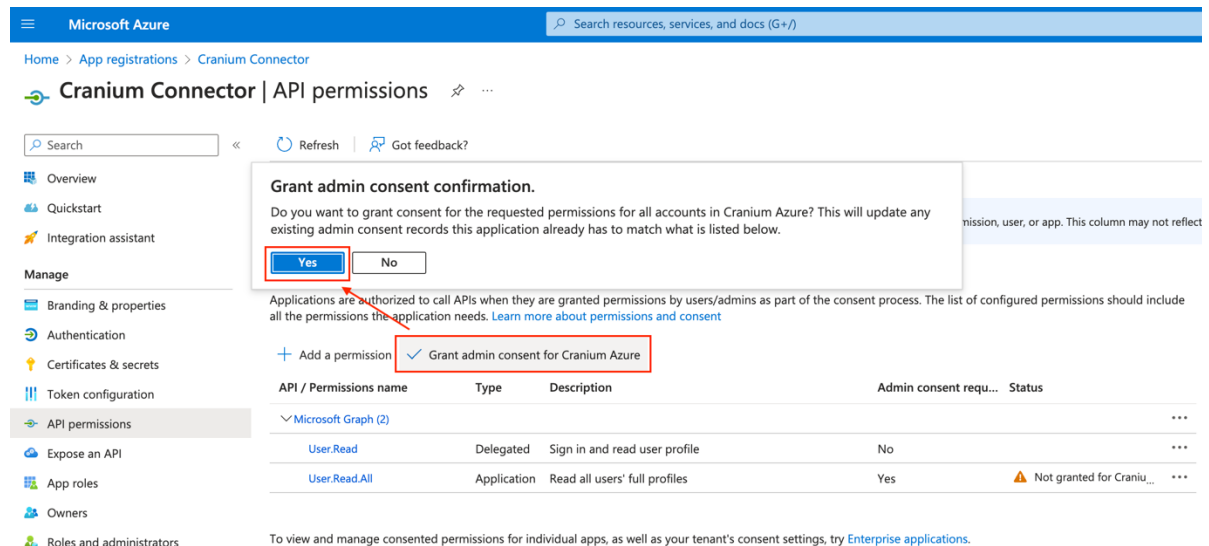
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cranium Azure

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Craniu... ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

- a. For Azure admins granting API permissions, navigate to "App registrations" and find the new Cranium Connector, click "Grant admin consent for ____", and "Yes"



Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > Cranium Connector

Cranium Connector | API permissions

Search

Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Cranium Azure? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

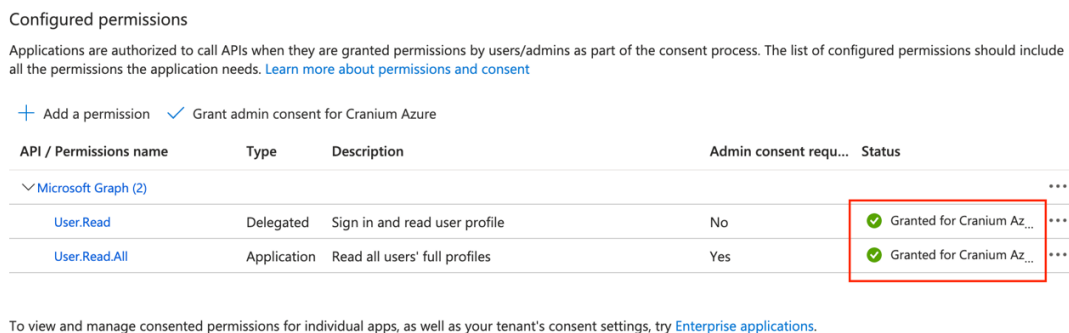
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cranium Azure

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Craniu... ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

- b. Confirm that permissions are granted under "Status"



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](#)

