## 

[**CloudSoc Console - Configuring Azure connection 1**](#_hpi6f48j9h3f)

[**CloudSoc Console - Create Public API keys 1**](#_a6k5xnlwjg46)

[**Variables Used 2**](#_ht6oywb3z847)

[**Convert publickey, secret key to base 64 encoding 3**](#_g9c8tdp6mwcv)

[**Generate JWT Token 3**](#_975l6wobu68o)

[**Activating Azure Connection 4**](#_yte1h6ogj5zo)

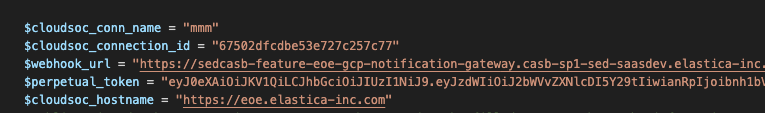
[**Validate Azure Connection 5**](#_h73yg0h3d42h)

**Creating Azure App Registration……………………………………………………………………..6**

## **Please Note: All the items marked in red below is needed to run the API**

## CloudSoc Console - Configuring Azure connection

1. Log in to your CloudSoc account
2. Goto Securlet and click on IaaS
3. You will be routed to connections page
4. Click on Add Connections and Select Azure
5. You will be directed to Azure Configuration page
6. Give a connection name and save the connection
7. Then press “Download Script”. The script will be downloaded in your default folder.
8. Copy following values from script and keep it handy.You can search for ("cloudsoc\_conn\_name”, ”cloudsoc\_connection\_id”, “cloudsoc\_hostname”)key word in shell script. This will be used later to run public APIs

For example:  


## CloudSoc Console - Create Public API keys

1. On the right hand top of CloudSoc console click the gear icon, it will take you to the settings page
2. Under that on left pane click on API keys
3. Under API key, type the name of your key and click on Add new API Key
4. New API key will be generated in the pane below
5. Just on the right of the API keys in the Action column, there is a download key option to download the keys. Click on that and download the file, we will need following information

"tenant": "xxxx",

"api\_server": “xxxx”

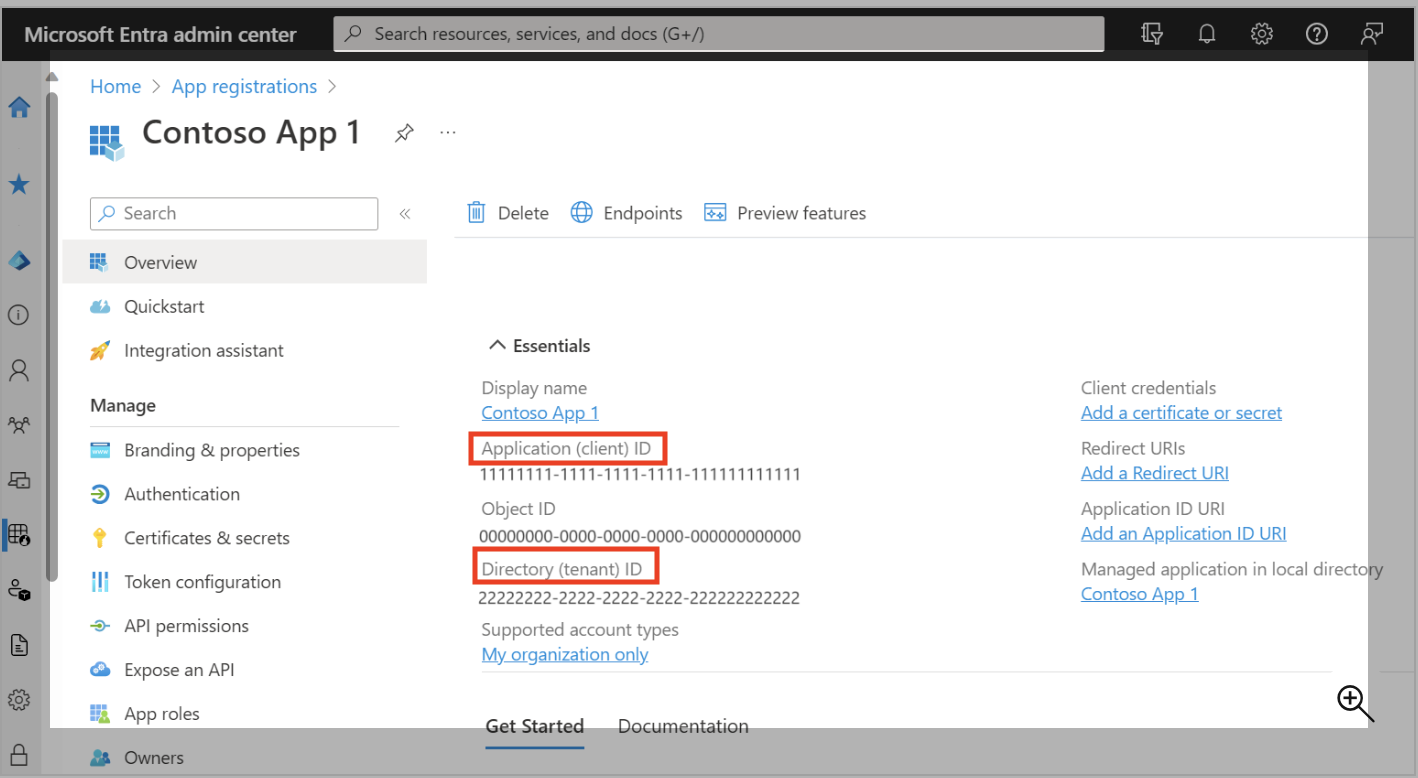
"user\_id": “xxxx”

