

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

The screenshot shows the 'Create Web App' form in the Azure portal. Red arrows from the instructions on the left point to the following fields in the form:

- Subscription:** VT_SHARED SERVICES
- Resource Group:** API_SHARED_DEV
- Name:** app-z-d-bcnd-invgen00-01
- Publish:** Code (selected)
- Runtime stack:** .NET Core 3.1 (LTS)
- Operating System:** Windows (selected)
- Region:** East US 2
- App Service Plan:** plan-c-d-shrd-slapi00-01 (P1v2)
- Sku and size:** Premium V2 P1v2

The form also includes a 'Review + create' button at the bottom left and a 'Next : Monitoring >' button at the bottom right.

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

Home > App Services > Create Web App

Basics **Monitoring** Tags Review + create

Application Insights is a code-less attach to provide detailed observability in to your application. [Learn more](#)

Application Insights

Enable Application Insights * ☐ No ☒ Yes

Application Insights * appi-z-d-shrd-monitor0-01 (East US 2) [Create new](#)

Region East US 2

- c) Click Next: [Tags](#)
- Application (1)
 - Environment (1) DEV
 - BuildBy (1)
 - BuildDate (1)
 - ClientName (1)
 - Role (1) Application
 - Tier (1) 3
 - Status (1) LIVE

Basics Monitoring **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.

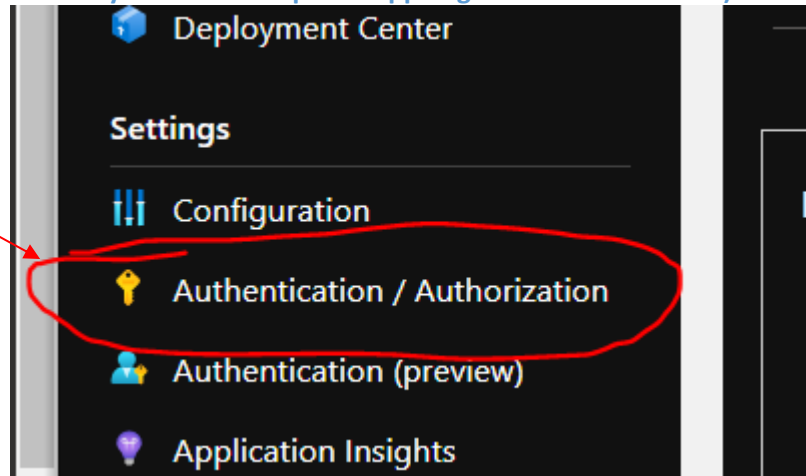
Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
Application	: Invoice Generation	Web App
Environment	: DEV	Web App
BuildBy	: james.lee@advantasure.com	Web App
BuildDate	: 01/22/2021	Web App
ClientName	: BCND	Web App
Role	: Application	Web App
Tier	: 3	Web App
Status	: LIVE	Web App
	:	Web App

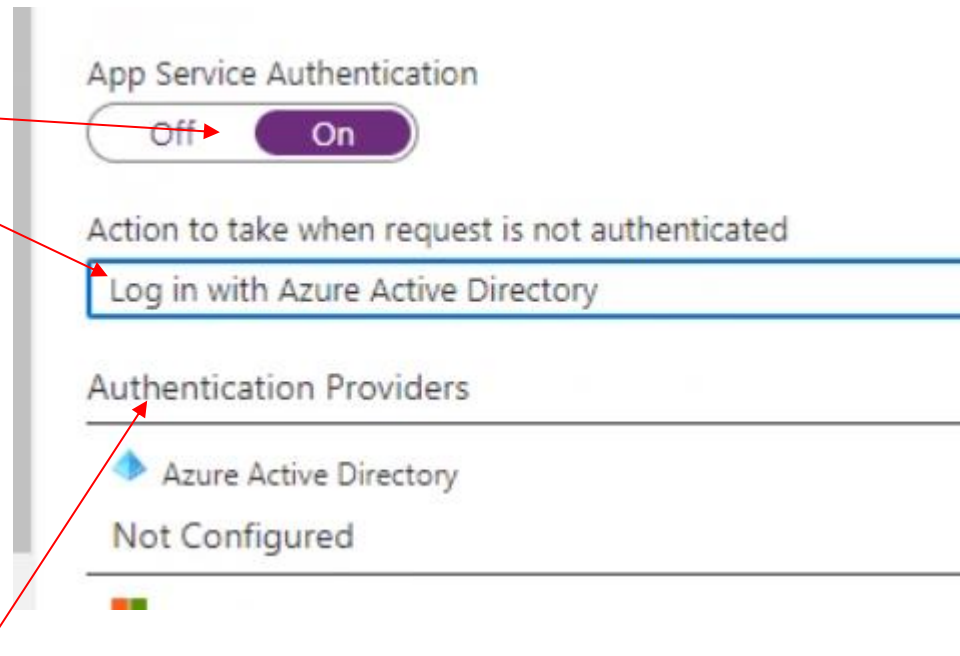
- d) Click: Next: [Review + create](#)
- e) Verify everything is correct, then click: [Create](#)

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

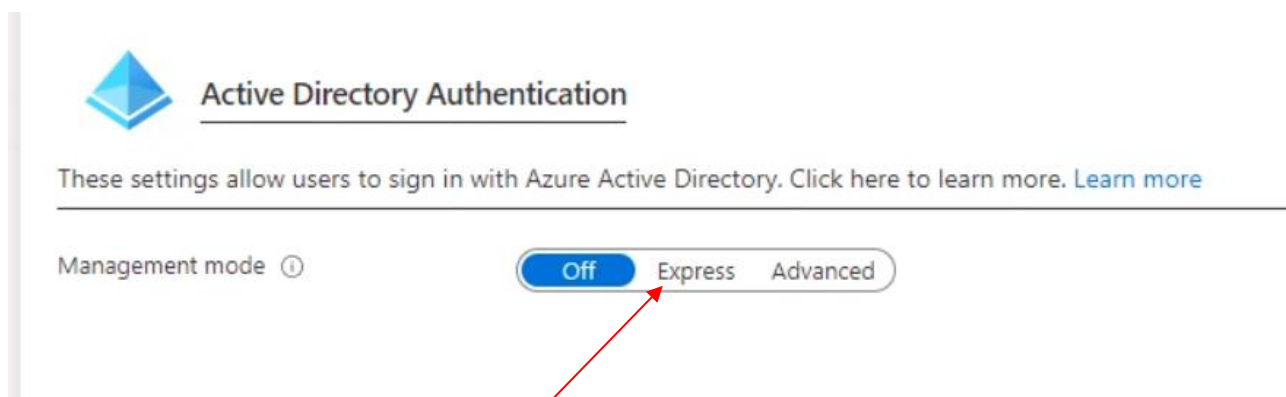
- a) Within the API go to the middle panel and select [Authentication / Authorization](#)



- 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:

Active Directory Authentication

These settings allow users to sign in with Azure Active Directory. Click here to learn more. [Learn more](#)

Management mode ⓘ Off **Express** Advanced

Express mode allows user to create an AD Application or select an existing AD application in your current Active Directory.

Current Active Directory IKASYSTEMS

Management mode Create New AD App Select Existing AD App

Create App * app-z-q-bcnd-invgen00-01

Grant Common Data Services Permissions On **Off**

Save Discard

To enable Authentication / Authorization, please ensure all y...

