API and API Management Configuration

Tuesday, February 09, 2021

General Overview:

- API Backend Setup
- Configure API to API Management
- Security

1) Go to App Services from: Home → App Services →

a) Click + Create

(1) Refer to Section 1 in the API template document for steps A – J.

ii) Choose the appropriate Subscription

iii) Choose the appropriate Resource Group

iv) Supply the Instance Details

(1) Name

(2) Publish (Code or Docker Container)

(a) Default Code

(b) Runtime Stack

(3) (default to .NET Core 3.1 LTS) *Note: This .NET Core IS backwards compatible to .NET Core 2.1*

v) Operating System (Windows or Linux)

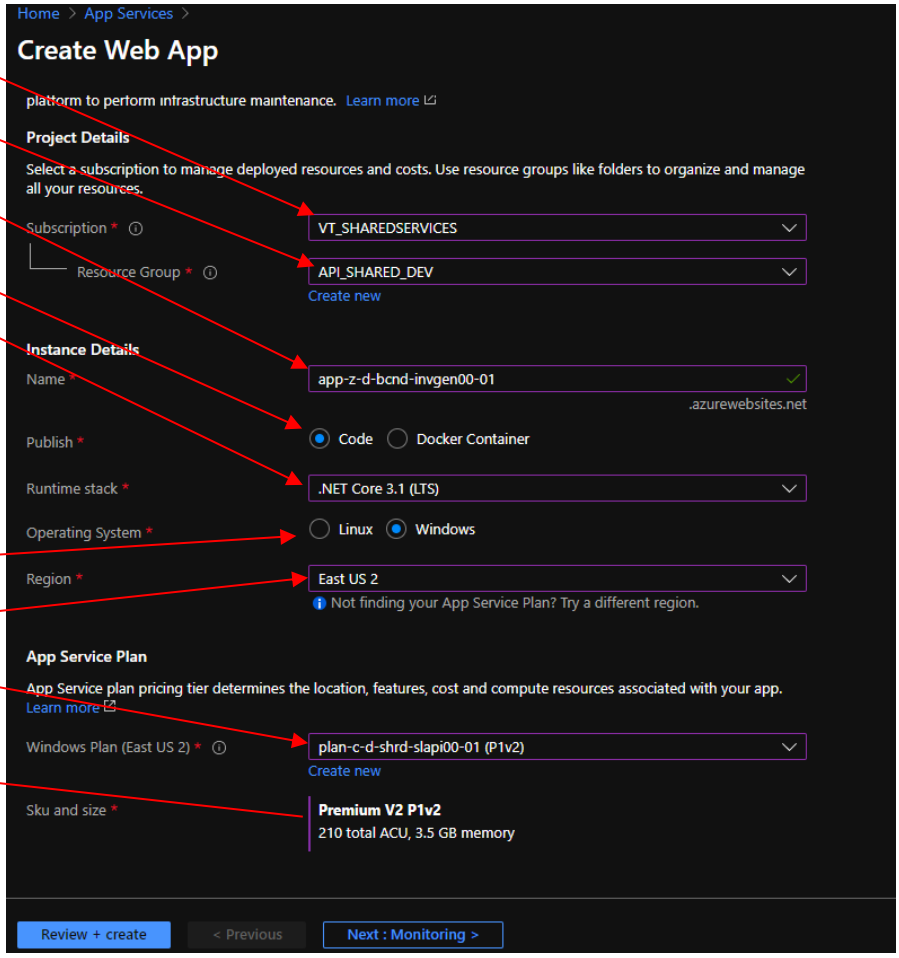
(1) Default Windows

vi) Region

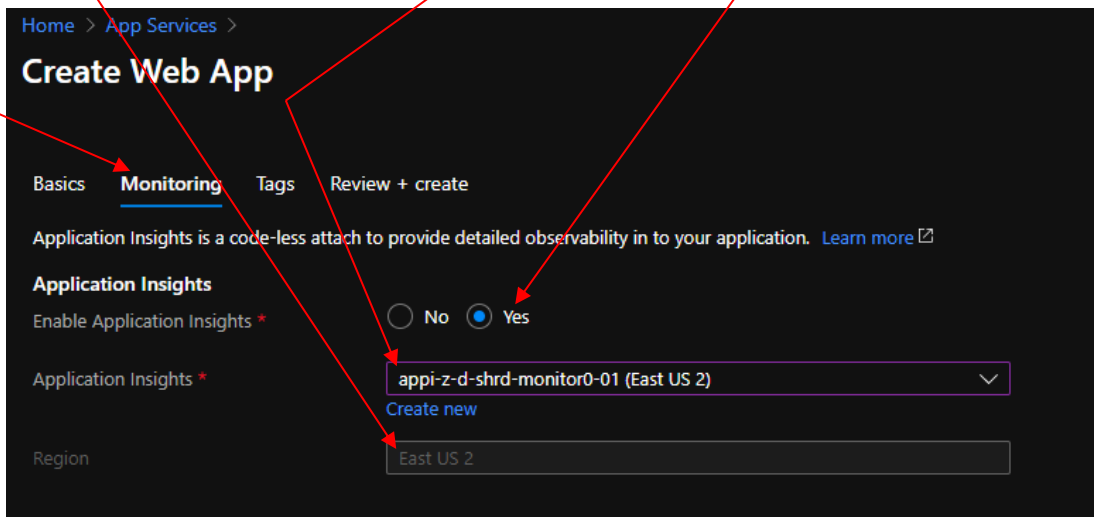
(1) East US 2

vii) Select App Service Plan

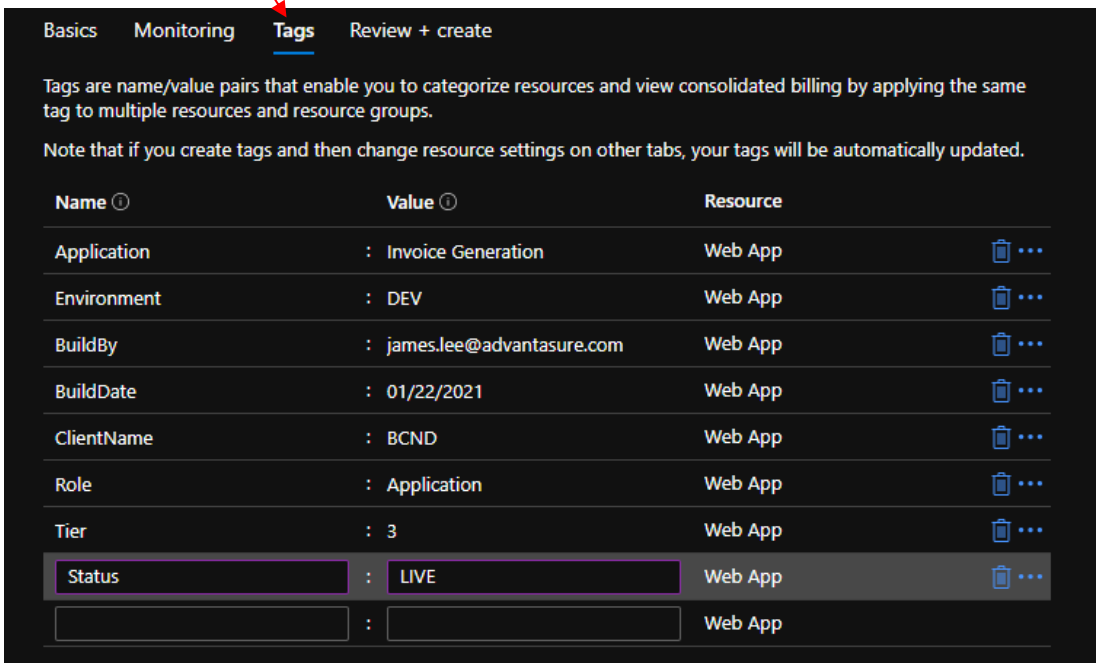
viii) Use the selected (default) SKU based on the service plan unless otherwise directed to use another



b) Click Next: Monitoring
   i) Enable Application Insights
      (1) Select from the drop down, the monitor0-01 for the environment
      (For example: api-c-t-shrd-monitor0-01)
      (2) Region: East US 2



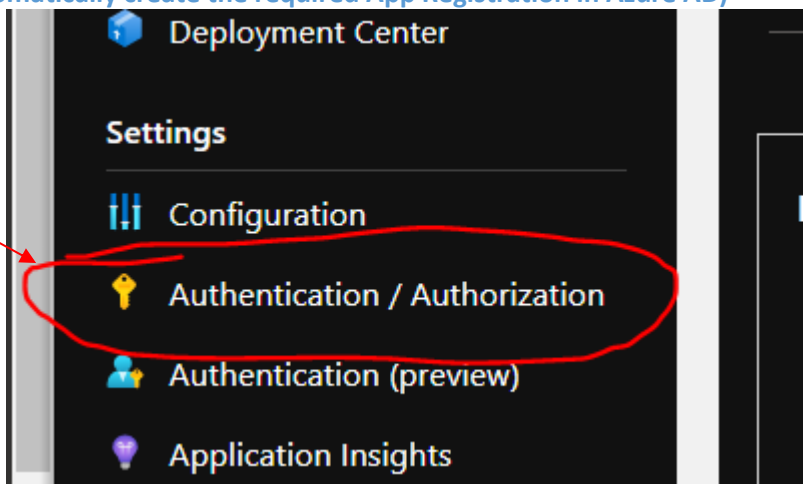
c) Click Next: Tags
   i) Application
      (1)
   ii) Environment
      (1) DEV
   iii) BuildBy
      (1)
   iv) BuildDate
      (1)
   v) ClientName
      (1)
   vi) Role
      (1) Application
   vii) Tier
      (1) 3
   viii) Status
      (1) LIVE



d) Click: Next: Review + create
e) Verify everything is correct, then click: Create

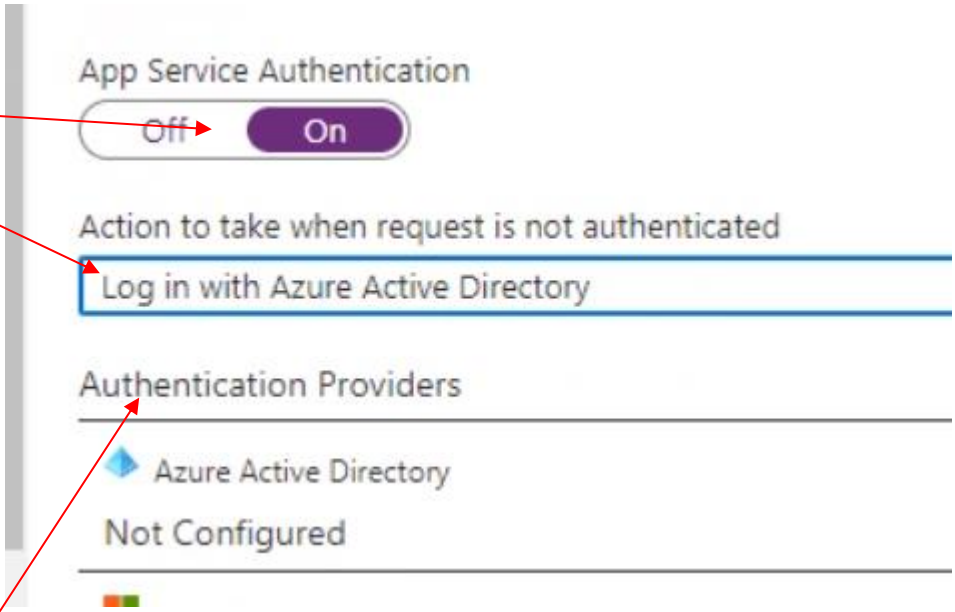
2) Configure API for OAuth2 (which will automatically create the required App Registration in Azure AD)

a) Within the API go to the middle panel and select Authentication / Authorization