"key\_id": “xxxx”

"key\_secret": “xxxx”

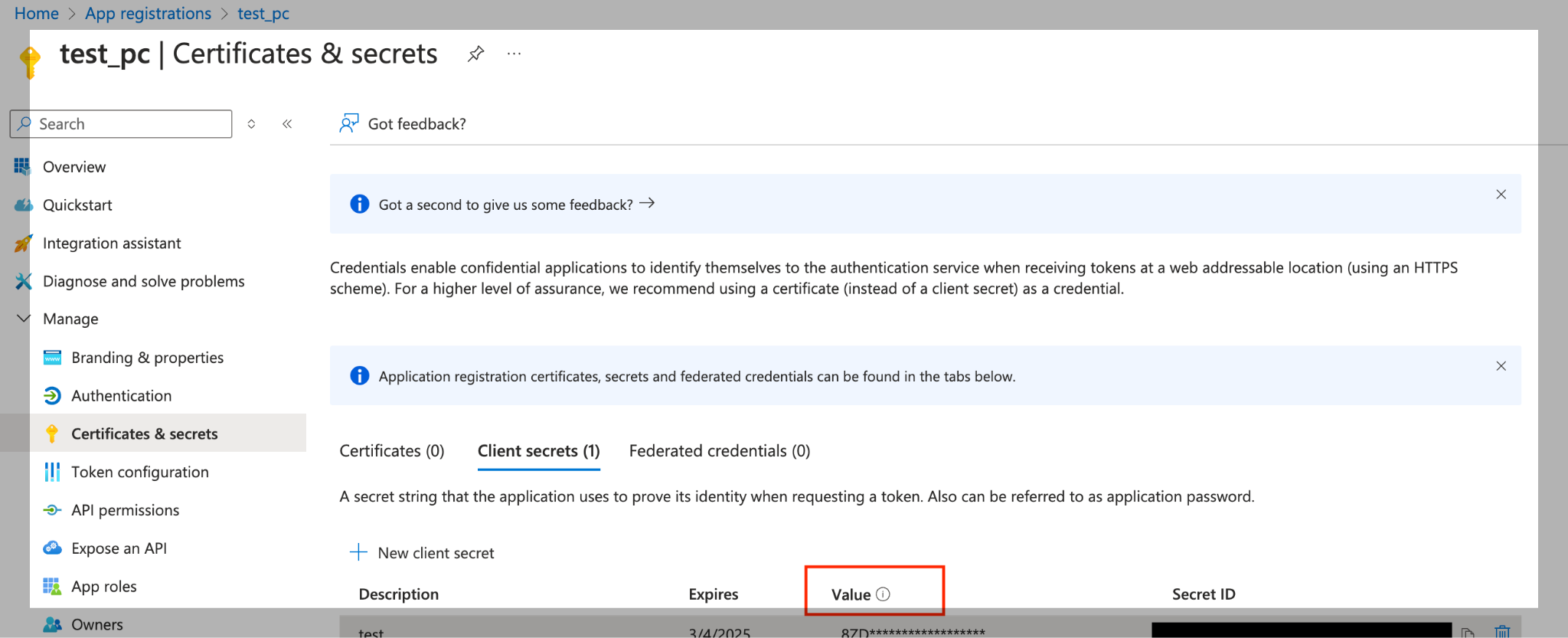
## Creating Azure App Registration

**Register an App**<https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app?tabs=client-secret#register-an-application>  
  
Copy Application (client) ID and Directory (tenant) ID, which will be needed for Public API



**Add a secret to it**<https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app?tabs=client-secret>

Copy the Value



**Give User Related Permission On AzureApp**

This is a one time step and needs Administrator permission.

Please assign User.Readall, Directory.ReadAll and Application.ReadAll permissions to Active Directory Application created for Application

1. Log in to Azure console as an Administrator

2. Goto Azure Active Directory services in Azure.

3. Go to ‘App Registrations’ and All Applications

4. Select application created [here](#_6pjdsifr3w7s)

5. Go to ‘API permissions’ and Add permission

6. Select Microsoft Graph and Application Permission

7. Select User.ReadAll, Directory.ReadAll and Application.ReadAll

8. Grant admin consent for your account

**Note**: If you fail to give above permissions CloudSoc will not be able to get User related data

## Variables Used

Below tables list all the variables which are used in public APIs and it also provides a way to get them.

| **Variables** | **Source** | **Remarks** | **Link** |
| --- | --- | --- | --- |
| **publickey:secretkey** | key\_id:key\_secret | You get these values in json when you click on download key | [Here](#_a6k5xnlwjg46) |
| **encoded\_key** | You get this by running command echo -n 'publickey:secretkey' | base64 |  | [Here](#_g9c8tdp6mwcv) |
| **tenant** | Stored in downloaded shell script in cloudSocTenantId variable | This is needed while running public APIs | [Here](#_a6k5xnlwjg46) |