App Service Authentication Off **On**

Action to take when request is not authenticated Log in with Azure Active Directory

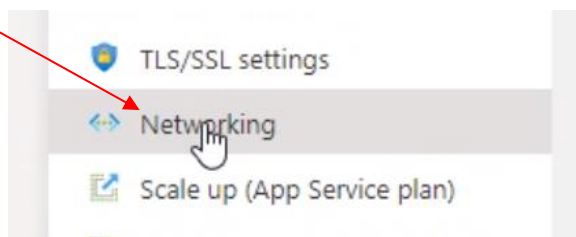
Authentication Providers

- Azure Active Directory
- Configured (Express Mode : Create)

Microsoft

- 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

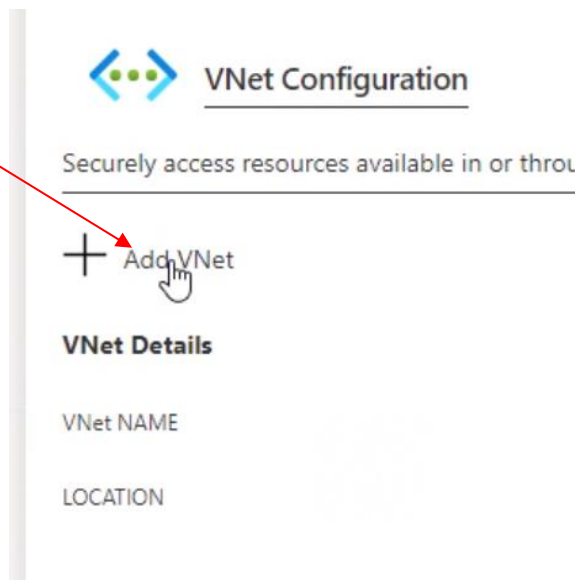
3) Click on [Networking](#) in middle pane of the App Service



a) Now select: [Click here to configure](#) under the VNet Integration section:

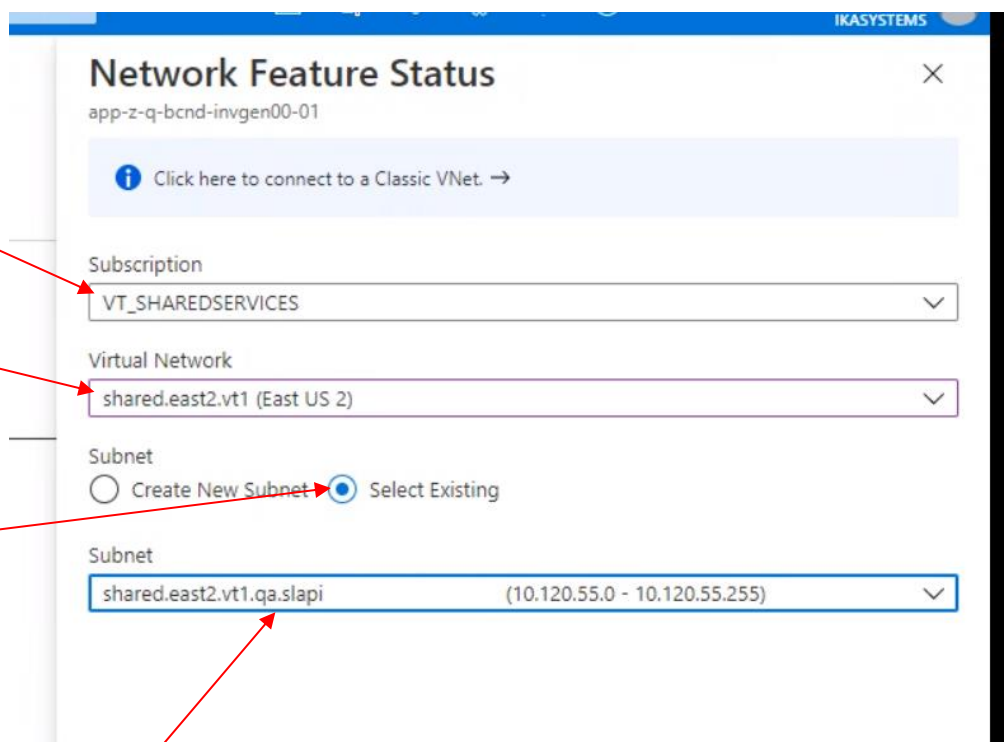


b) Click: [Add VNet](#):



c) In the far right pane fill in the following:

- Subscription – should fill in with the default/same [Subscription](#) as the API was created under
- Virtual Network – select the [shared.east2.vt](#) (East US2) unless directed to use another network
- Ensure [Select Existing](#) is chosen for the Subnet
- For the [Subnet](#), click on the down arrow for the drop down menu
- 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](#)