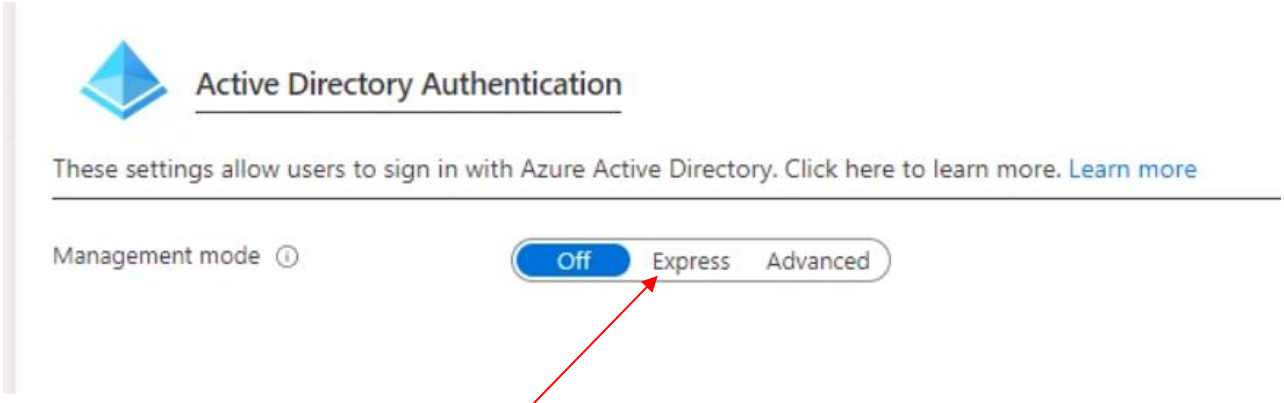


b) Turn the App Service Authentication option to On

c) In the Action to take when request is not authenticated field, click the down arrow for the drop down menu and select Log in with Azure Active Directory

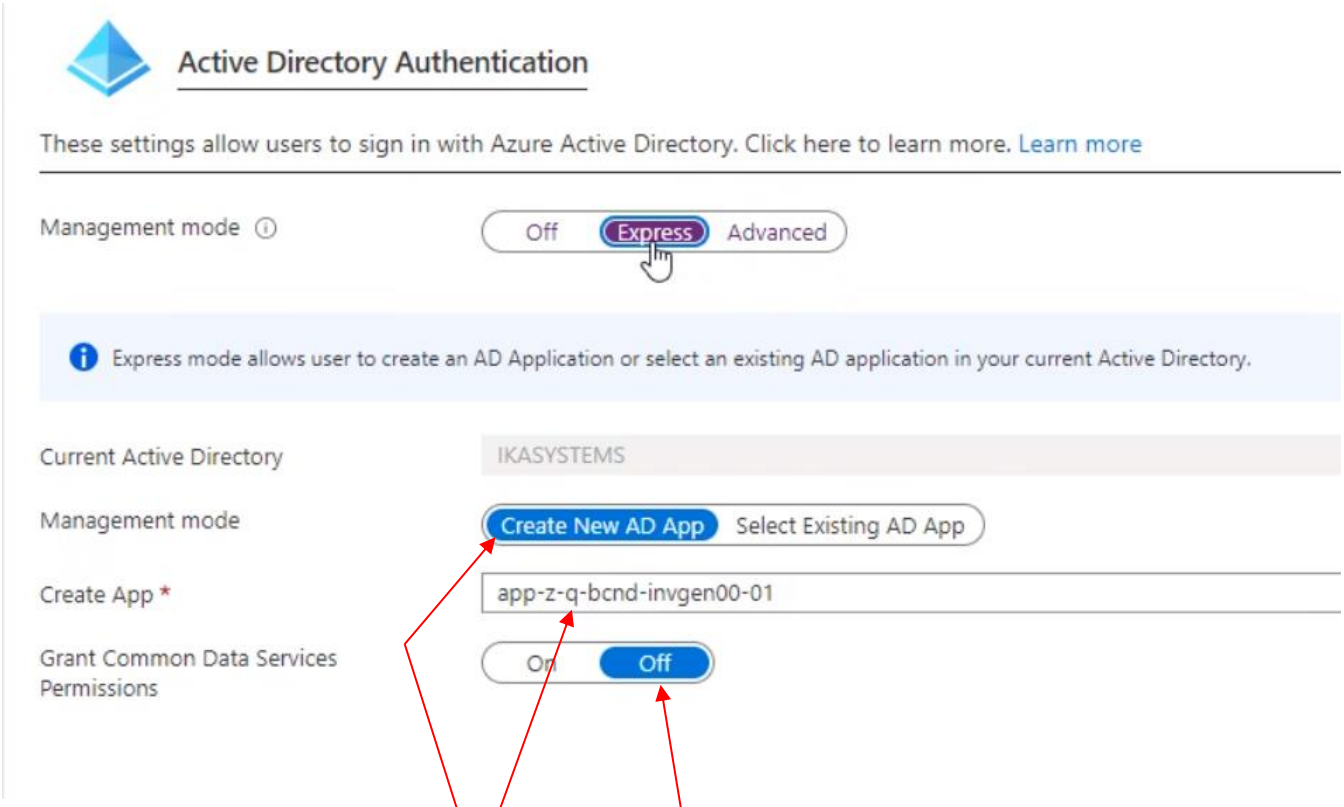


d) Next click on Authentication Providers, this brings up the following screen:



e) Click Express for the Management mode

f) You will see this next:



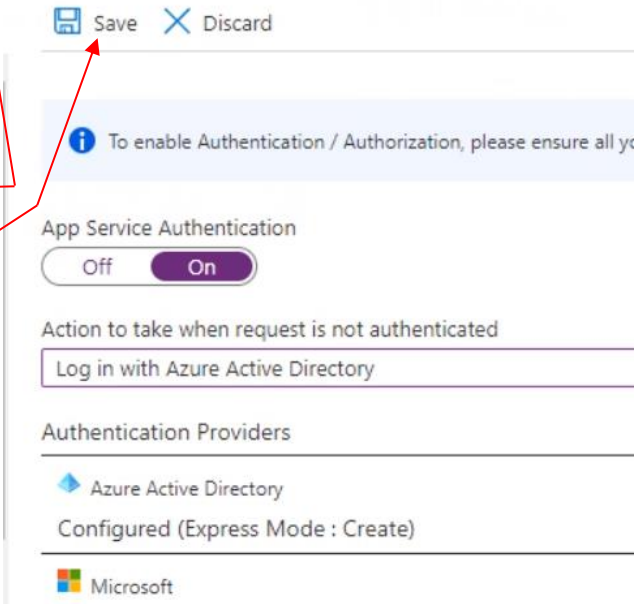
g) Keep the default settings for the Management mode & Create App. If you named the API correctly when you first created it, this name should fill in by default and should not need to be changed

h) Keep the Grant Common Data Services Permissions set to off (default)

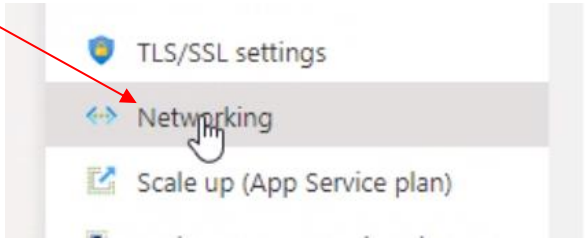
i) In the bottom left of the pane click OK

j) You will be brought back to this screen and the setting should look similar this

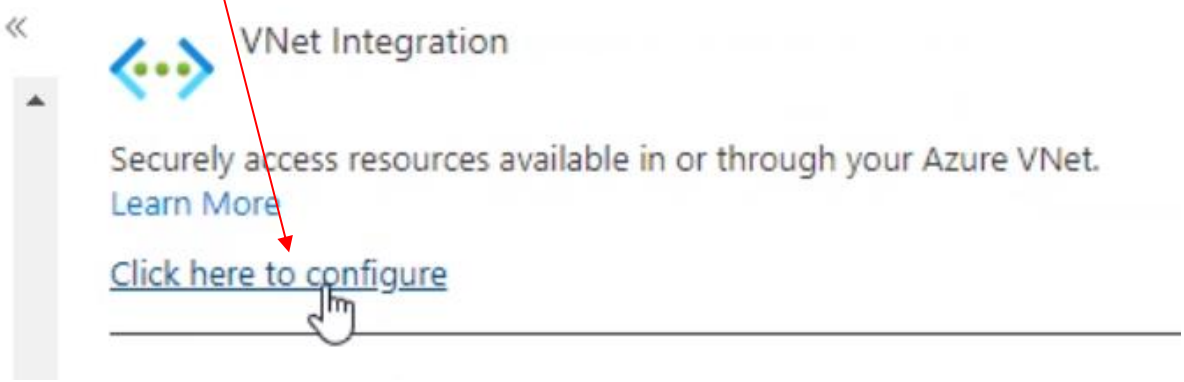
k) Finally click Save at the top of the pane



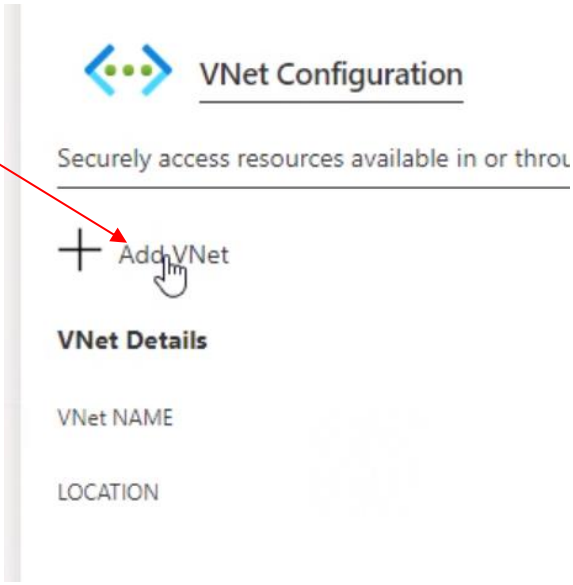
3) Click on Networking in middle pane of the App Service



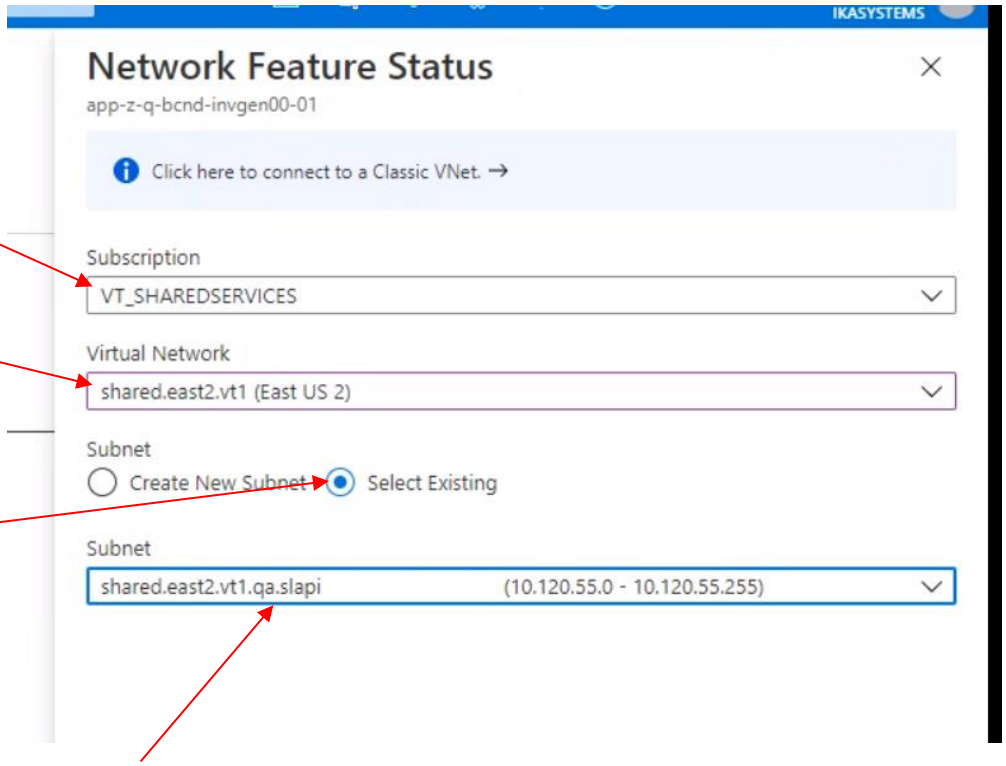
a) Now select: Click here to configure under the VNet Integration section:



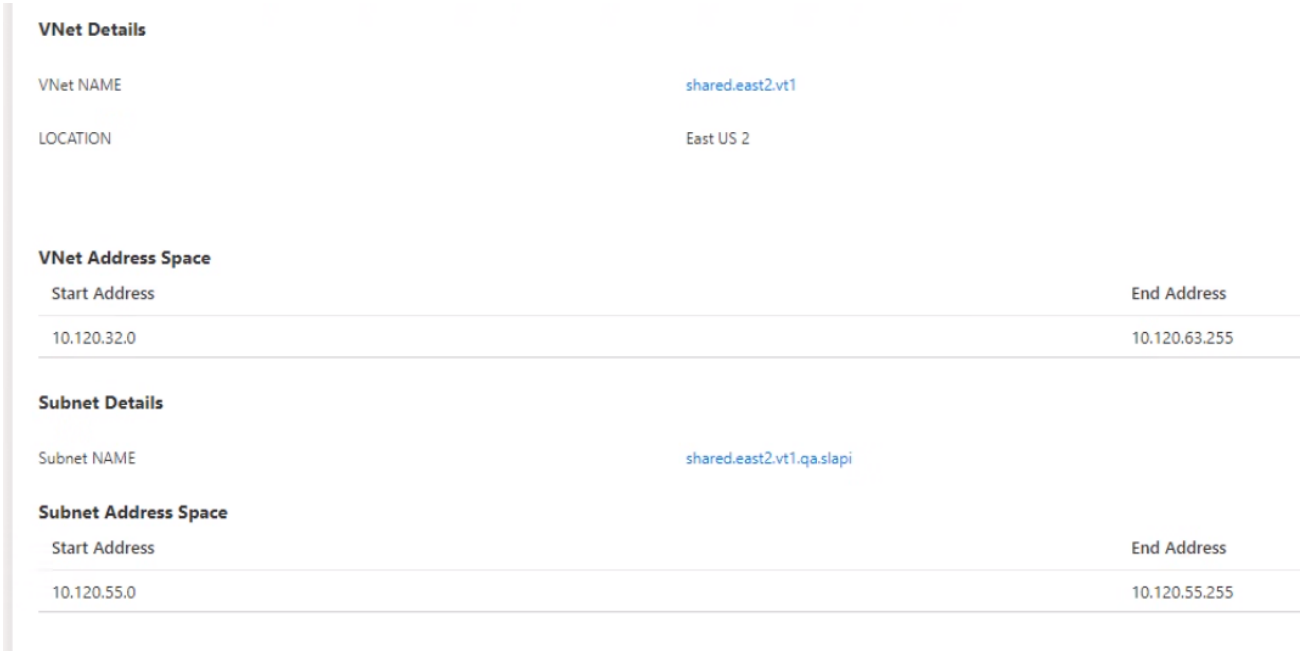
b) Click: Add VNet:



c) In the far right pane fill in the following:
   i) Subscription – should fill in with the default/same Subscription as the API was created under
   ii) Virtual Network – select the shared.east2.vt (East US2) unless directed to use another network
   iii) Ensure Select Existing is chosen for the Subnet
   iv) For the Subnet, click on the down arrow for the drop down menu
   v) Then find the appropriate environment that matched the API's and it ends with slapi as shown here



d) Click OK in the lower left of this pane to save the changes



VNet Details

VNet NAME	shared.east2.vt1
LOCATION	East US 2

VNet Address Space

Start Address	End Address
10.120.32.0	10.120.63.255

Subnet Details

Subnet NAME	shared.east2.vt1.qa.slapi

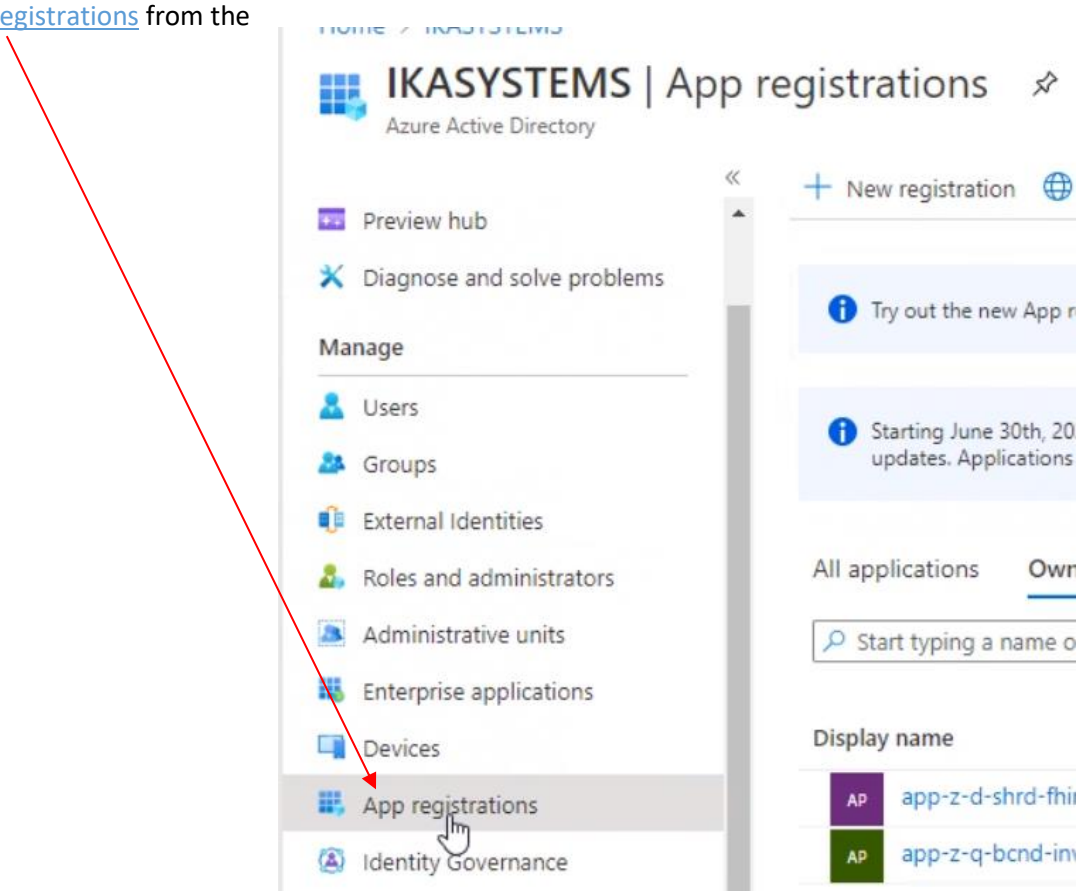
Subnet Address Space

Start Address	End Address
10.120.55.0	10.120.55.255

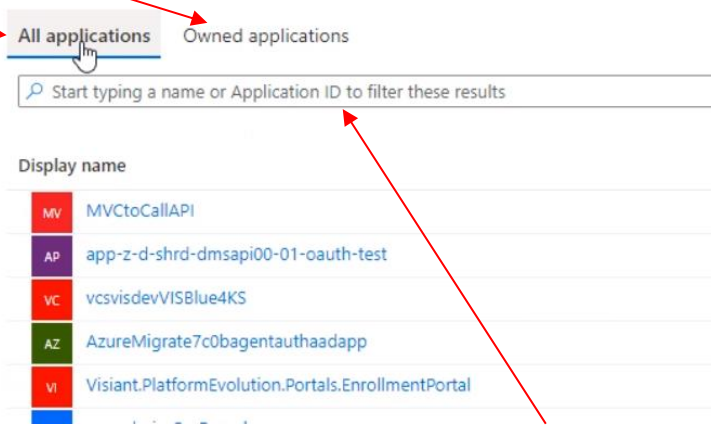
e) This should conclude the API Service creation. Next we will move on to API Management setup.

4) Configure App Registration: Home → Azure Active Directory → App Registration

a) Select the App registrations from the middle pane

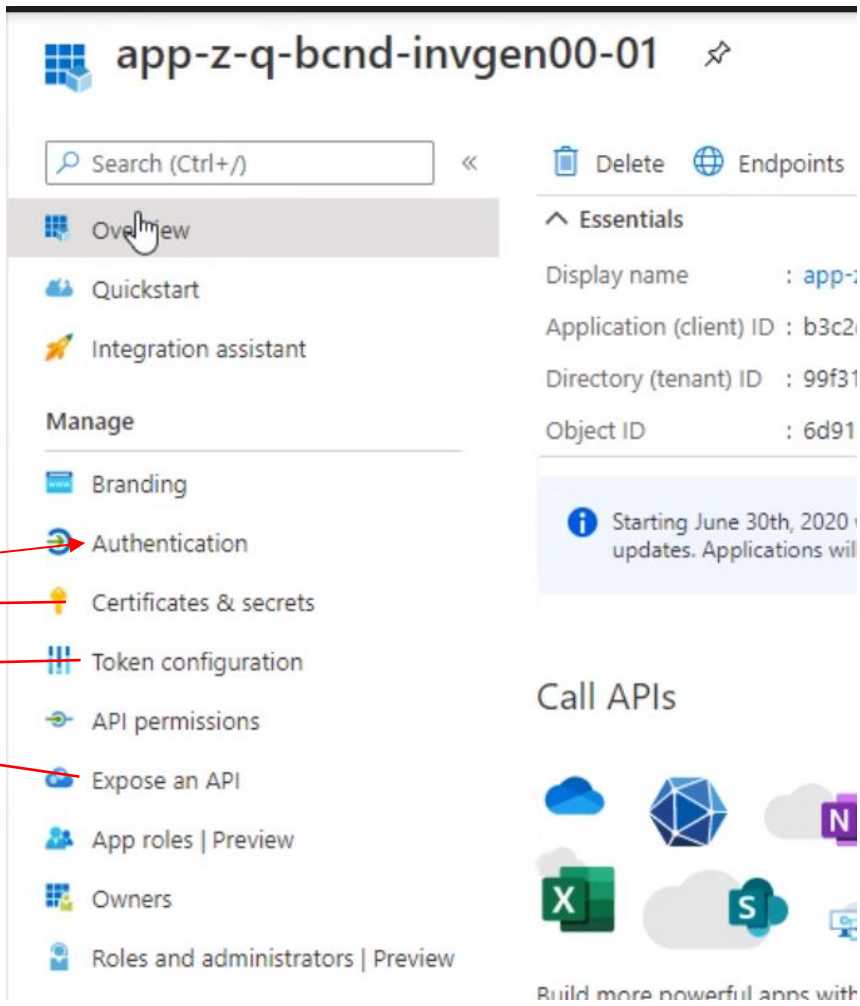


b) On the following screen you will be on the Owned applications by default. These show the APIs you created, if you did not create the API then you need to look under the All applications:



c) If you need to use All applications, you will need to type the specific application name in the search bar and then select it from the list (e.g. app-z-q-bcnd for app-z-q-bcnd-invgen00-01)

d) Next you will see a screen similar to this:



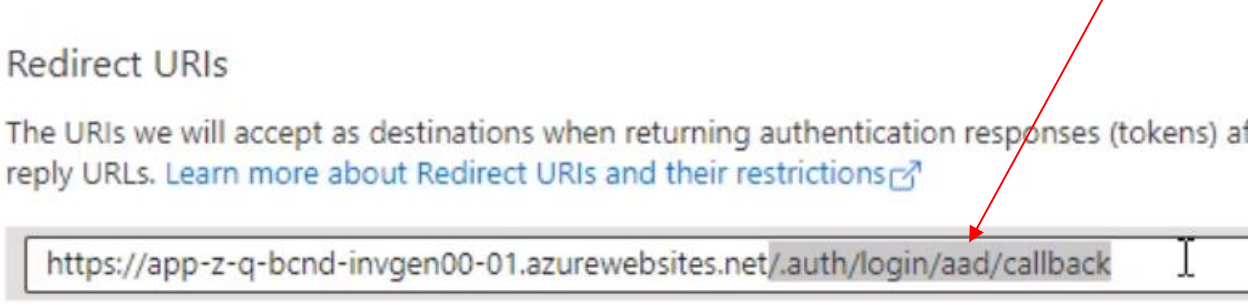
e) From the center panel, select Authentication.

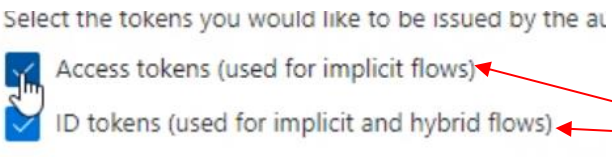
#1

#2

#3

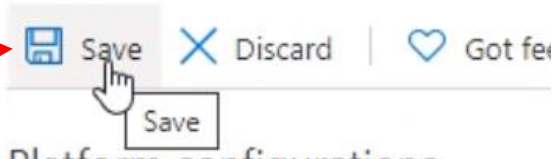
f) Verify the Redirect URI is correct (e.g. https://APIServicename.azurewebsites.net/.auth/login/aad/callback)





g) Next under Implicit grant and hybrid flows select the Access tokens check box and leave ID tokens checked also.