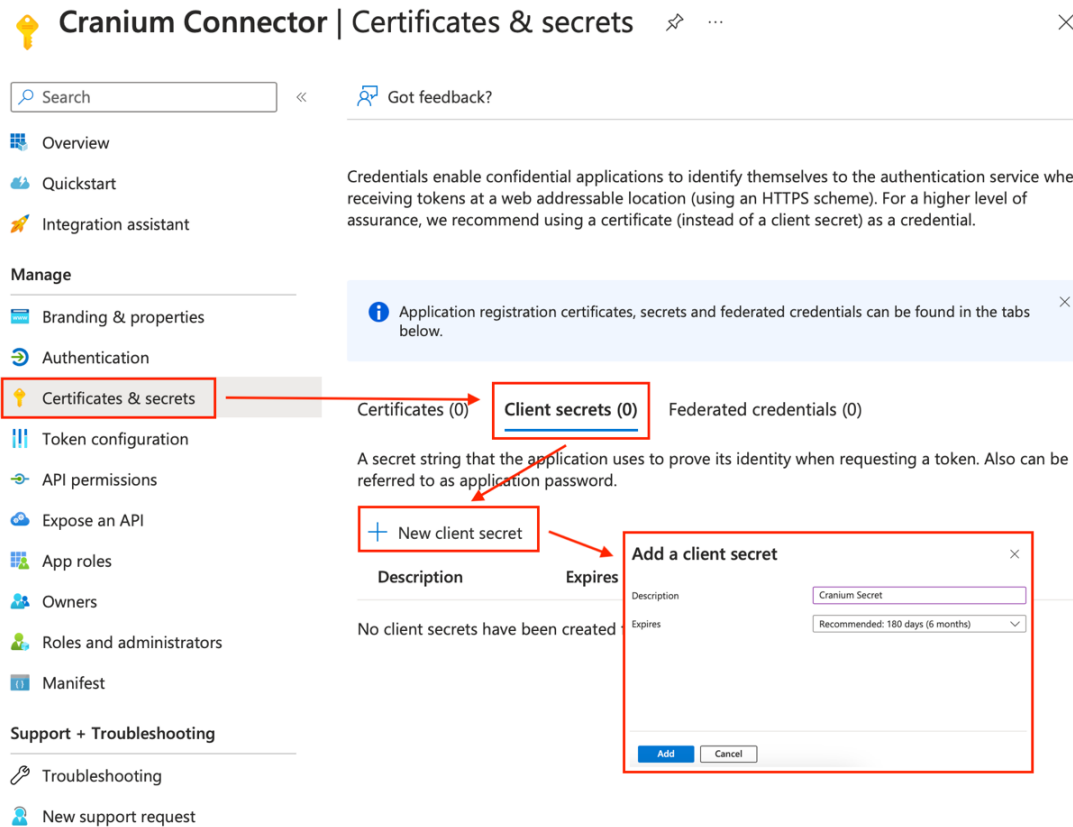
+ Add a permission ✓ Grant admin consent for Cranium Azure

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Cranium Az...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Cranium Az...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

- In "Certificates & Secrets", add a new Client secret with any description and save the secret value somewhere safe

[Home](#) > [App registrations](#) > [Cranium Connector](#)



Cranium Connector | Certificates & secrets

Search < Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

Troubleshooting
New support request

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.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