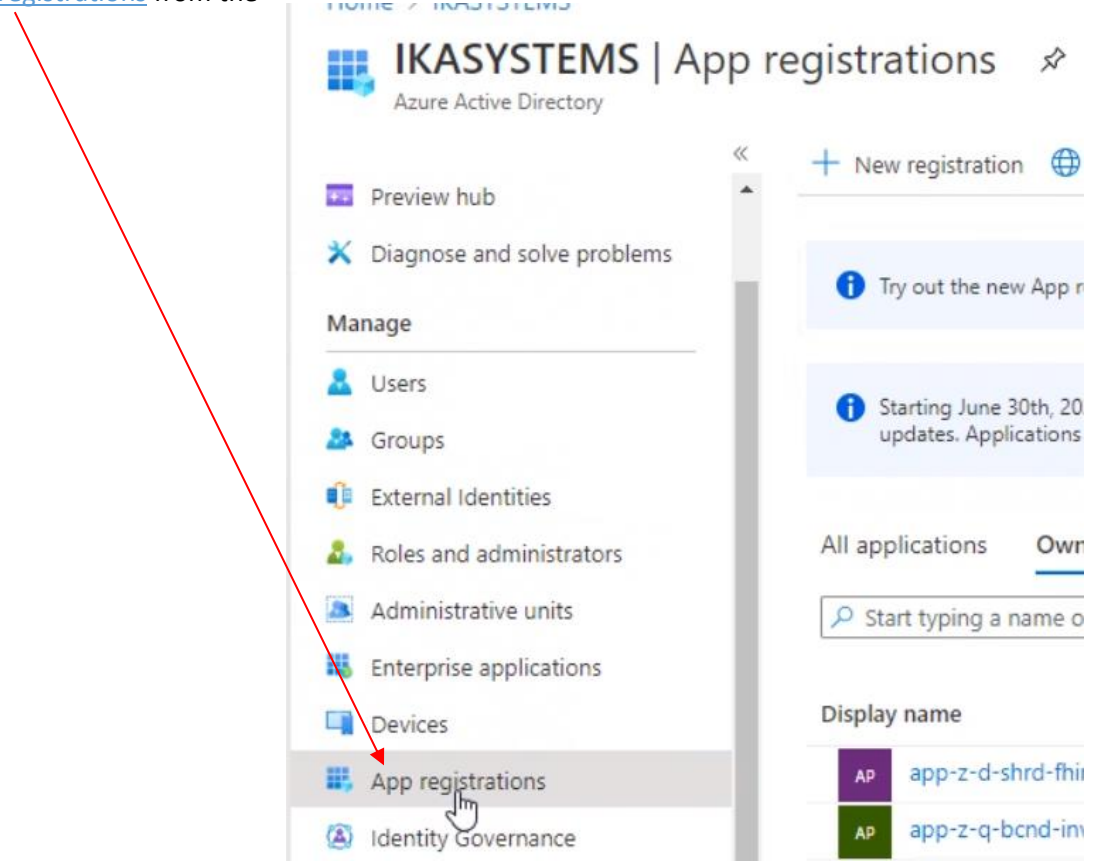
Subnet Address Space

Start Address	End Address
10.120.55.0	10.120.55.255

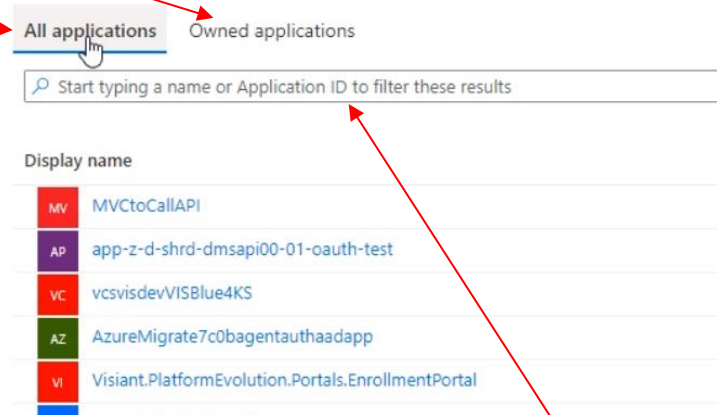
e) This should conclude the API Service creation. Next we will move on to API Management setup.

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

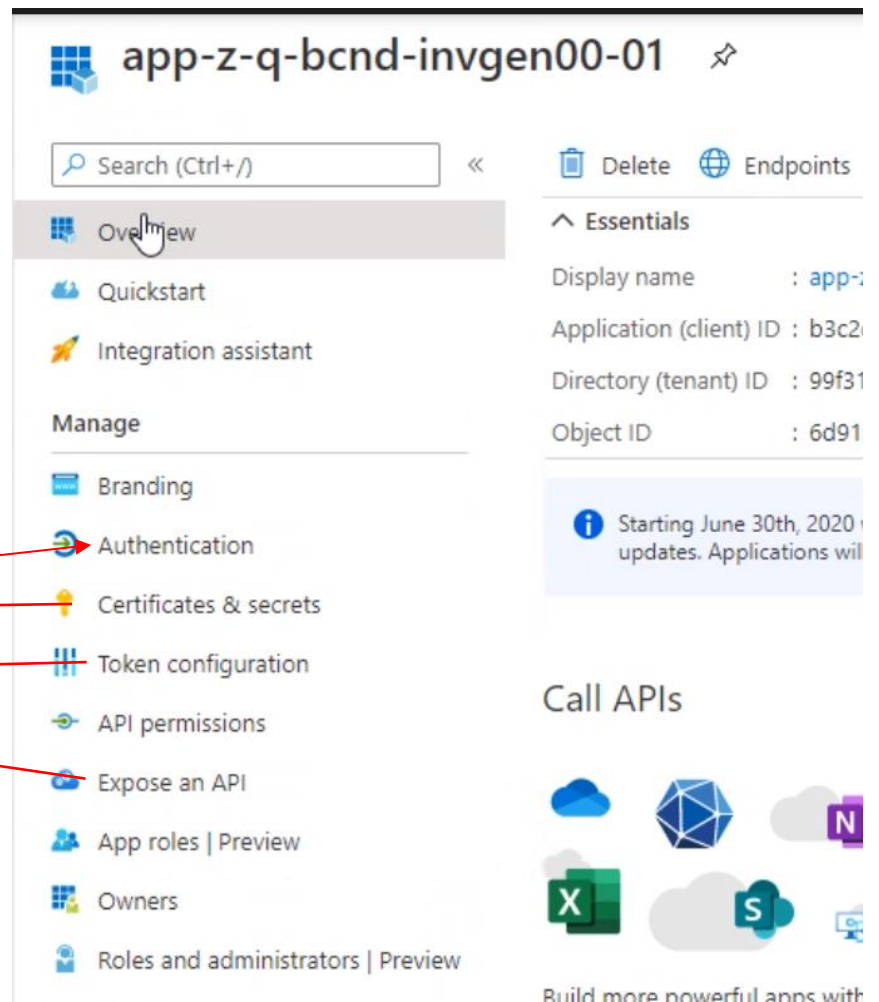
a) Select the [App registrations](#) from the middle pane



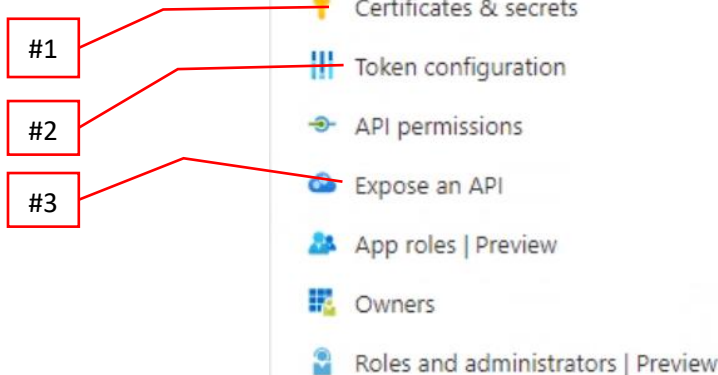
- b) On the following screen you will be on the [Owned applications](#) by default. These show the APIs you created, if you did not create the API then you need to look under the [All applications](#):



- 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](#).



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

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) at reply URLs. [Learn more about Redirect URIs and their restrictions](#)

<https://app-z-q-bcnd-invgen00-01.azurewebsites.net/.auth/login/aad/callback>

Select the tokens you would like to be issued by the application:



☒ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

- 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:

[Save](#) [Discard](#) [Got feedback](#)

See #1 above

- i) Now select [Certificates & Secrets](#) in the middle pane
j) Under Client secrets click [New client secret](#):

Client secrets

A secret string that the application uses to



New client secret

Description

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](#)

Add a client secret

Description

BCND_InvoiceGeneration_02042021

Expires

☐ In 1 year

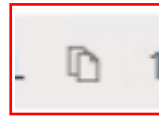
☒ In 2 years

☐ Never

Add

Cancel

- n) Click on the icon to the right of the Value you just created it in the appropriate place

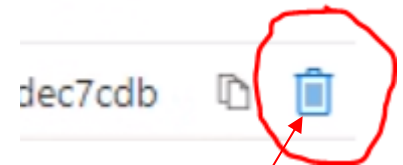


to copy it to the clipboard and record it in the appropriate place

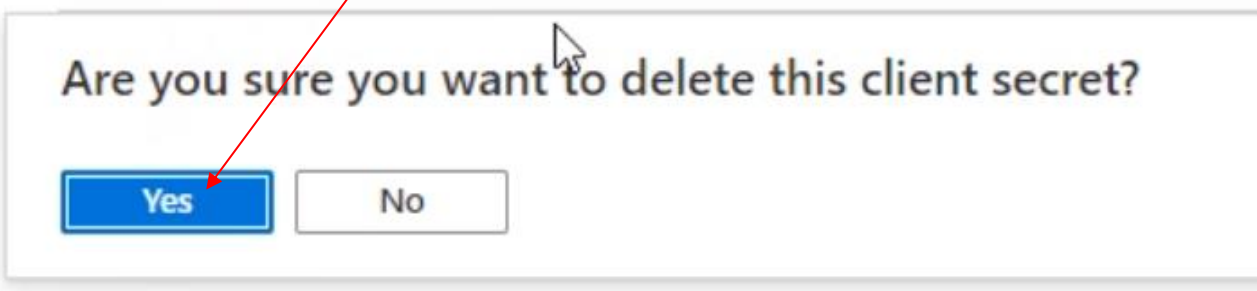
Value
wyC*****

- 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](#)