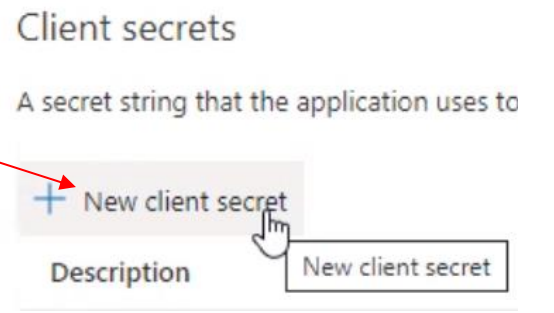
h) Lastly, click on Save at the top of the screen:



See #1 above

i) Now select Certificates & Secrets in the middle pane

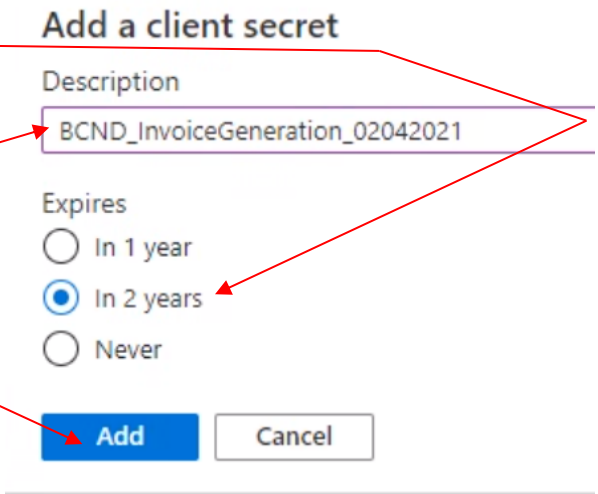
j) Under Client secrets click New client secret:

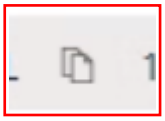


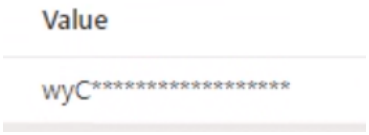
k) The following pop up window will appear, select the Expires in 2 years radio button

l) Supply a meaning full Description for the Client secret

m) Then click on Add

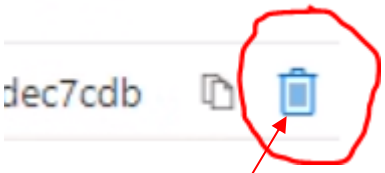


n) Click on the icon to the right of the Value you just created  to copy it to the clipboard and record it in the appropriate place

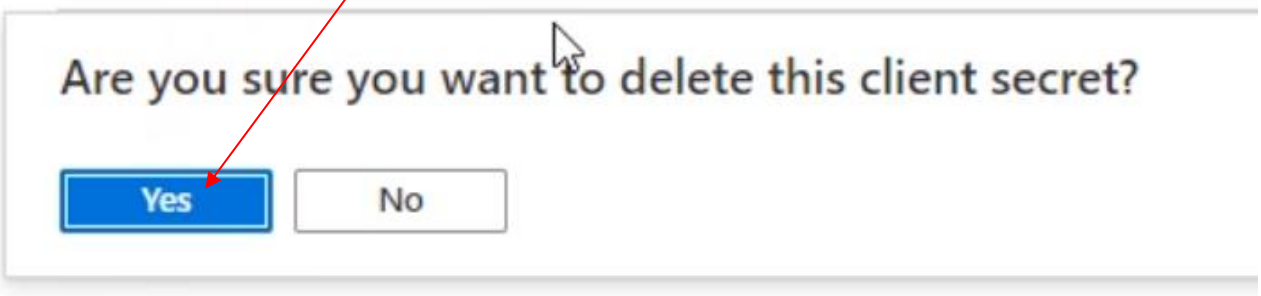


o) IMPORTANT – Before changing screens, copy the Value that was created as it will become hidden as shown on the left.

p) Lastly, delete the secret that was auto generated and does not have a description by clicking on the blue trash can to the right of the ID number



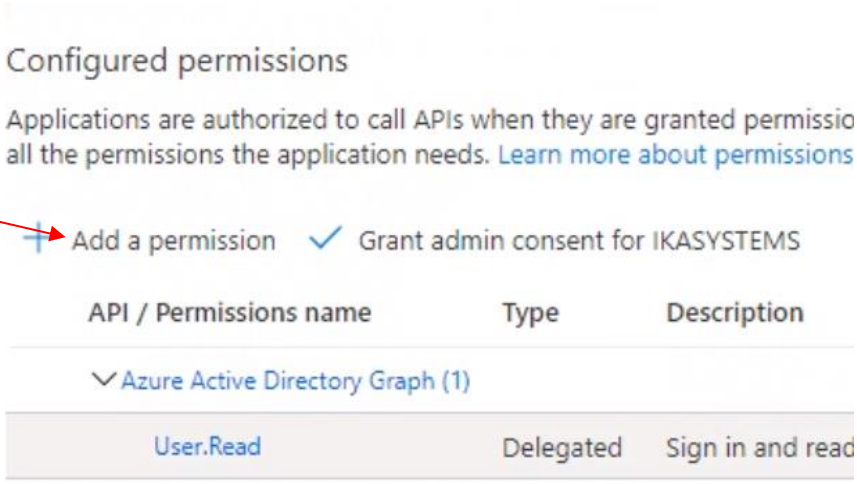
q) On the pop up window select Yes to confirm the deletion



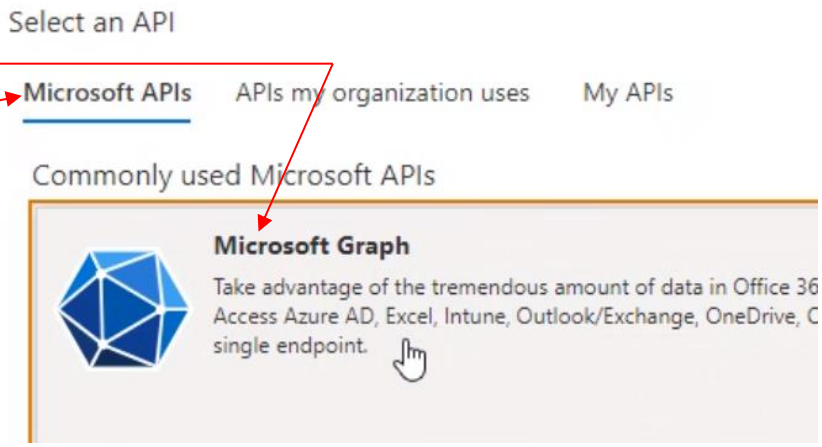
r) Select API permissions in the middle panel

See #2 above

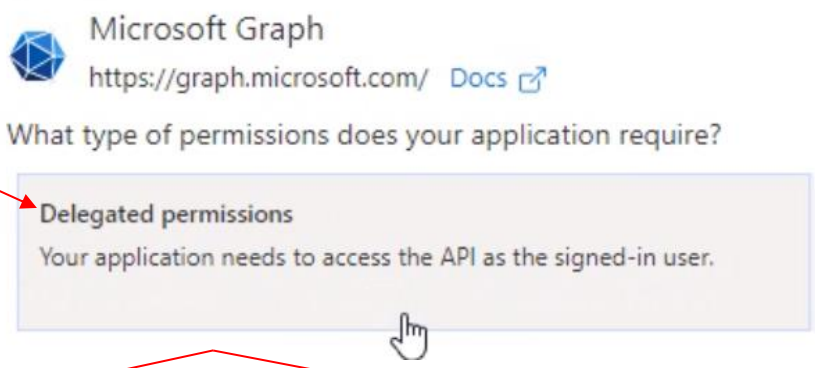
s) Under Configure permissions, select Add a permission



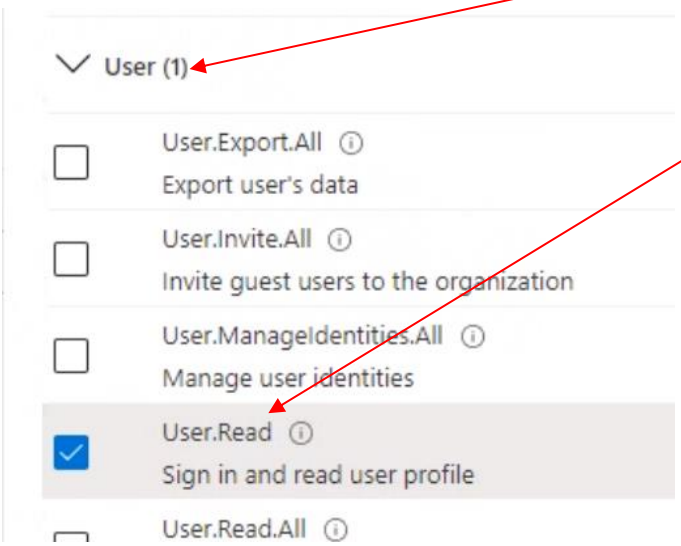
t) Then select the Microsoft Graph under the Microsoft APIs



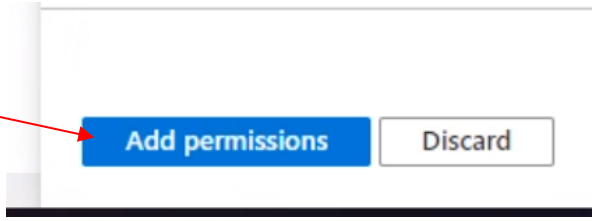
u) Select the Delegated permissions block



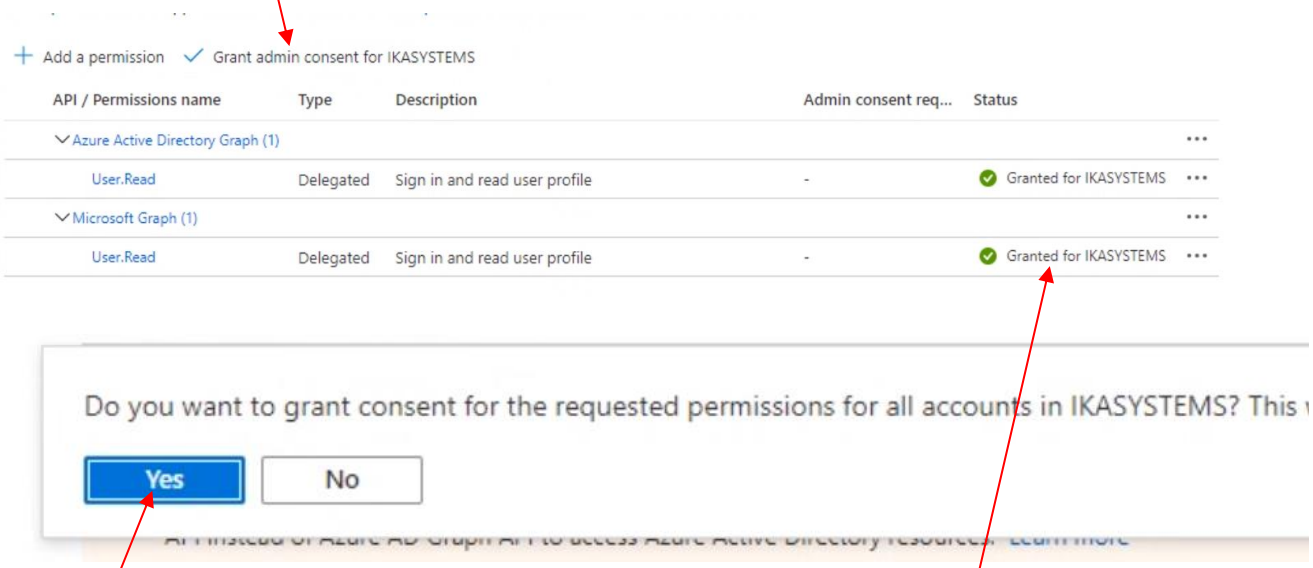
v) Scroll down the list and find User, expand the list and select User.Read only as shown here:



w) Now select Add permissions at the bottom of the window:



x) Next click on Grant admin consent for IKASYSTEMS (if you have permission)



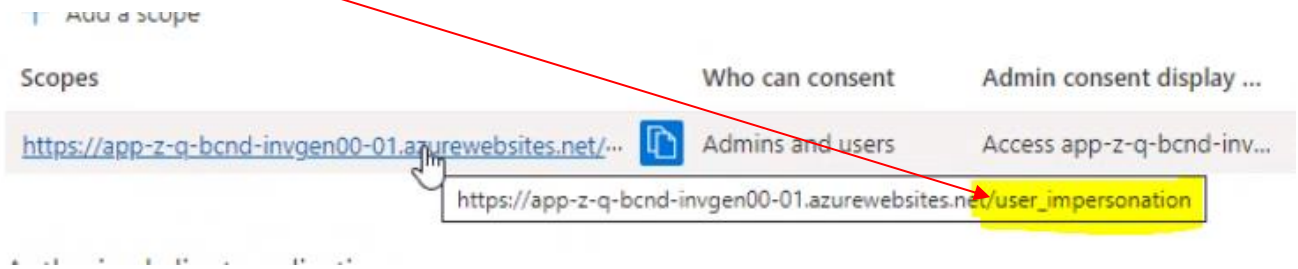
y) Click Yes in the pop up window to complete the action:

z) Finally under the Status column you will see that the permission has been granted

aa) Select Expose an API

See #3 above

bb) Look under the Scopes verify the scope name as https://APIServicename.azurewebsites.net/user_impersonation Emphasis being that the link ends with user_impersonation