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

+ New client secret

No client secrets have been created

Add a client secret

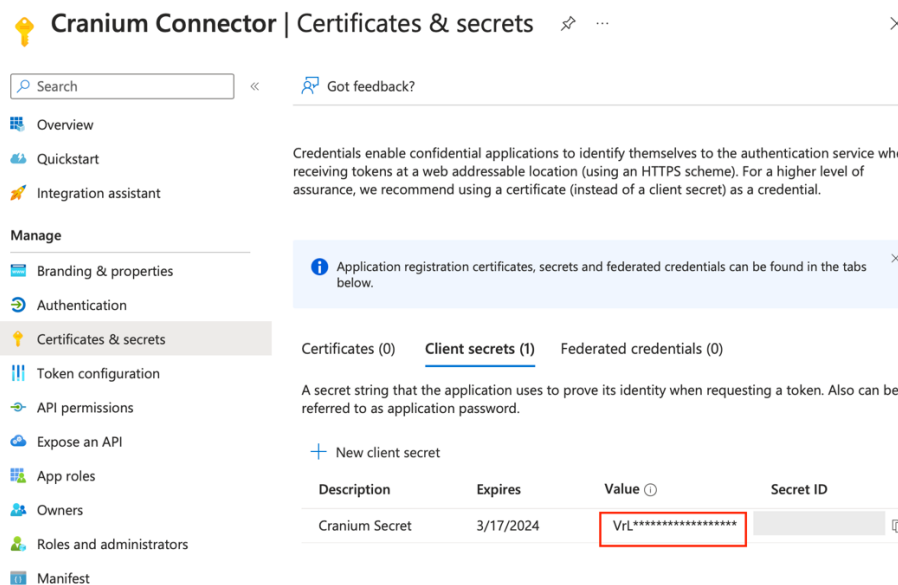
Description:

Expires:

Add Cancel

- IMPORTANT:** Copy and save the client secret value somewhere to be used in Step 4

[Home](#) > [Cranium Connector](#)



Cranium Connector | Certificates & secrets

Search < Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

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.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

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

+ New client secret

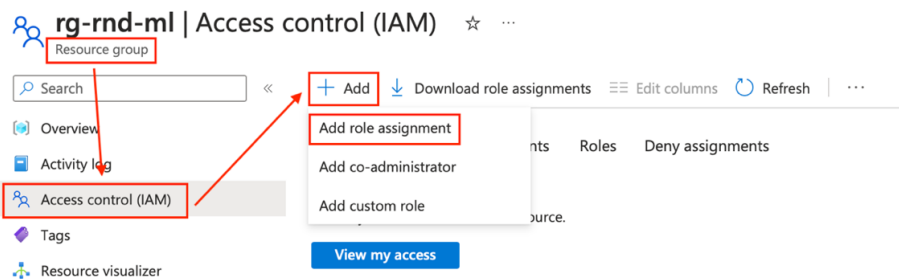
Description	Expires	Value	Secret ID
Cranium Secret	3/17/2024	VrL*****	

Step 3: Assign “Contributor” role for the Cranium Connector member to the Azure ML resource group or Azure OpenAI service

For Azure ML

1. Navigate to the resource group, subscription, or management group to configure “Access control (IAM)” and “Add role assignment”

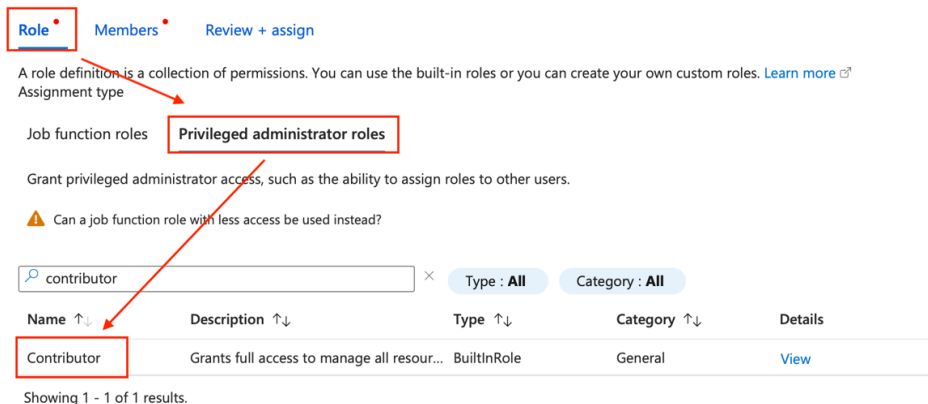
Home > Management groups > Microsoft Azure Sponsorship | Resource groups > rg-rnd-ml