Configured permissions

Applications are authorized to call APIs when they are granted permission all the permissions the application needs. [Learn more about permissions](#)

[+ Add a permission](#) [✓ Grant admin consent for IKASYSTEMS](#)

API / Permissions name

Type

Description

▼ Azure Active Directory Graph (1)

User.Read

Delegated

Sign in and read

- t) Then select the [Microsoft Graph](#) under the [Microsoft APIs](#)

Select an API

[Microsoft APIs](#)

[APIs my organization uses](#)

[My APIs](#)

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, and more from a single endpoint.

- u) Select the [Delegated permissions](#) block



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.

- v) Scroll down the list and find [User](#), expand the list and select [User.Read](#) only as shown here:

✓ User (1)



User.Export.All ⓘ

Export user's data



User.Invite.All ⓘ

Invite guest users to the organization



User.ManageIdentities.All ⓘ

Manage user identities



User.Read ⓘ

Sign in and read user profile



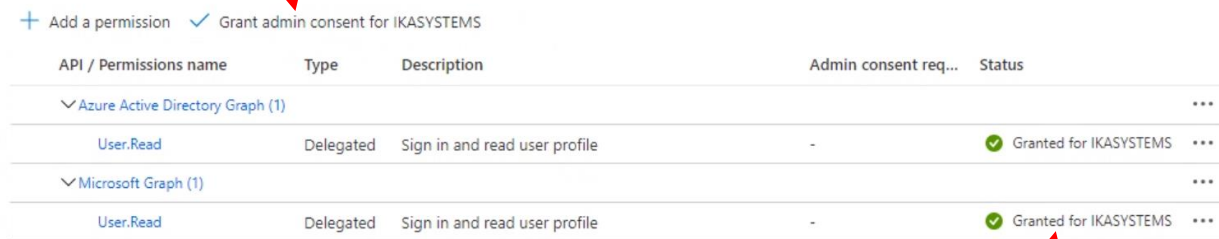
User.Read.All ⓘ

- w) Now select [Add permissions](#) at the bottom of the window:

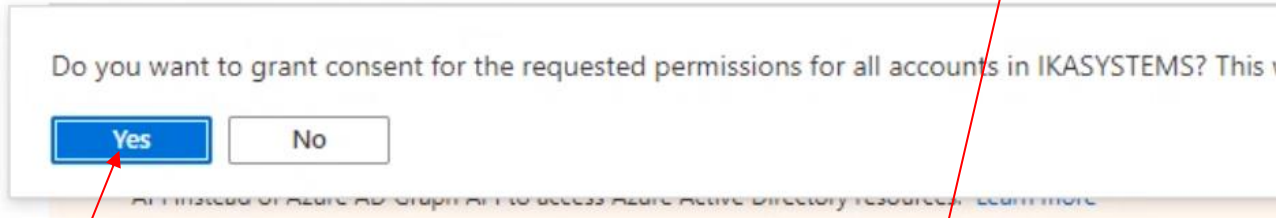
Add permissions

Discard

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



API / Permissions name	Type	Description	Admin consent req...	Status
▼ Azure Active Directory Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	Granted for IKASYSTEMS
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	Granted for IKASYSTEMS



y) Click [Yes](#) in the pop up window to complete the action:

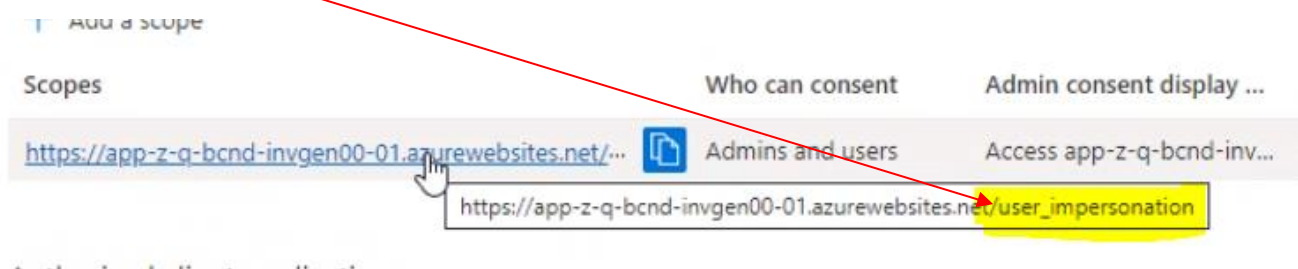
z) Finally under the [Status column](#) you will see that the permission has been granted

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](#)



Scopes	Who can consent	Admin consent display ...
https://app-z-q-bcnd-invgen00-01.azurewebsites.net/...	Admins and users	Access app-z-q-bcnd-inv...

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

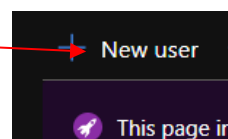
(1) Click on [New user](#)

(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_billIntfy = Blue Cross Michigan_PROD_Biller Notification)

☒ **Create user**
Create a new user in your organization. This user will have a user name like `alice@ikasystems.onmicrosoft.com`.
[I want to create users in bulk](#)

☐ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * ✓ @ 
The domain name I need isn't shown here

Name * ✓

First name

Last name

Job info

Job title ✓

Department


Company name ✓

Manager

(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

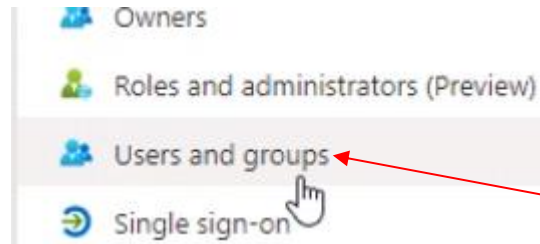
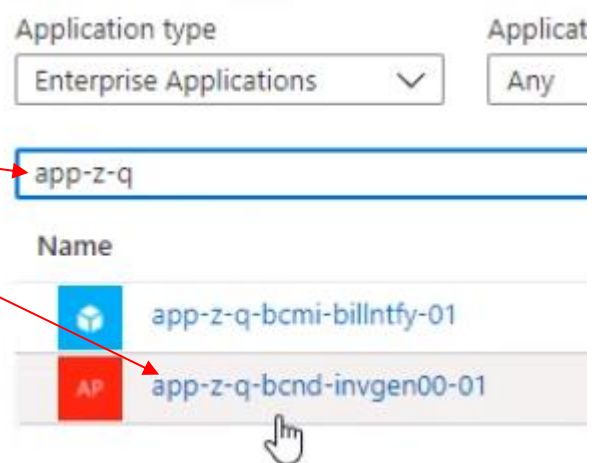


A blue button with the text "Create" in white, located at the bottom right of the form.