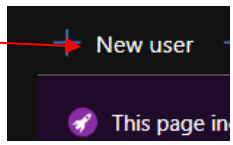


5) Set up the Client AD user Account: Home → Azure Active Directory → Users

a) Before proceeding, if you have not and need to create a new client user account for the App Service, please follow the steps outlined here:

i) Go to Home → Azure Active Directory → Users

(1) Click on New user



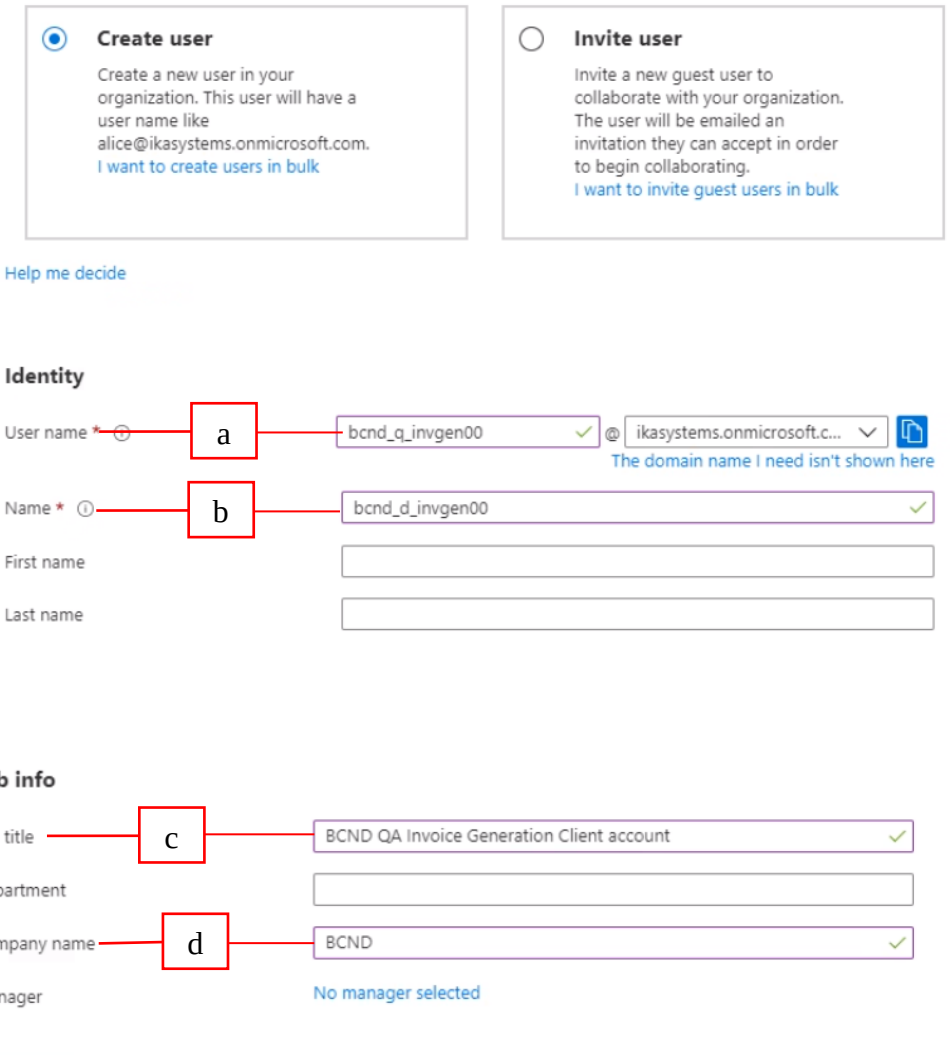
(2) Account naming should be as follows

(a) Client (4 Characters)

(b) Environment (1 character)

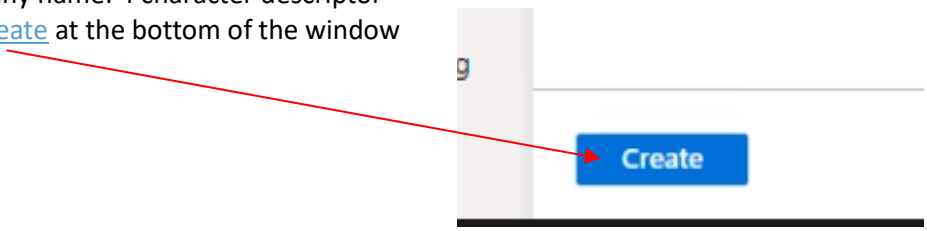
(c) API functional name/purpose (8 characters)

(d) (example bcmi_p_billntfy = Blue Cross Michigan_PROD_Biller Notification)



(3) Fill in the following fields for the new user account:
   (a) User name: as described above
   (b) Name: use the same as the User name
   (c) Job title: Client-Environment-App Function (see example)
   (d) Company name: 4 character descriptor

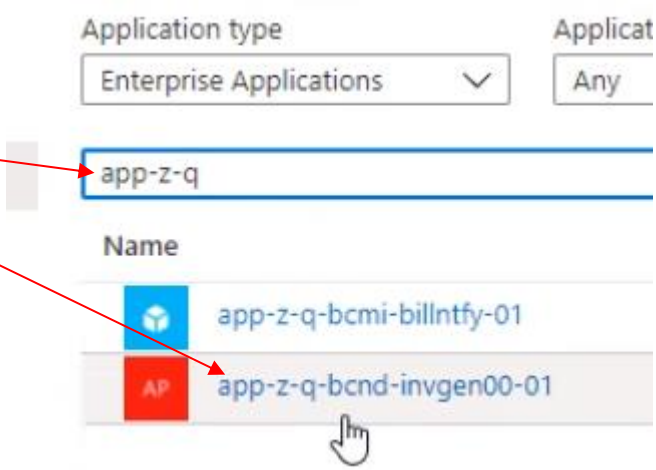
(4) Click on Create at the bottom of the window

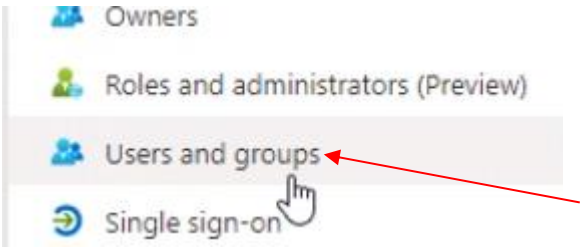


6) **Set up the Enterprise application: Home → Azure Active Directory → Enterprise applications**

a) To find your application, you will need to type the specific application name in the search bar and then select it from the list (e.g. app-z-q-bcnd for app-z-q-bcnd-invgen00-01)

b) Then select the application from the list

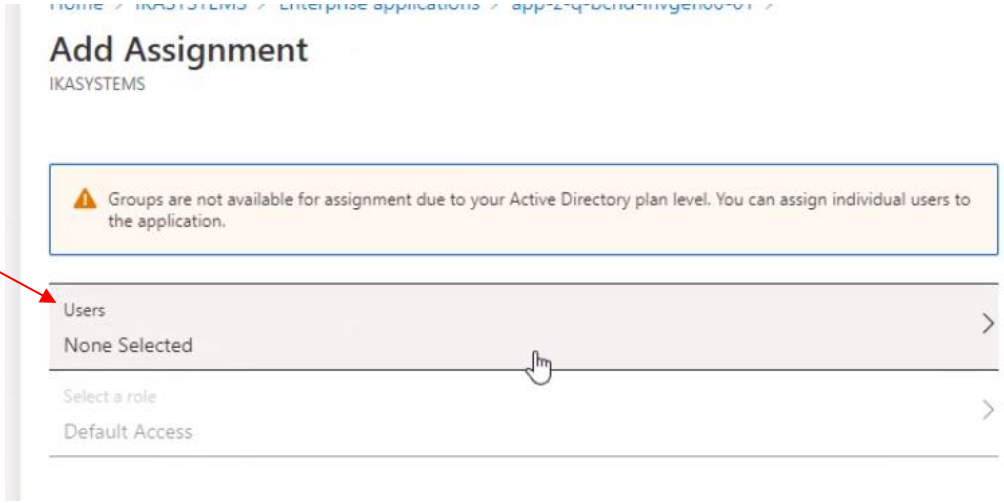




c) On the next screen, from the middle panel, select Users and Groups

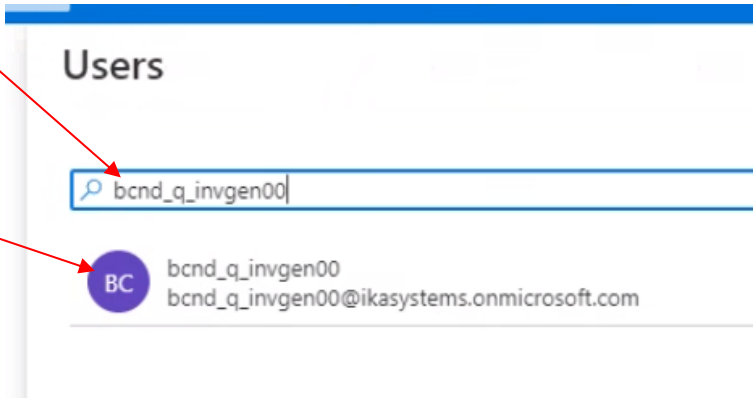
d) Select Add user/group

e) On the next screen under the Add Assignment, click on the Users bar



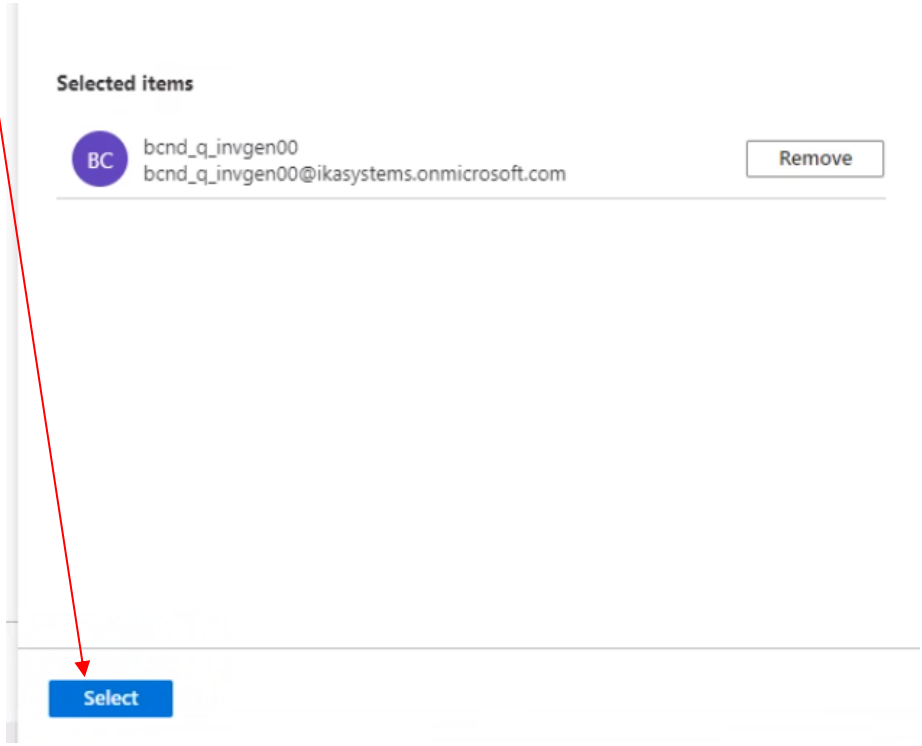
f) On the far right of the screen under Users, type in the name of the account you want to add