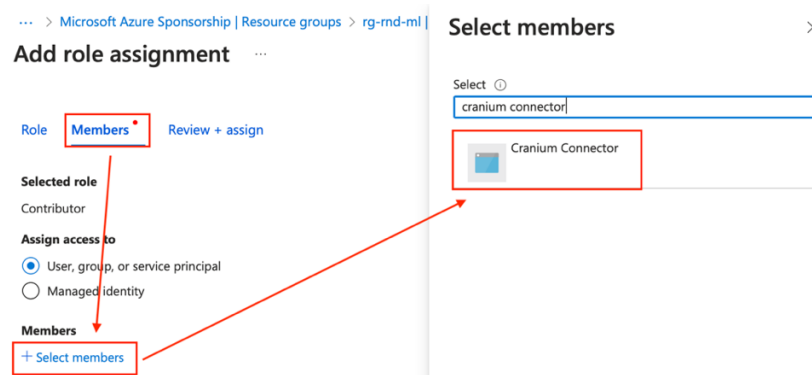
- Cranium recommends following the principle of least privilege access by adding role assignments at the resource group level
 - Note that Access Control is only available to Azure users with "Owner" permissions
2. For the “Role”, navigate to “Privileged administrator roles” to find and select “Contributor”

... > Microsoft Azure Sponsorship | Resource groups > rg-rnd-ml | Access control (IAM) >

Add role assignment



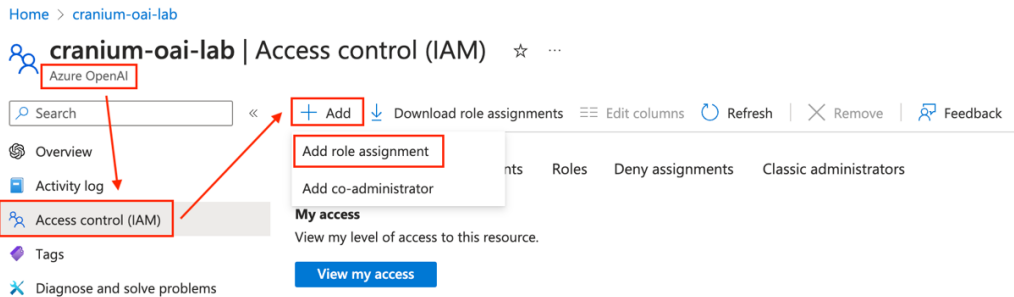
3. For the “Members”, click “Select members”, find and select the new Service Principal