| **hostname** | Stored in downloaded shell script in cloudSocHostname variable | This is needed for calling Public APIs and {hostname} should be replaced by these values depending on the environment that you are in | [Here](#_a6k5xnlwjg46) |
| **valid\_token** | You get this by running /iaas/api/public/v2/token API mentioned below | This is used to authenticate public APIs for valid information | [Here](#_975l6wobu68o) |
| **cloudsoc\_connection\_id** | Stored in downloaded shell script in cloudsoc\_connection\_id variable | This is used to trigger the public API on right connection | [Here](#_hpi6f48j9h3f) |
| **cloudsoc\_conn\_name** | Stored in downloaded shell script in cloudsoc\_conn\_name variable | This is used to trigger the public API on right connection | [Here](https://docs.google.com/document/d/1QyLKLkp4wDZyUv27O5uw5w3ujTouGtb_i4AmfKXSUuc/edit?tab=t.0#heading=h.hpi6f48j9h3f) |
| appID | You will get this by Creating Azure App Registration Application (client) ID -> appID |  | [Here](#_6pjdsifr3w7s) |
| azure\_subscription\_tenant\_id | You will get this by Creating Azure App Registration Directory (tenant) ID -> azure\_subscription\_tenant\_id |  | [Here](#_6pjdsifr3w7s) |
| app\_secret\_key | You will get this by Creating Azure App Registration app\_secret\_key |  | [Here](#_6pjdsifr3w7s) |

## Convert publickey, secret key to base 64 encoding

You can generate this on MAC by using the following command.

echo -n 'publickey:secretkey' | openssl base64

You will get the 'publickey’(Key\_id), ‘secretkey’(key\_secret). Copy the output from the above command and keep it for next steps. This will generate the encoded\_key which is needed in subsequent APIs

## Generate JWT Token

This will be used in subsequent APIs. This is used to authenticate the public APIs.