g) Click on the user to add it to the Selected items list lower in the screen

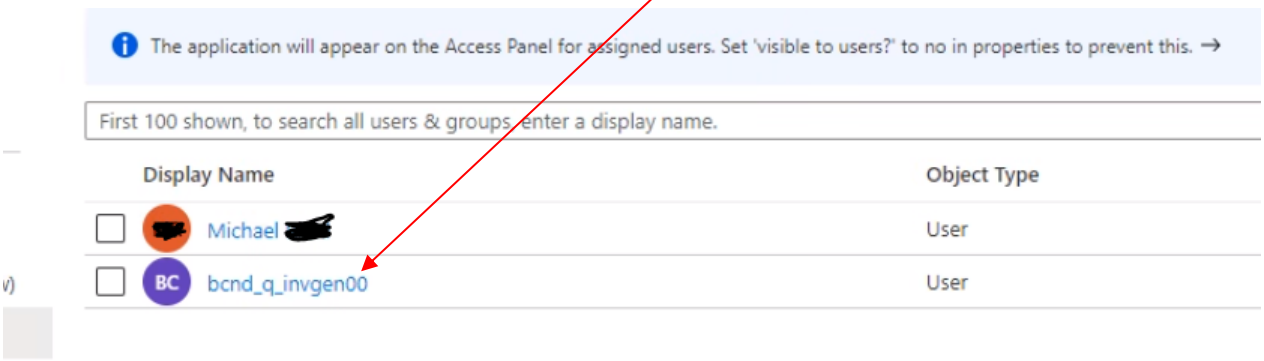


h) Then click the Select button at the bottom

i) Finally click on Assign in the lower left of the screen



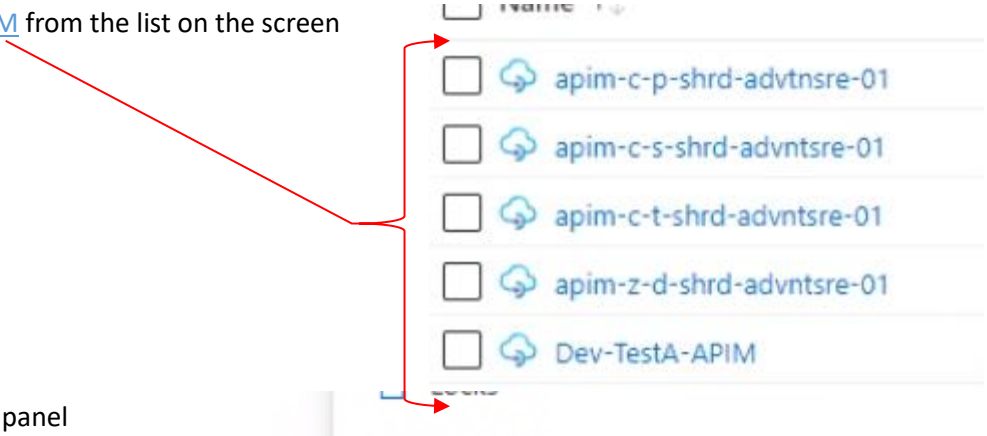
j) You should now see the account in the list as shown here



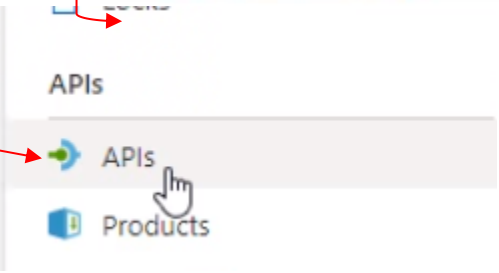
7) In Azure AD, navigate to Enterprise Applications again. Find and select your app registration like you did in 6a above and go to Properties. Set "User Assignment Required" to Yes. Click on Save.

8) Configure API to API Management Service: Home → API Management Services

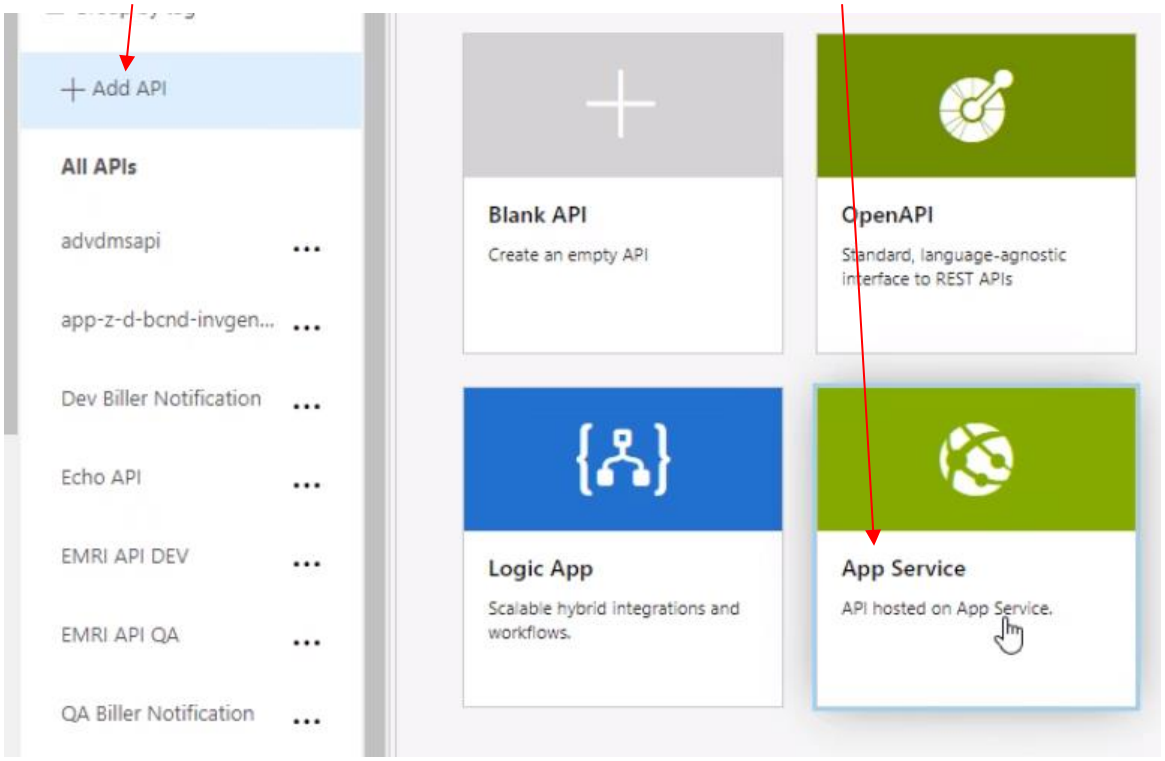
a) Select the appropriate APIM from the list on the screen



b) Click on APIs in the middle panel

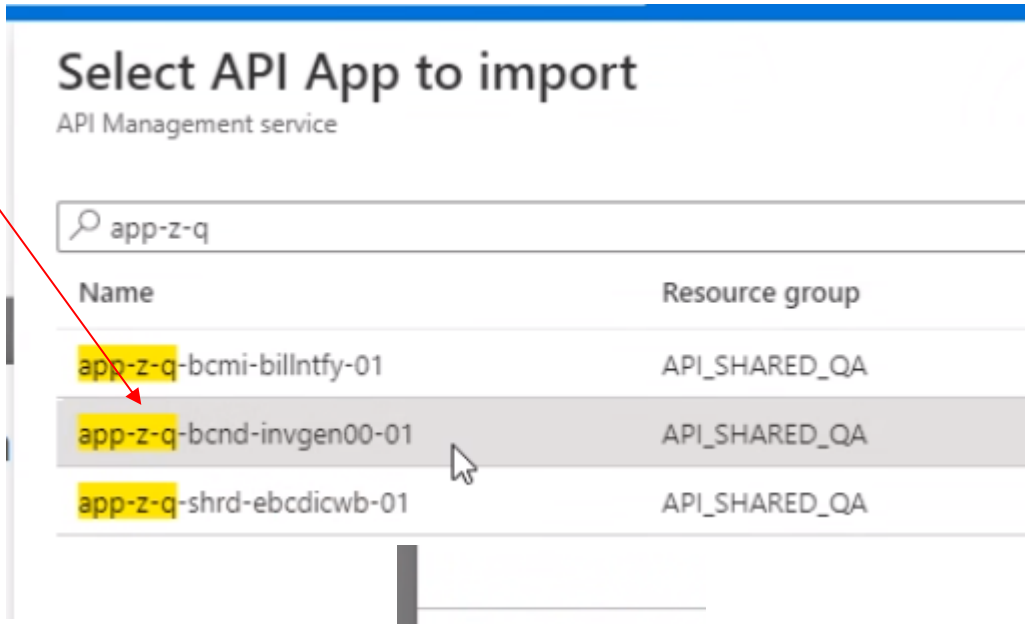


c) Be sure the Add API option is selected in the third column, the select App Service to add the service



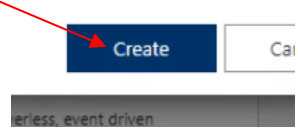
d) The following screen appears

i) Click the Browse button to locate and select the App

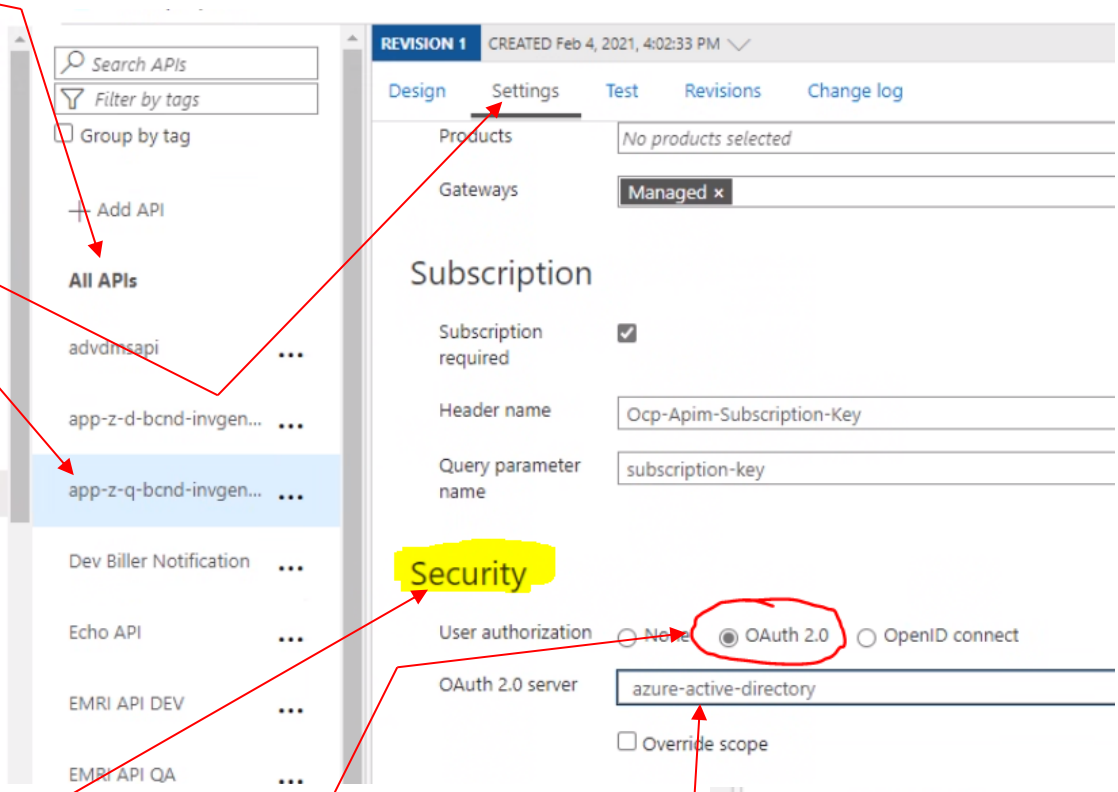


ii) Click on Select in the lower left of the window

iii) Display name: Use the App Service/API name (e.g. app-z-q-bcnd-invgen00-01)
iv) Name: Use the App Service/API name (e.g. app-z-q-bcnd-invgen00-01)
v) API URL suffix: Use a logical short name such as environment-client-function e.g. qa-bcnd-invgen)
vi) Base URL: Automatically self populates (Note: this is also known as the DNS record for the App
vii) Click on Create