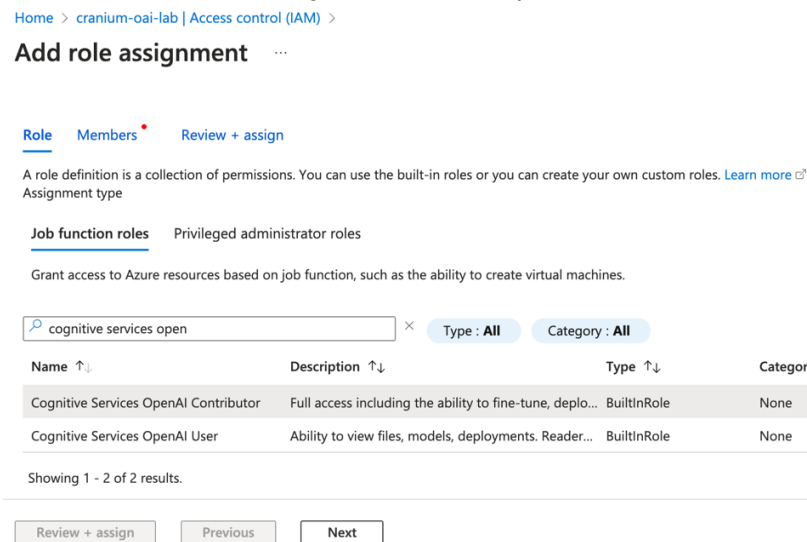
4. Review + assign

For Azure OpenAI

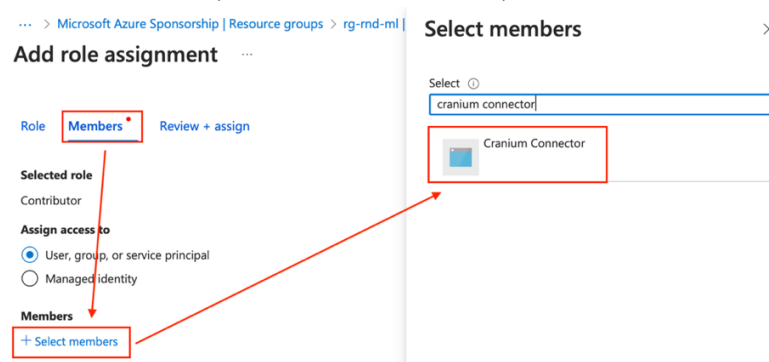
1. Navigate to the Azure OpenAI service to configure “Access control (IAM)” and “Add role assignment”



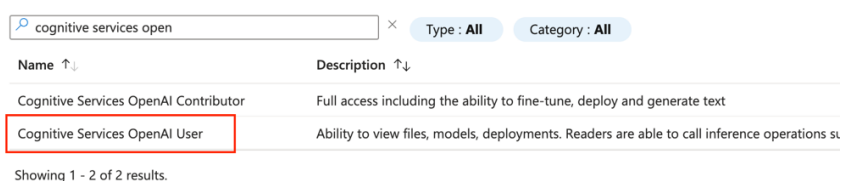
- Note that Access Control is only available to Azure users with "Owner" permissions
2. For the “Role”, find the “Cognitive Services OpenAI Contributor” role and click “Next”



3. For the “Members”, click “Select members”, find and select the new Service Principal

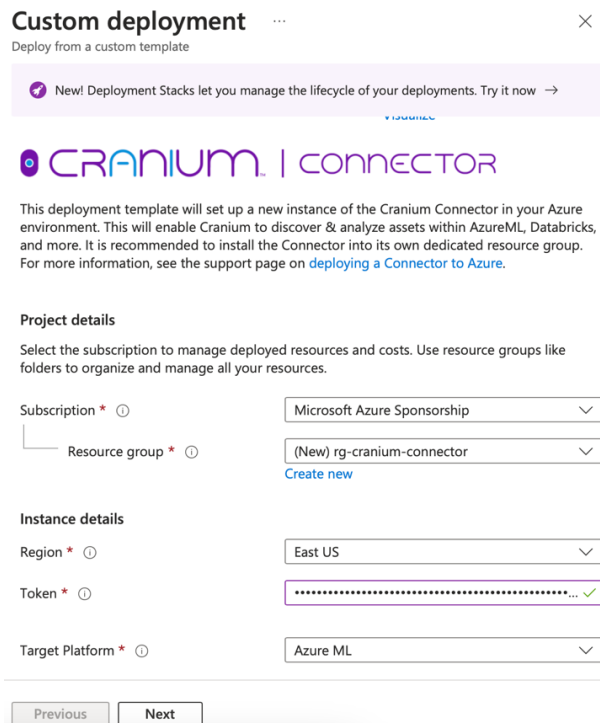


4. Review + assign
5. Complete steps 2-4 for the “Cognitive Services OpenAI User” role



Step 4: Deploy the Cranium Connector ARM Template

1. Open the Cranium Connector ARM Template: [Deploy the Cranium Connector](#)
2. Enter the Subscription and Resource group where you'd like to deploy
 - Cranium recommends setting up a new, dedicated resource group for the deployment
3. Fill the integration Token from step 1 and click "Next"



Custom deployment ... X

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

CRANIUM | connector

This deployment template will set up a new instance of the Cranium Connector in your Azure environment. This will enable Cranium to discover & analyze assets within AzureML, Databricks, and more. It is recommended to install the Connector into its own dedicated resource group. For more information, see the support page on [deploying a Connector to Azure](#).

