

# 5. How to setups Multi-tenant in azure portal.

We already deployed and setups the power apps for single tenant. Now we are going to setup Multi-tenant in azure portal, It requires Application registers users, groups, custom domain for Front-end (portal web app service) and power-apps setups (business unit and security)

1. **Application register users and azure AD group:** we already know how to create a Applications user and group in documents number 4 (how to setups power-apps) and synchronization with power-apps (dynamic 365)

so here our Application user is "MVS-QA-EVENTS-APP-REG" and its group is "MVS-UAT- EVENTS\_qa\_internal-ADMINS"

2. **Custom sub-domain:** Go to the azure resource groups and selects the yours resource group i.e "UAT" and click on front-end web-app ( "uat-events-portal") and then click on the custom domain and create a sub-domain i.e "qa.uat.events.signetic.com" and adds DNS records in the Azure dns zone.

Microsoft Azure

Search resources, services, and docs (G+)

Home > UAT

Overview

Activity log

Access control (IAM)

Tags

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Essentials

Subscription (change) : MVS Events Subscription

Subscription ID : c3b7ee20-0543-4fe1-9186-a1c37cec394f

Deployments : 1 Failed, 2 Succeeded

Location : Central US

Tags (change) : uat:env

Filter for any field...

Type == all

Location == all

Add filter

Showing 1 to 5 of 5 records.

Show hidden types

No grouping

List view

Name	Type	Location
uat-events-api	App Service plan	Central US
uat-events-api	App Service	Central US
uat-events-portal	App Service plan	Central US
uat-events-portal	App Service	Central US
uat-events-portal	Application Insights	Central US

Microsoft Azure

Search resources, services, and docs (G+)

Home > UAT > uat-events-portal

uat-events-portal | Custom domains

App Service

Search (Ctrl+)

Refresh

Troubleshoot

FAQs

You have custom domains that are not secured and will cause browser warnings/errors when accessed over https. Click on "Add binding" to secure your custom domains.

Custom Domain Verification ID: 785FCF5508142ECD6280FD94D4848833DF415F32559C61D6C7907DC28D809754

HTTPS Only: On

Add custom domain

Status Filter

Add custom domain

Custom domain \* qa.uat.events.signetic.com

Validate

- Now bind the ssl custome domain "qa.uat.events.signetic.com" click on the TLS/SSL and click on icon private certificate key and choose the "Create App Service Managed Certificates" to create a SSL and bind it.

Microsoft Azure | Search resources, services, and docs (G+)

Home > UAT > uat-events-portal

uat-events-portal | TLS/SSL settings

Search (Ctrl+/) | Refresh | Delete bindings | Buy Certificate | Troubleshoot | FAQs

Authentication | Authentication (classic) | Application Insights | Identity | Backups | Custom domains | **TLS/SSL settings** | Networking | Scale up (App Service plan) | Scale out (App Service plan) | WebJobs | Push | MySQL In App | Properties | Links

Bindings: **Private Key Certificates (.pfx)** | Public Key Certificates (.cer)

**Private Key Certificate**

Private key certificates (.pfx) can be used for TLS/SSL bindings and can be loaded to the certificate store for your app to consume. To understand how to load the certificates for your app to consume click on the learn more link. Uploaded certificates are not available for manual download from the Azure Management Portal, they can only be used by your app hosted on App Service after the required App Settings are set properly or used for TLS/SSL. [Learn more](#)

+ Import App Service Certificate | + Upload Certificate | + Import Key Vault Certificate | **+ Create App Service Managed Certificate**

**Private Key Certificates**

Status Filter: **All** | Healthy | Warning | Expired

Health Status	Hostname	Expiration	Thumbprint
Healthy	test.uat.events.signetic.com	10/23/2021	24A9CA12503E7FE839DB98042DB893D6614EE658 ***
Healthy	registration.uat.events.signetic.com	10/16/2021	5174DBE6CEDE9CEDC0CC59463E284A39A96F83F1 ***
Healthy	qa.uat.events.signetic.com	10/23/2021	6E5293127D3A78E352929C2654034838CA28E6EA ***

**3. Now update the backend configuration records for multi-tenant: Go to the azure resource groups and click on the web-app service i.e (uat-events-api) and click on the configuration to add the configs i.e,**

a. MULTITENANT\_ENABLED: true

b. MULTITENANT\_APPLICATION\_USERS: { "qa": [{ "CLIENT\_ID": "c5837740-f72f-469c-923d-0d760d9427e6", "CLIENT\_SECRET": "7LYX--WmGzn6.CKFBx7U3Km.-C4A~u~JLy" }] }

Home > uat-events-api

## uat-events-api | Configuration

App Service

Search (Ctrl+/) Refresh Save Discard

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Events (preview)
- Deployment
  - Quickstart
  - Deployment slots
  - Deployment Center
- Settings
  - Configuration**
  - Authentication