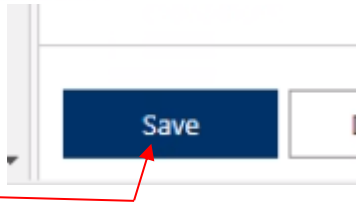
e) Under All APIs find and select your attached API and click on Settings in the window to the right



i) Scroll down and find Security

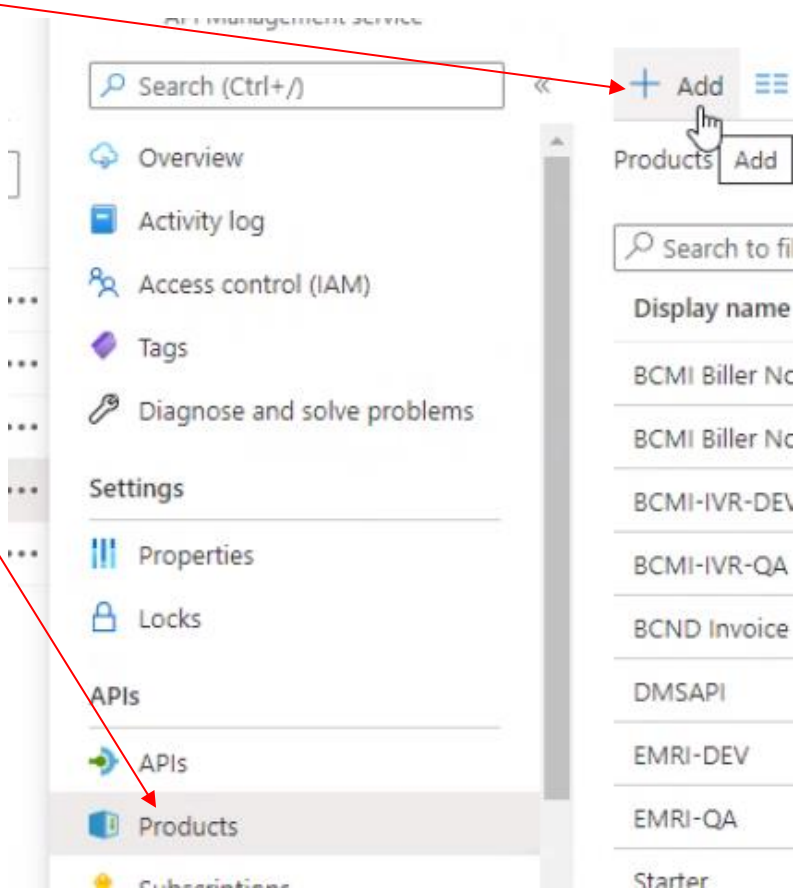
ii) Next to User authorization click the OAuth 2.0 radio button

iii) Next click the arrow for the drop down for OAuth 2.0 server and select azure-active-directory

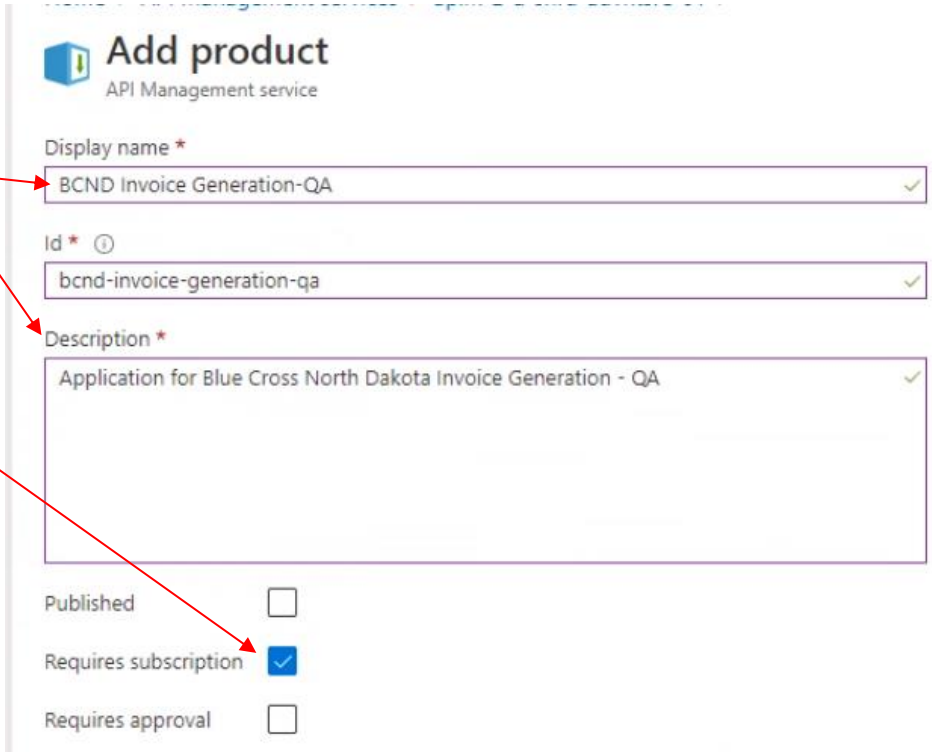


iv) Then click on Save at the bottom

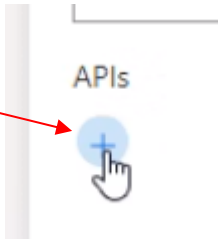
f) Click on Products and click on Add



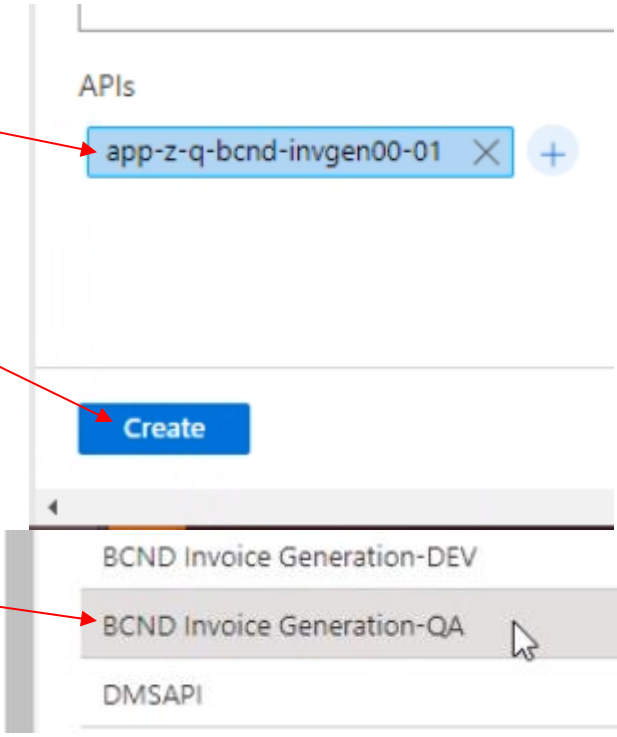
g) Fill in the Display name: client function-environment
h) Add a Description
i) Leave the check box for Requires subscription checked



j) Next, click on the "+" under APIs

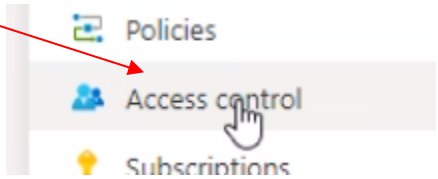


k) Type in the name of the Application Service/API you created and select it
l) Finally click on the Create button

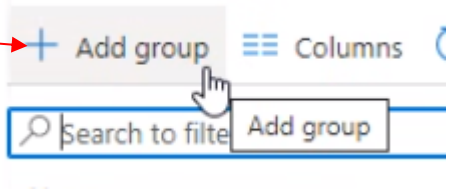


m) Find the App in the list and click on it to select it

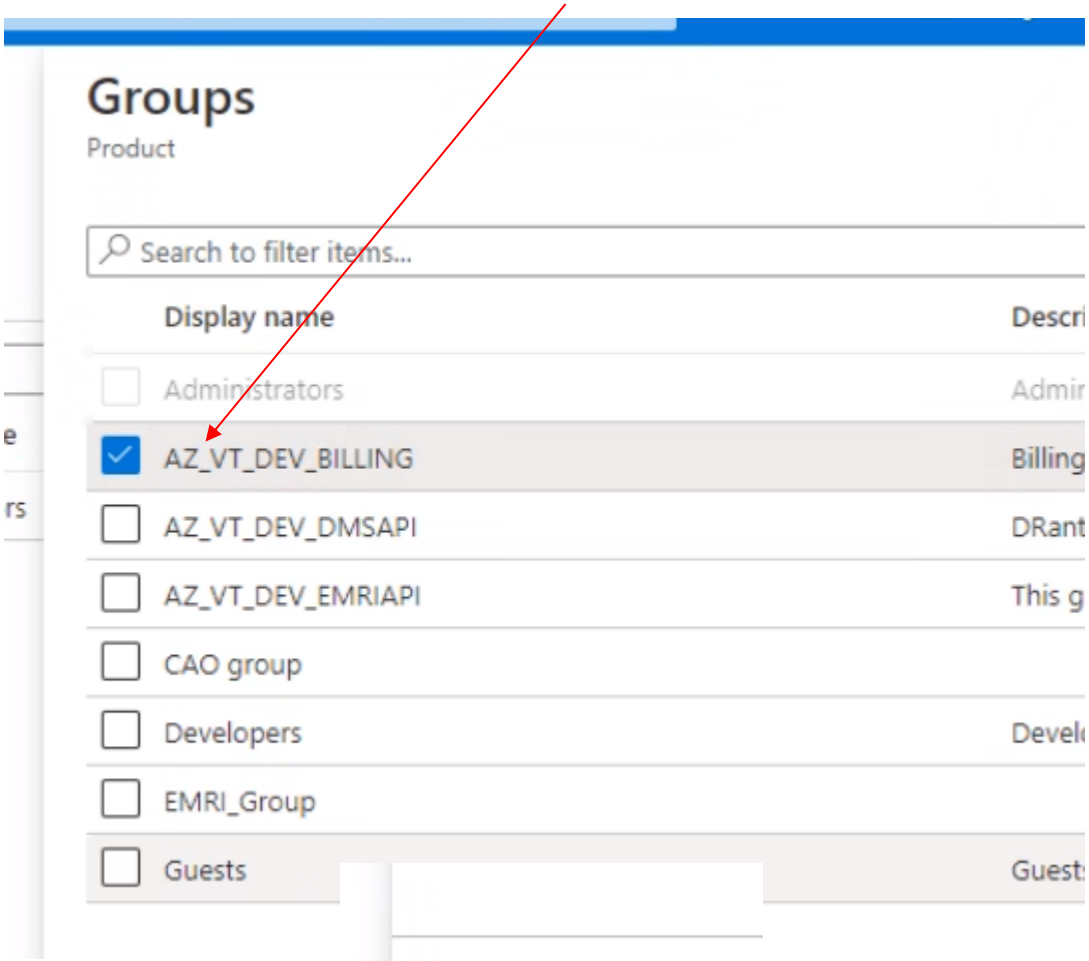
n) Click on Access control from the left pane