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Microsoft Azure Sponsorship

Resource group * ⓘ (New) rg-cranium-connector
[Create new](#)

Instance details

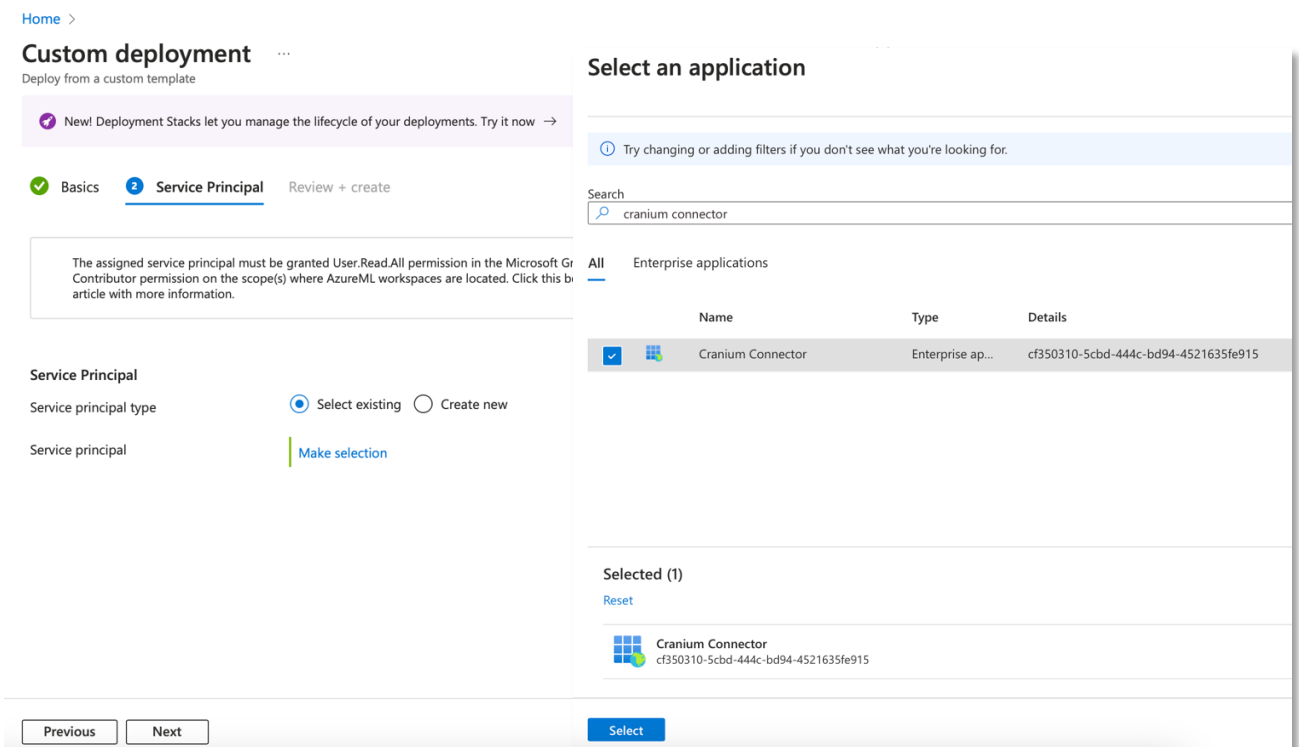
Region * ⓘ East US

Token * ⓘ

Target Platform * ⓘ Azure ML

[Previous](#) [Next](#)

4. "Select existing" Service Principal and select your new Cranium Connector app



[Home](#) >

Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Basics **2 Service Principal** Review + create

The assigned service principal must be granted User.Read.All permission in the Microsoft Graph Contributor permission on the scope(s) where AzureML workspaces are located. Click this [article](#) with more information.