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

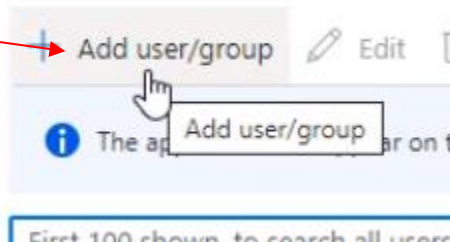
- a) To find your application, you will need to type the specific application name in the [search bar](#) and then select it from the list (e.g. app-z-q-bcnd for app-z-q-bcnd-invgen00-01)

- b) Then [select the application](#) from the list

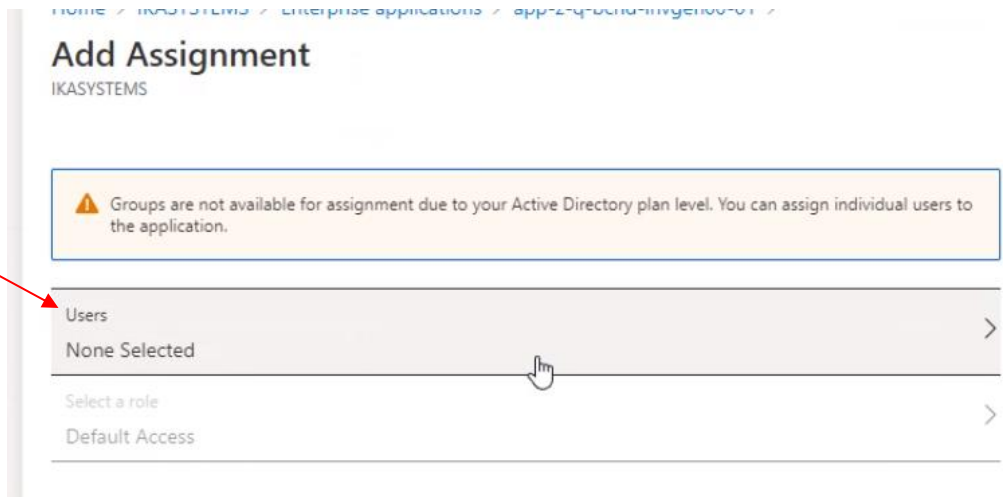


- c) On the next screen, from the middle panel, select [Users and Groups](#)

- d) Select [Add user/group](#)

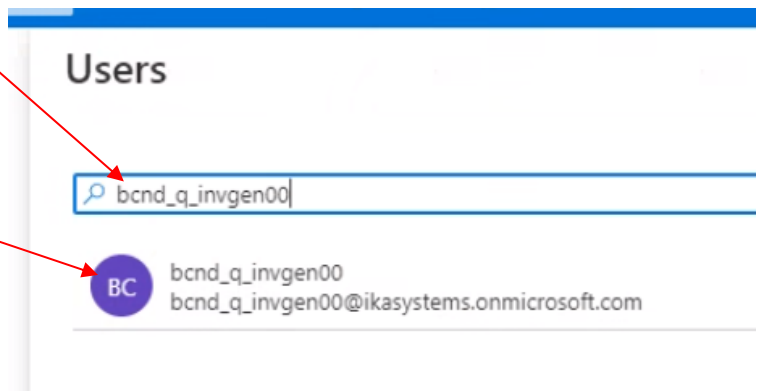


- e) On the next screen under the Add Assignment, click on the [Users](#) bar

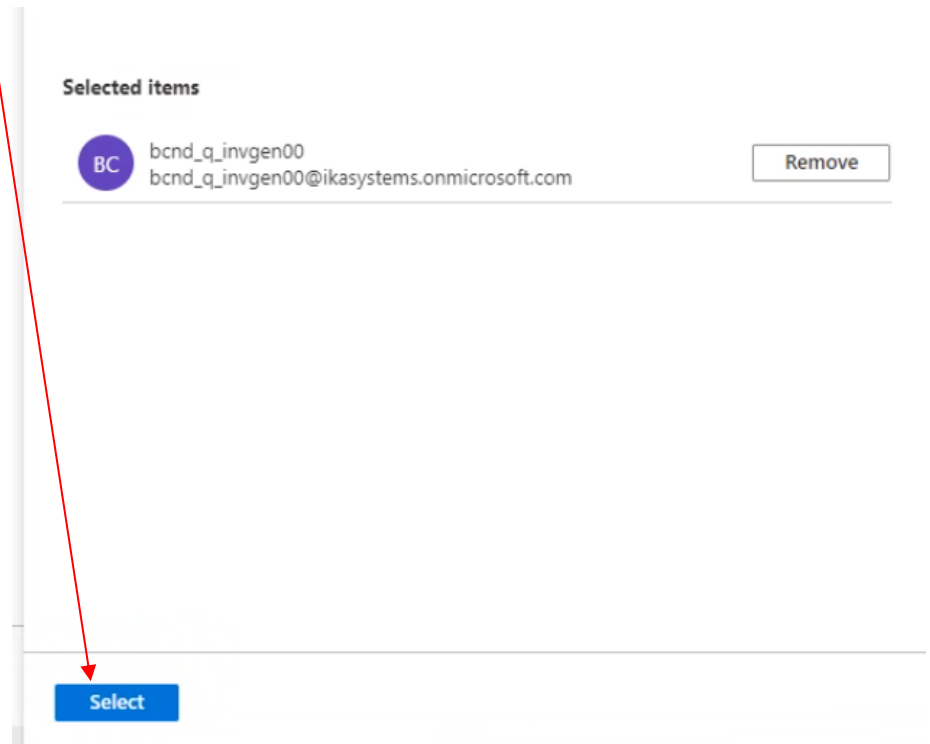
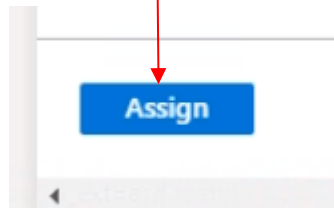


- f) On the far right of the screen under Users, [type in the name](#) of the account you want to add

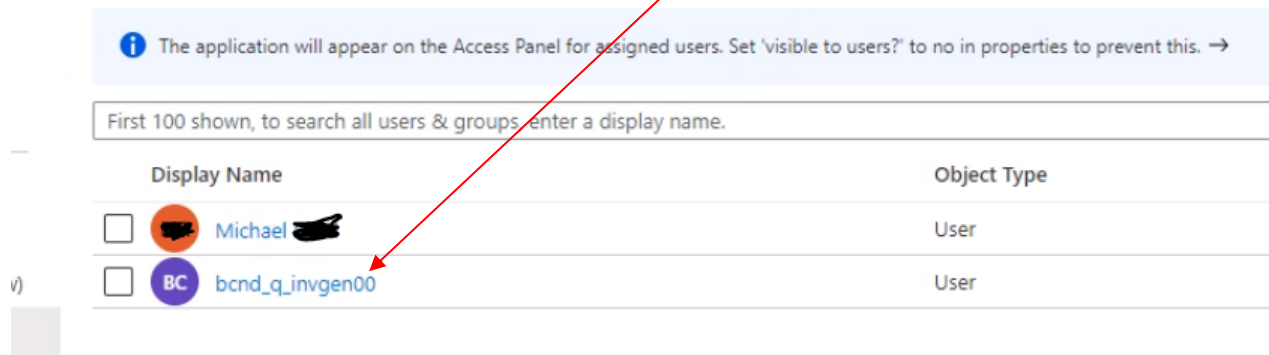
- g) Click on the user to [add it to the Selected](#) items list lower in the screen



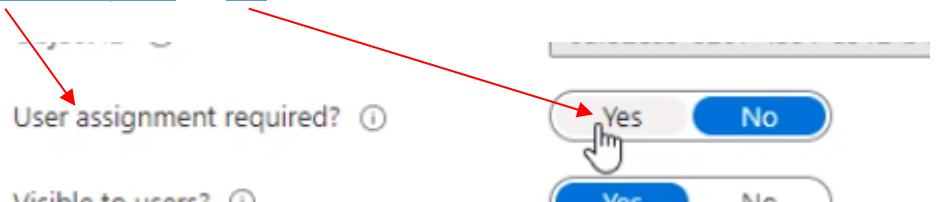
- h) Then click the [Select](#) button at the bottom
- i) Finally click on [Assign](#) in the lower left of the screen



- 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.