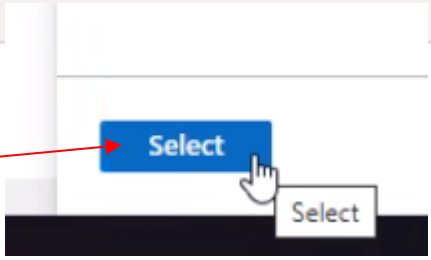
o) Now click on Add group at the top



p) From the window that appears find and select the group(s) to be added

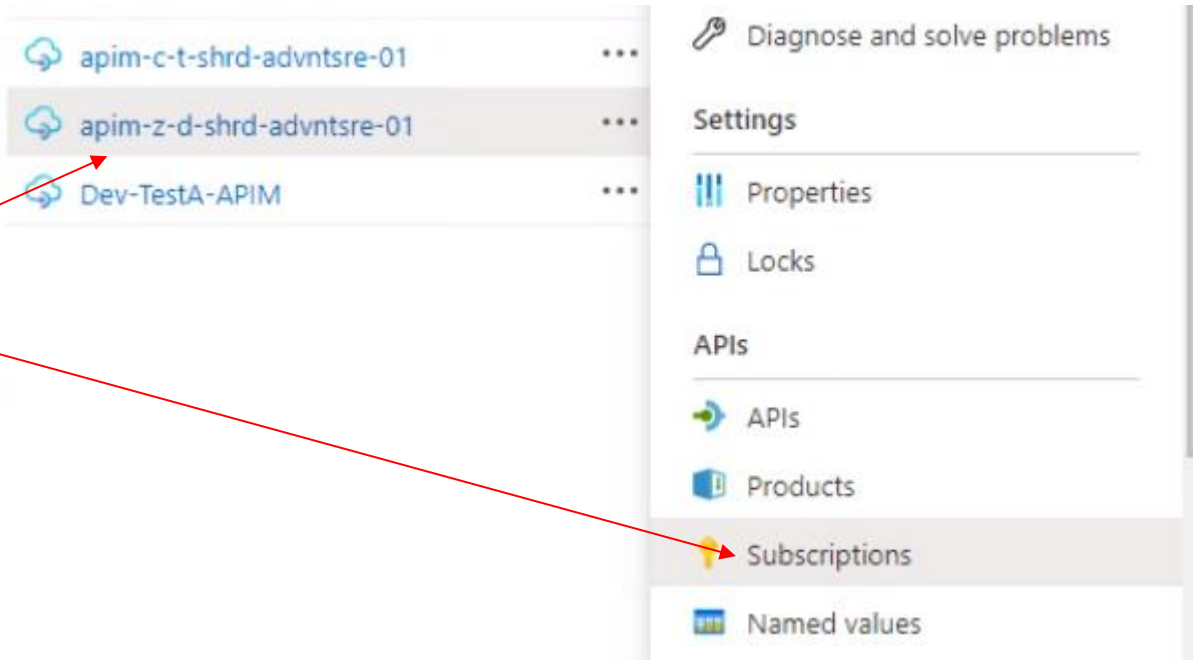


q) Press Select at the bottom

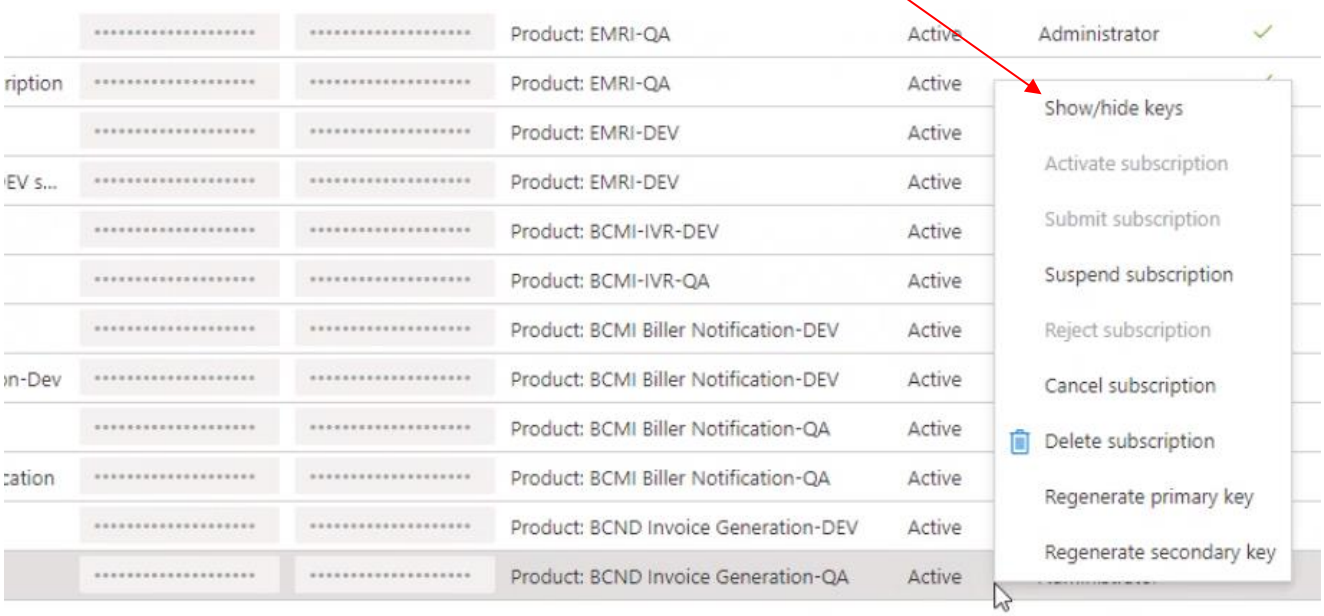


r) You should now see the group(s) you added in the Access control list

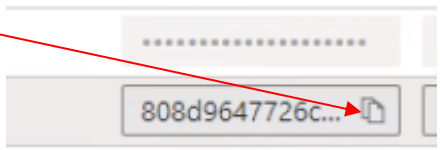
9) Go back to the main APIM page and select the appropriate APIM if necessary the click on Subscriptions



10) Find the Product you just created and click on the … at the far right of it or right click on the product and select Show/hide keys

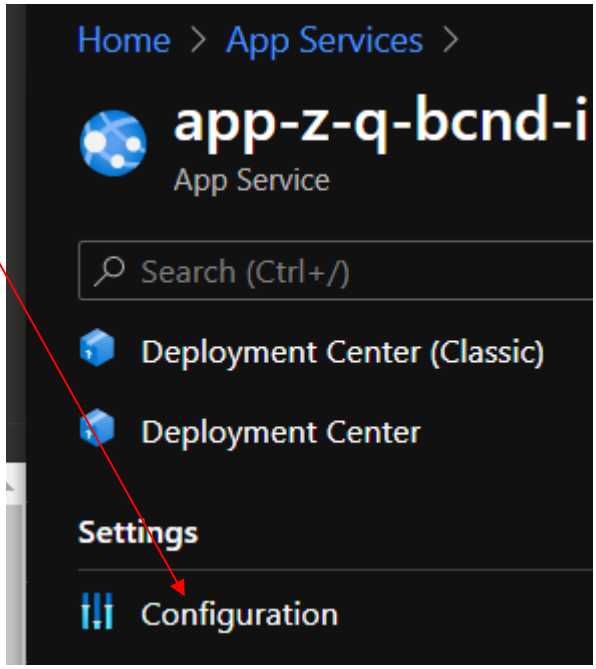


11) Click on the "Copy to clipboard" icon under the Primary key and record this in the build document

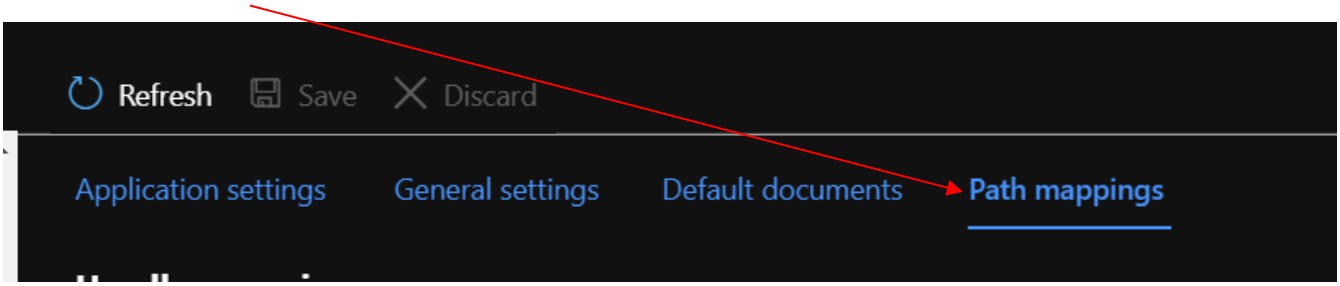


12) Optional if required Create Microservices for the App Service: Home → App Services

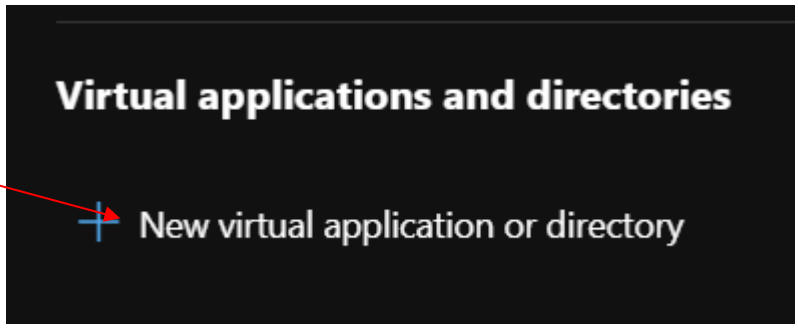
a) From the center panel select Configuration



b) Next select Path Mappings from the right panel

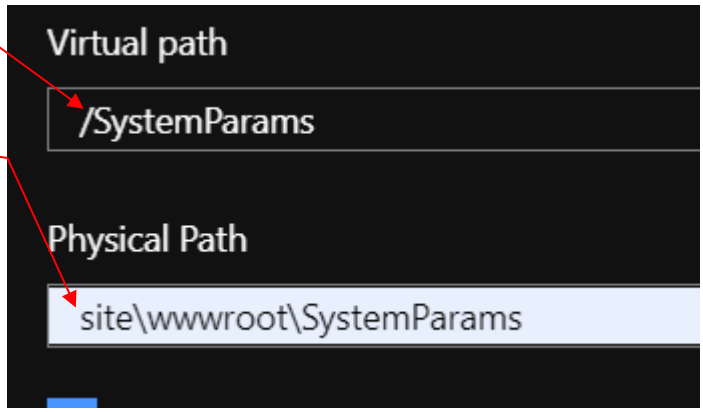


c) Under the Virtual applications and directories click on New virtual application or directory

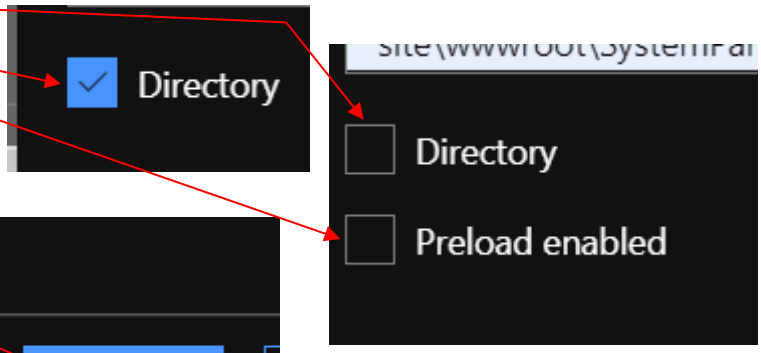


d) On the next window that opens up fill in the following:

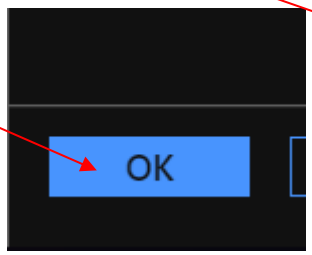
i) Virtual Path: This is the virtual folder name (e.g. /newfolder)
ii) Physical Path: This is the physical location of the virtual folder (e.g. site\wwwroot\newfolder)
iii) Note: The virtual path and physical path names should be the same as show above (e.g. newfolder)



iv) Uncheck the box for Directory and leave the other check box for Preload enabled unchecked



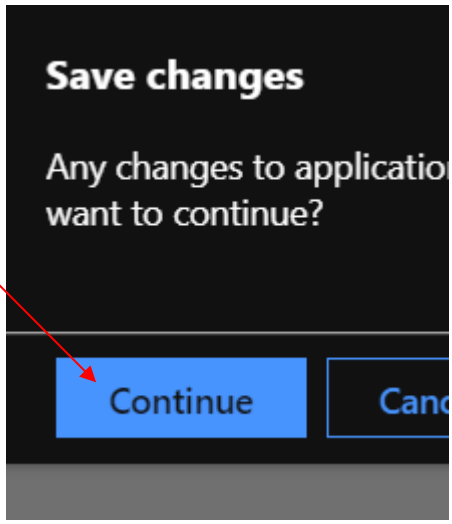
v) Click OK at the bottom of the screen to complete the creation



vi) Repeat steps i though v above for any additional virtual directories or "Microservices" to be created
vii) Do not refresh the screen until you click on Save at the top, otherwise all the newly created items will be discarded automatically

viii) You can create more than one virtual directory or as many as you like before saving, but be aware of the risks

ix) After clicking on Save you will need to click on Continue to finalize the process



Appendix A:

Check the naming convention confluence page for existing names

Overall naming scheme:
Service name (Microsoft Name Prefix) - Env - Shrd/Client - App Name - 01

Service name (Microsoft Name Prefix)
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging
Business Unit

- Z – Core Admin
- R – Risk and Quality
- C – Combined (CoreAdmin + Risk and Quality)

Env

- P - Prod
- D - Dev
- Q - QA
- S - Stage
- N - Int
- C - CSB
- R - Training
- T – Test
- TC – Test C
- TG – Test G
- TH – Test H
- U - UAT
- F - Perf
- I - Infrastructure

Shrd/Client (4 Letters)

- Reference client naming scheme

App Name

- 8 Characters
- All lowercase
- Use 0 as filler character at end

Number – (2) Optional

EXAMPLES:

app-z-t-bcmi-gwenroll-01
app-r-q-shrd-docwrite-01
apim-z-q-shrd-advntsr0-01
logic-z-p-prem-docwrt00-01
Recommended naming and tagging conventions - Cloud Adoption Framework
Learn detailed resource naming and tagging recommendations aimed specifically at supporting enterprise cloud adoption efforts.