URL: {hostname}/iaas/api/public/v2/token

Method: POST

Headers:

X-Elastica-Dbname-Resolved:true

Content-Type:application/json

Authorization:Basic <encoded\_key>

tenant:<tenant>

You will get the <encoded\_key> from above step and <tenant> (tenant) is present here

Body: N/A

Response: Please note we will be using this

{"token": "<valid\_token>"}

**Curl Request:**

| curl --location --request POST '{hostname}/iaas/api/public/v2/token' \  --header 'authorization: Basic <encoded\_key>' \  --header 'cache-control: no-cache' \  --header 'content-type: application/json' \  --header 'tenant:<tenant>' \  --header 'x-elastica-dbname-resolved: true' |
| --- |

## Activating Azure Connection

This will be used to onboard the GCP connection. If successful this API will make the connection as active in the cloudsoc console.

URL: {hostname}/iaas/api/public/v2/azure\_connection

Method: POST

Headers:

Content-Type:application/json

Authorization:Basic <valid\_token>

Body:

{

"id": "<connection\_id>",

"name": "<cloudsoc\_conn\_name>",

"mode": "multiple",

"type": "azure",

"azure\_tenant\_id": "<azure\_subscription\_tenant\_id>",

"azure\_client\_id": "<appID>",

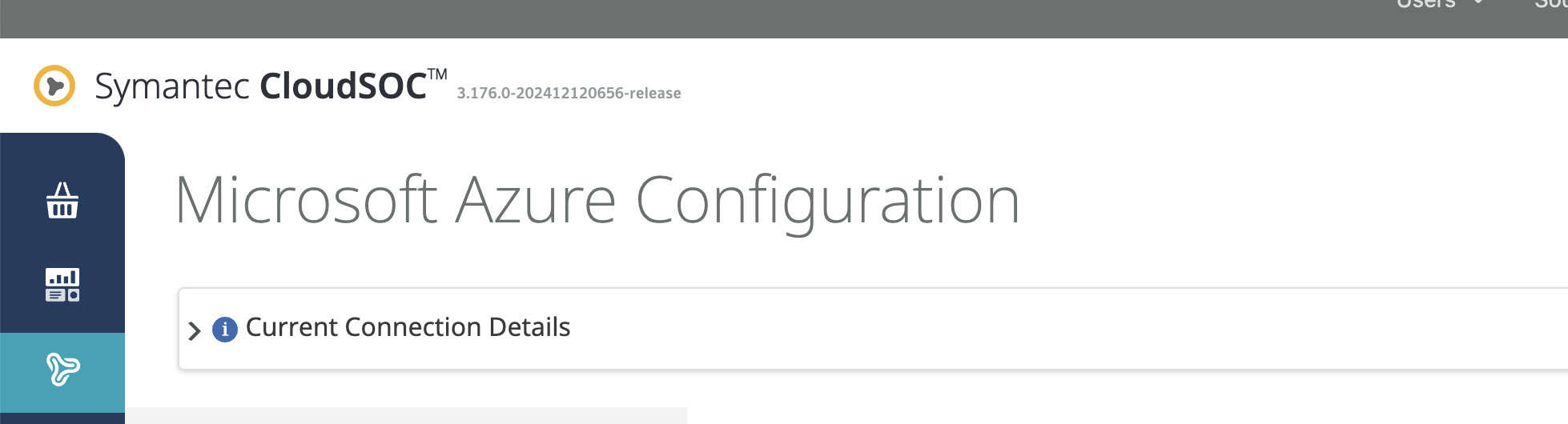
"azure\_client\_secret": "<app\_secret\_key>"

}

**Curl Request:**

| curl --location '{hostname}/iaas/api/public/v2/azure\_connection \  --header 'Authorization: Bearer {"<valid\_token>”}' \  --header 'Content-Type: application/json' \  --data-raw '{  "id": "<connection\_id>",  "name": "<cloudsoc\_conn\_name>",  "mode": "multiple",  "type": "azure",  "azure\_tenant\_id": "<azure\_subscription\_tenant\_id>",  "azure\_client\_id": "<appID>",  "azure\_client\_secret": "<app\_secret\_key>"  }' |
| --- |

## Validate Azure Connection

On the CASB Cloud Console, Edit the Azure Connection  
Once the successful connection is established, USer will see Connection Details.  


### 