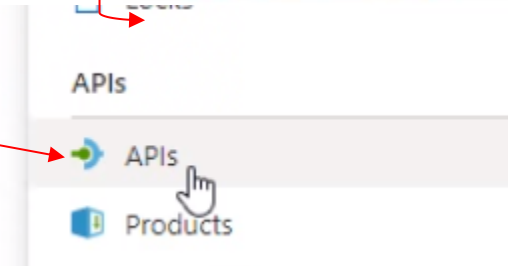


- 8) [Configure API to API Management Service: Home](#) → [API Management Services](#)

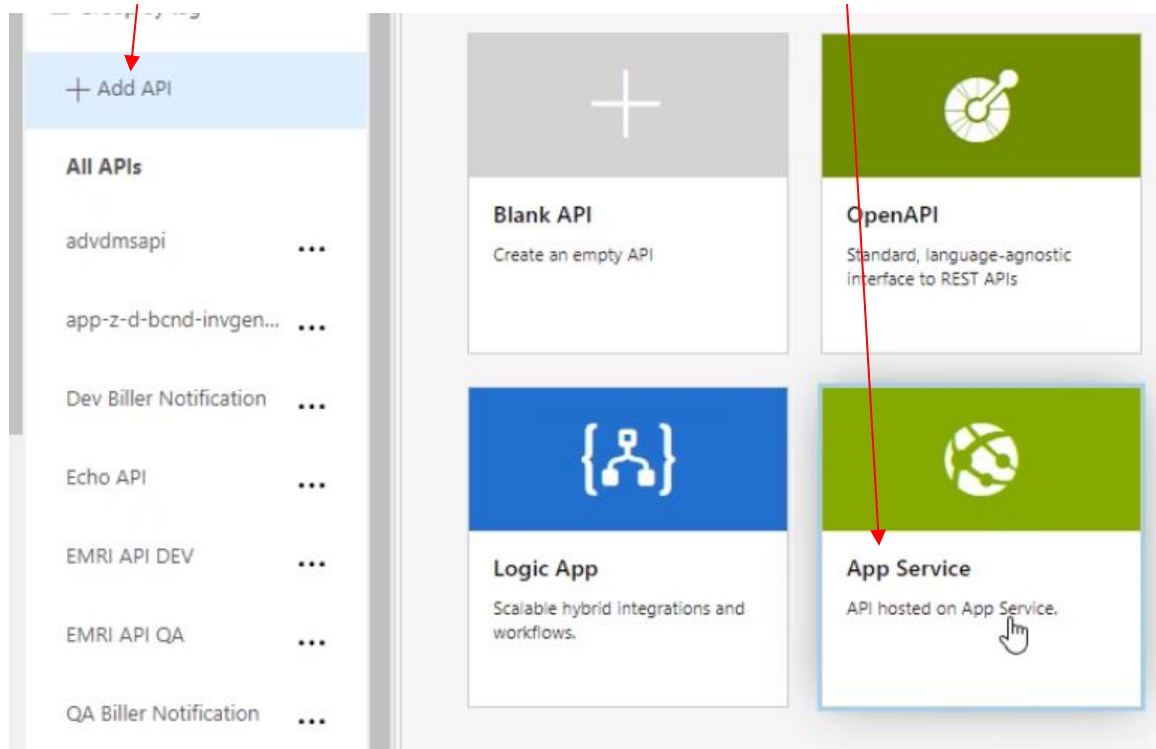
a) [Select the appropriate APIM](#) from the list on the screen



b) Click on [APIs](#) in the middle panel



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



d) The following screen appears

Create from App Service

Basic | Full

* App Service

* Display name

* Name

API URL suffix

Base URL

- i) Click the [Browse](#) button to locate and select the App

Select API App to import

API Management service

Name	Resource group
app-z-q-bcni-billntfy-01	API_SHARED_QA
app-z-q-bcnd-invgen00-01	API_SHARED_QA
app-z-q-shrd-ebcdicwb-01	API_SHARED_QA

- 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](#)

series, event driven

- e) Under [All APIs](#) find and [select your attached API](#) and click on [Settings](#) in the window to the right

REVISION 1 CREATED Feb 4, 2021, 4:02:33 PM

Design Settings Test Revisions Change log

Products No products selected

Gateways Managed x

Subscription

Subscription required ☒

Header name Ocp-Apim-Subscription-Key

Query parameter name subscription-key

Security

User authorization ☐ None ☒ OAuth 2.0 ☐ OpenID connect

OAuth 2.0 server azure-active-directory

☐ Override scope

Save

- 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](#)

Search (Ctrl+/)

+ Add

Products Add

Search to filter

Display name

- BCMI Biller No
- BCMI Biller No
- BCMI-IVR-DEV
- BCMI-IVR-QA
- BCND Invoice
- DMSAPI
- EMRI-DEV
- EMRI-QA
- Starter

APIs

- APIs
- Products
- Subscriptions

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

Add product
API Management service

Display name *
BCND Invoice Generation-QA ✓

Id * ⓘ
bcnd-invoice-generation-qa ✓

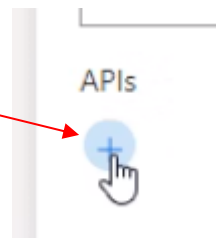
Description *
Application for Blue Cross North Dakota Invoice Generation - QA ✓