Service Principal

Service principal type ☒ Select existing ☐ Create new

Service principal [Make selection](#)

Select an application

Try changing or adding filters if you don't see what you're looking for.

Search
cranium connector

	Name	Type	Details
☒	Cranium Connector	Enterprise ap...	cf350310-5cbd-444c-bd94-4521635fe915

Selected (1)
[Reset](#)

 **Cranium Connector**
cf350310-5cbd-444c-bd94-4521635fe915

[Previous](#) [Next](#) [Select](#)

5. Enter the service principal Client Secret from step 2, click "Next"

Home >

Custom deployment

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Basics **2 Service Principal** Review + create

The assigned service principal must be granted User.Read.All permission in the Microsoft Graph API, as well as Contributor permission on the scope(s) where AzureML workspaces are located. Click this box to view the support article with more information.

Service Principal

Service principal type ☒ Select existing ☐ Create new

Service principal **Cranium Connector**
[Change selection](#)

Client Secret * ⓘ

Previous Next

6. Click "Create" to complete deployment!

Home >

Custom deployment

Deploy from a custom template

Basics **Service Principal** **Review + create**

Summary

Customized template
45 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Previous Next **Create**

- Deployment should take 20-30 minutes

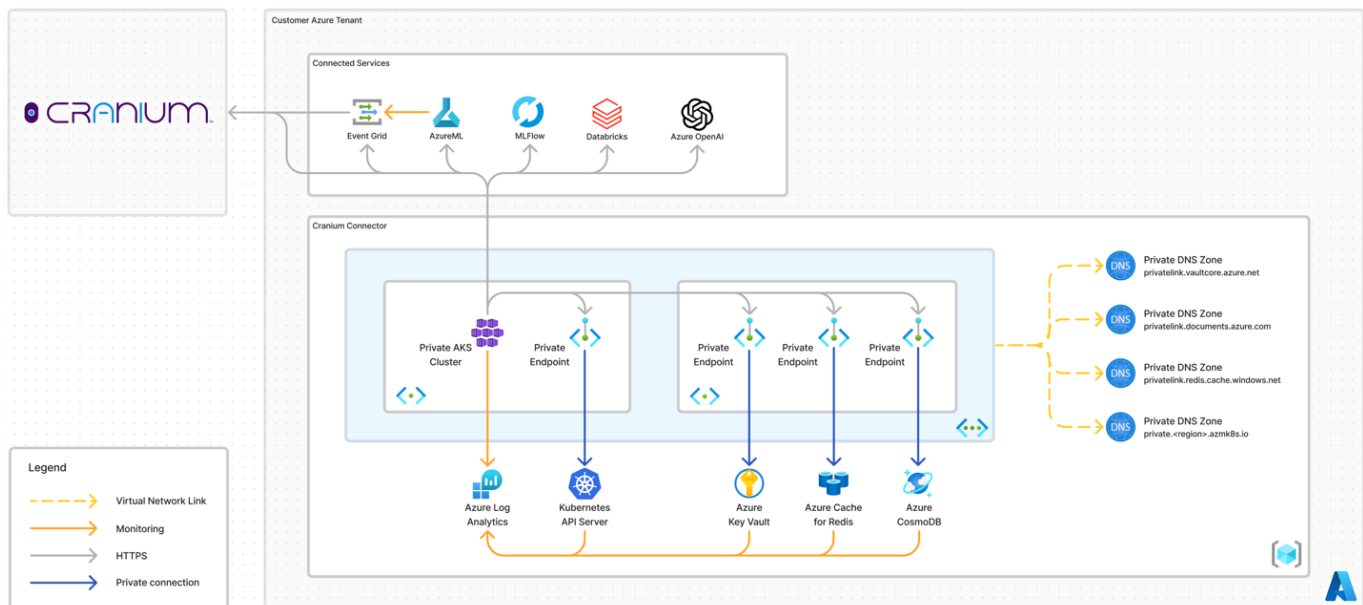
Getting Started with Cranium

The following links from the Cranium Knowledge Base can help when starting out with the Cranium platform after a connector has been deployed. Note that the Knowledge Base requires a Cranium account in order to access.