Published ☐

Requires subscription ☒

Requires approval ☐

- 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

APIs

app-z-q-bcnd-invgen00-01 X +

Create

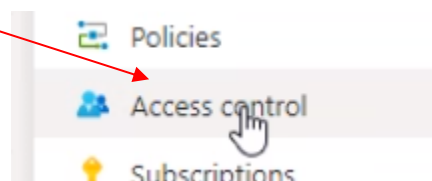
BCND Invoice Generation-DEV

BCND Invoice Generation-QA

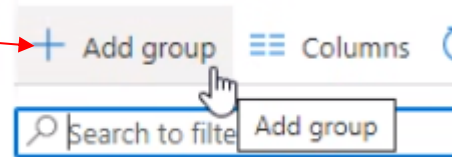
DMSAPI

- m) [Find the App](#) in the list and click on it to select it

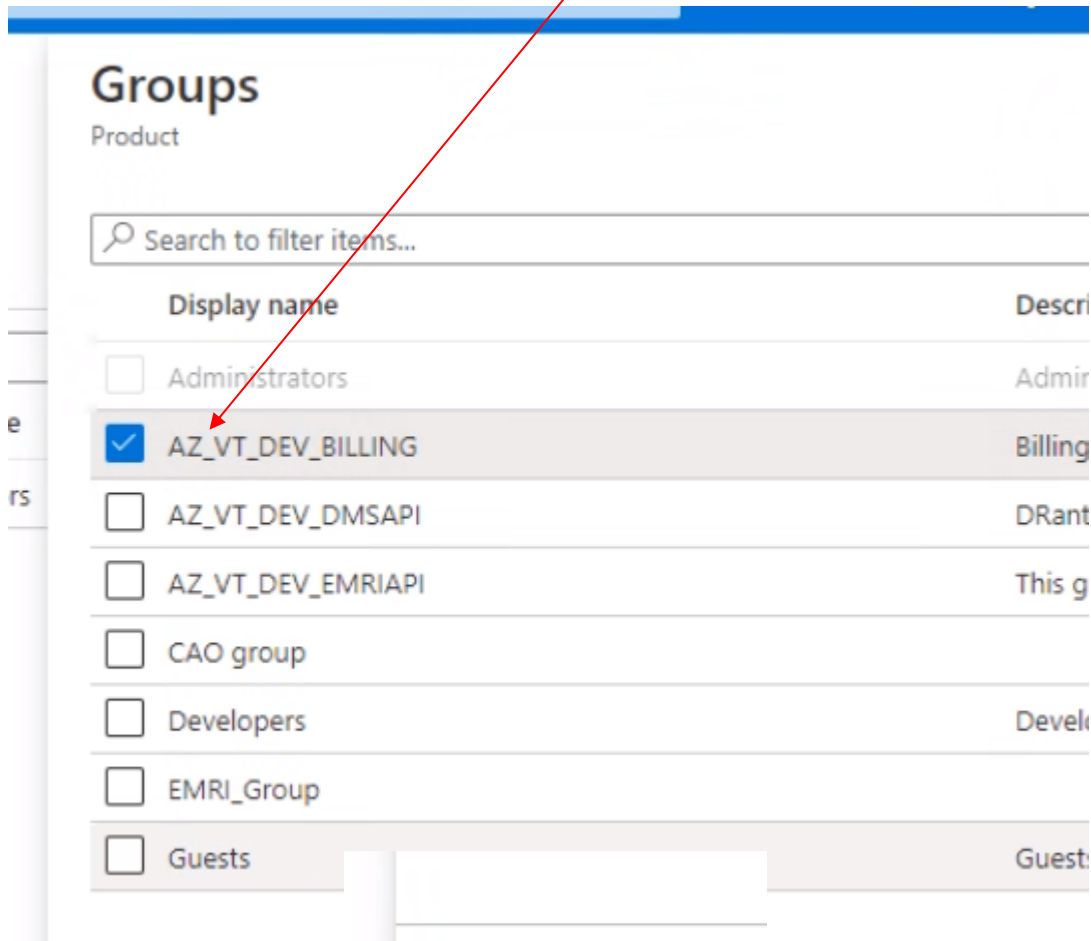
- n) Click on [Access control](#) from the left pane



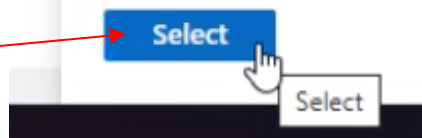
o) Now click on [Add group](#) at the top



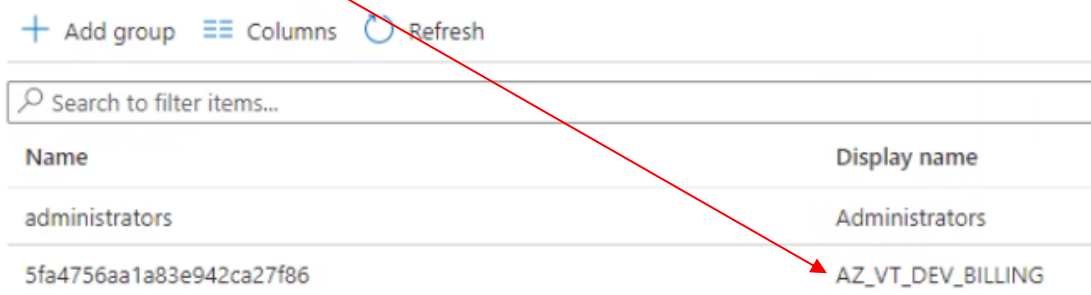
p) From the window that appears [find and select the group\(s\)](#) to be added



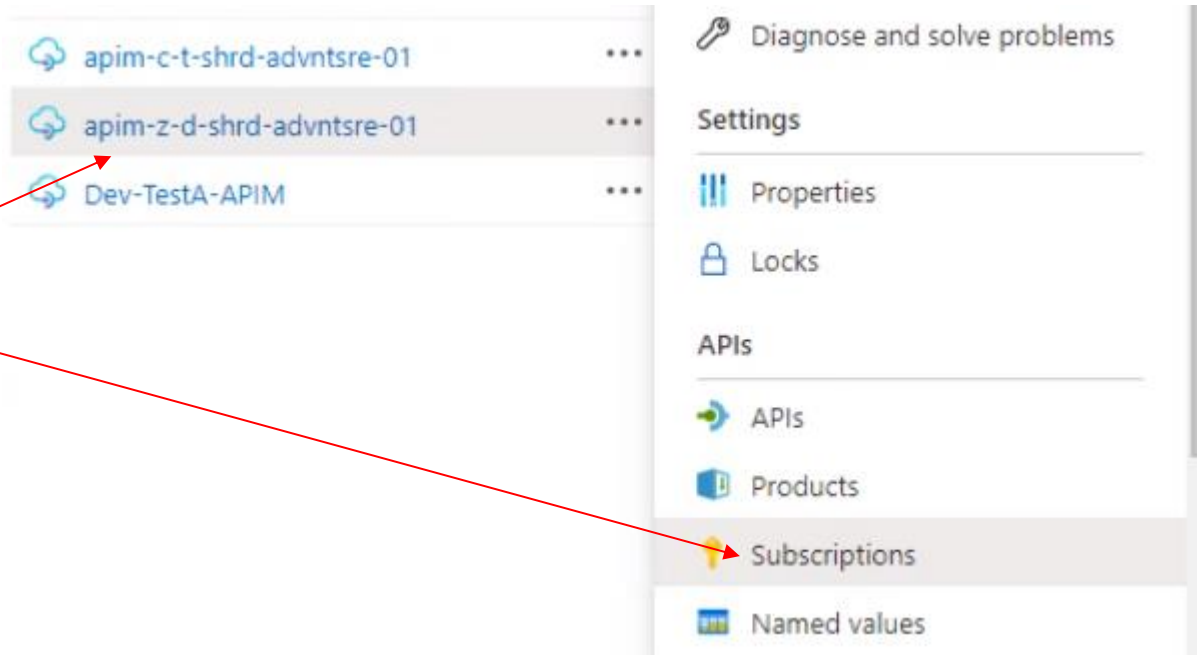
q) Press [Select](#) at the bottom



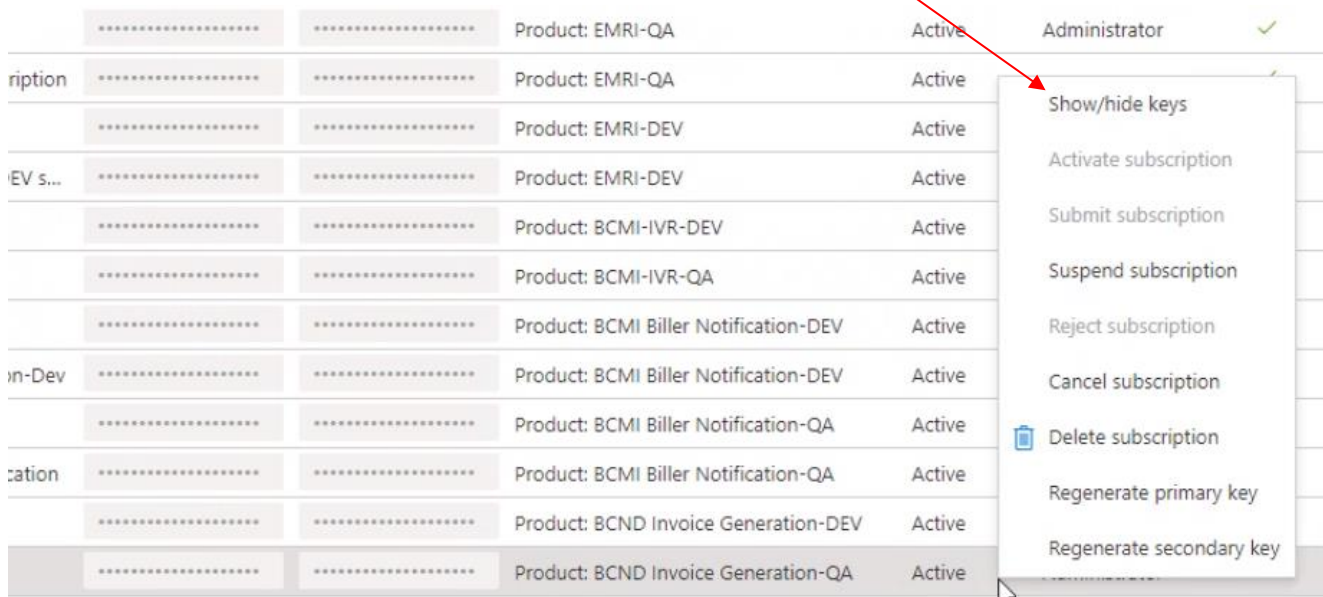
r) You should now see the [group\(s\)](#) you added in the Access control list



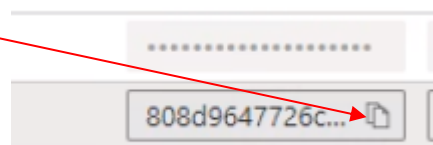
- 9) Go back to the main APIM page and [select the appropriate APIM](#) if necessary the click on [Subscriptions](#)



- 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](#)

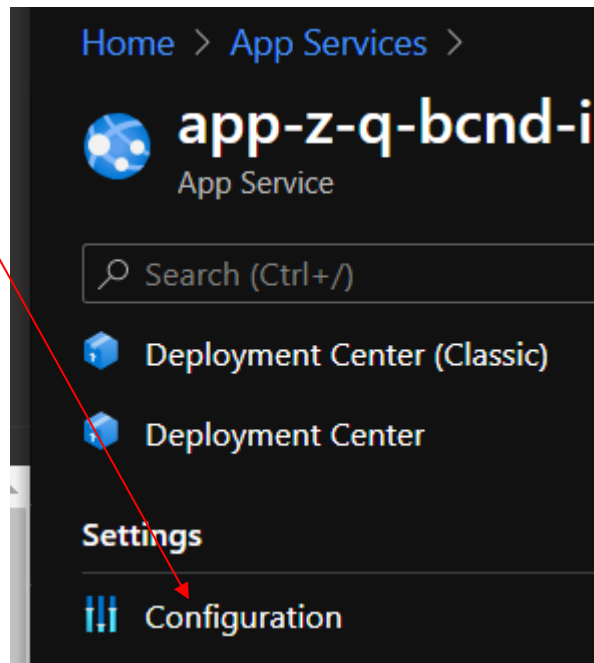


- 11) Click on the ["Copy to clipboard"](#) icon under the Primary key and record this in the build document

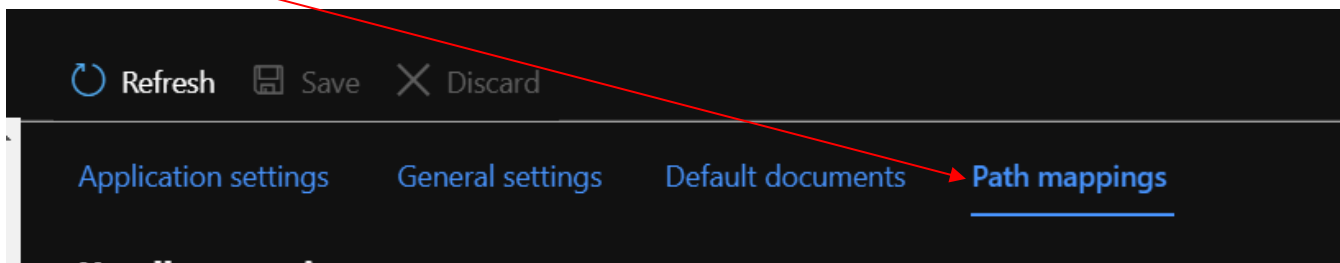


12) **Optional if required Create Microservices for the App Service: Home → App Services**

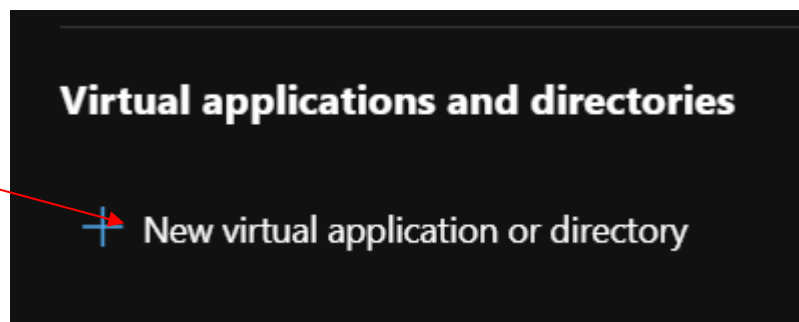
- a) From the center panel select [Configuration](#)



- 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)

A screenshot of a form with two input fields. The first field is labeled "Virtual path" and contains the text "/SystemParams". The second field is labeled "Physical Path" and contains the text "site\wwwroot\SystemParams". Red arrows point from the instructions to these fields.

- iv) [Uncheck the box for Directory](#) and [leave the other check box for Preload enabled unchecked](#)

A screenshot of a checkbox labeled "Directory". The checkbox is checked, indicated by a blue checkmark. A red arrow points from the instruction to this checkbox.

A screenshot of two checkboxes. The first is labeled "Directory" and is unchecked. The second is labeled "Preload enabled" and is also unchecked. Red arrows point from the instruction to both checkboxes.

- v) Click [OK](#) at the bottom of the screen to complete the creation

A screenshot of a blue button labeled "OK". A red arrow points from the instruction to this button.

- 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

A screenshot of a blue button with a floppy disk icon and the text "Save". A red arrow points from the instruction to this button.

- 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

A screenshot of a dialog box titled "Save changes". The text inside says "Any changes to application want to continue?". At the bottom, there are two buttons: "Continue" and "Cancel". A red arrow points from the instruction to the "Continue" button.

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-bcml-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.