- [Asset Overview](#)
- [Pipeline Overview](#)
- [Monitoring Overview](#)
- [Creating a Pipeline](#)
- [Creating Alert Rules](#)

Architecture Diagram

The diagram below describes the networking and Azure components included in a connector deployment. The in-scope components are those within the “Cranium Connector” box. All other components shown are for reference as to the nature of network connections being made.



Asset Information Received from Connector

The table below lists the asset attributes sent from the Cranium Connector through Azure back to Cranium.

Asset	Cranium	Azure
Model	ID	Azure ID
	Name	Model -> Name
	Version	Model -> Version
	Description	Model -> Description
	Job ID	Model -> Job ID
	Experiment	Model -> Job ID -> Experiment
	Created By	Model -> Created By
	Created On	Model -> Created On
	Runs	–
	Datasets	–
	Event (Add Model version Update version Delete version)	–
Experiment	ID	Azure ID
	Name	Experiment -> Name
	Latest Job	Experiment -> Run
	Job types	Experiment -> Type
	Event (Created Delete)	–
Run	ID	Azure ID
	Type (AutoML Pipeline Script)	Job -> Job Type
	Experiment	Job -> Experiment
	Duration	Job -> Runtime
	Compute Target	Job -> Compute -> Target
	Status (Completed Failed)	Job -> Status
	Parent Run	Job -> Parent
	Created By	Job -> Created By
	Created On	Job -> Created On
	Datasets	–
	Models	–
Deployment	Result	–
	ID	Azure ID
	Name	Endpoint -> Display Name
	Type (Realtime Batch)	Endpoint -> Type
	Compute Type	Deployment -> Compute -> Type
	Compute Target	Deployment -> Compute -> Target
	Created By	Deployment -> Created By
	Created On	Deployment -> Created On
Dataset	Models	–
	Event (Add Delete)	–
	ID	Azure ID
	Name	Dataset -> Name
	Version	Dataset -> Version
	Description	Dataset -> Description
	Storage Type	Data Store Type (Azure Blob Storage, Azure File Share, etc)
	Type (Table File Folder)	–
	Created By	Dataset -> Created By
	Created On	Dataset -> Created On
	Runs	–
User	Models	–
	Event (Add Update version Delete)	–
	ID	Azure Graph -> User -> ID
	First Name	Azure Graph -> User -> Given Name
	Last Name	Azure Graph -> User -> Surname
	Email	Azure Graph -> User -> Email
	Actions	–

Analysis Information Received from Connector

The table below lists the analysis fields and metrics sent from the Cranium Connector through Azure back to Cranium.

Asset	Analysis Type	Calculated Fields & Metrics
Model	Metrics	Accuracy
		Precision
		Recall
		F-score
		ROC
Dataset	Structure	AUC
		Normalized RMS Error
		Spearman Correlation
		R2 Score
		Normalized Mean Absolute Error
Dataset	Features	Name
		Path
		Type
		Size
Dataset	Numeric Features	Name
		Type
		missing/mistyped values
Dataset	Categorical Features	Mean
		Median
		Minimum
		Maximum
		Distribution
		Correlation
Dataset	Data/Feature Shift	Unique value hashed
		Frequency
Detection	Poison Detection	JS test
		WS distance
		KS test
Detection	Backdoor Detection	Result
		Confidence
		Poisoned dataset IDs
		Model IDs
		Poisoned data primary keys
		Clean dataset IDs
Detection	Backdoor Detection	Result
		Confidence
		Dataset IDs
		Model IDs
		Calculated trigger heatmap image