Name	Value	Source
AUTHENTICATION_URL	Hidden value. Click to show value	App Service Config
BASE_URL	Hidden value. Click to show value	App Service Config
CAPTCHA_ENABLED	Hidden value. Click to show value	App Service Config
CAPTCHA_SECRET	Hidden value. Click to show value	App Service Config
CLIENT_ID	Hidden value. Click to show value	App Service Config
CLIENT_SECRET	Hidden value. Click to show value	App Service Config
ELIGIBILITY_PASS	Hidden value. Click to show value	App Service Config
ELIGIBILITY_USER	Hidden value. Click to show value	App Service Config
ELIGIBILITY_USER	Hidden value. Click to show value	App Service Config
<b>MULTITENANT_APPLICATION_USERS</b>	Hidden value. Click to show value	App Service Config
<b>MULTITENANT_ENABLED</b>	Hidden value. Click to show value	App Service Config
PHICURE_ELIGIBILITY_API	Hidden value. Click to show value	App Service Config
PORT	Hidden value. Click to show value	App Service Config
POWER_APPS_ENV_URL	Hidden value. Click to show value	App Service Config
XDT_MicrosoftApplicationInsights_Mode	Hidden value. Click to show value	App Service Config

- now we also need to update this records in [vault.bitwarden.com](https://vault.bitwarden.com) collections "Events credentials"

My Vault

Filters

Search

Types

Folders

Collect

Even

SVNA

Name	Value
CLIENT_SECRET	.fr0W.IX50WrNg.S4f6.4DzX1L7n-08WCK
ELIGIBILITY_PASS	DOESNOT_APPLY
ELIGIBILITY_USER	DOESNOT_APPLY
PHICURE_ELIGIBILITY_API	https://rt.phicure-edl.com/api/Eligibility
PORT	3000
POWER_APPS_ENV_URL	https://events-uat.crm.dynamics.com/
CAPTCHA_ENABLED	true
AUTHENTICATION_URL	https://login.microsoftonline.com/f3e08015-
<b>MULTITENANT_ENABLED</b>	true
<b>MULTITENANT_APPLICATION_USERS</b>	{ "qa": [{" "CLIENT_ID": "c5837740-47-

**4. Deployed the new codes which includes multi-tenet in .env: To deployed this code we need to merge the "events: repo with master branch of "healthcommons-agencies" repo's.**

a. Clone the events repo

```
$ git clone https://github.com/signetic-mvs/events.git
```

```
$ git remote -v
```

b. now add the remote repo from which you want to merge

remote repo= healthcommons-agencies

```
$ git remote add agencies https://github.com/signetic-mvs/healthcommons-agencies.git
```

c. now pull from the remote repo

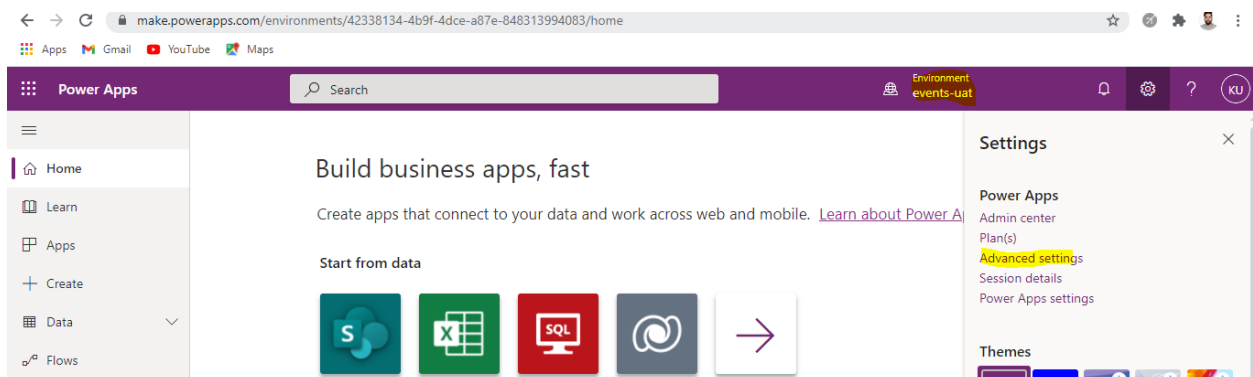
```
$ git pull agencies master
```

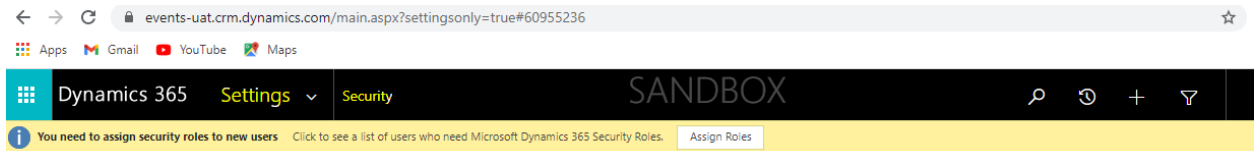
d. now push to the local clone repo "events"

```
<< git push origin master
```

The files from remote repo= healthcommons-agencies are merged with local origin repo= events.

**5. Business Unit: To create the business unit go to the power-apps and select the 'environments' "uat-events" and go to the advance 'setting' which redirects to you in the dynamics 365 portal and click on the 'security' and then choose the 'business unit'.**



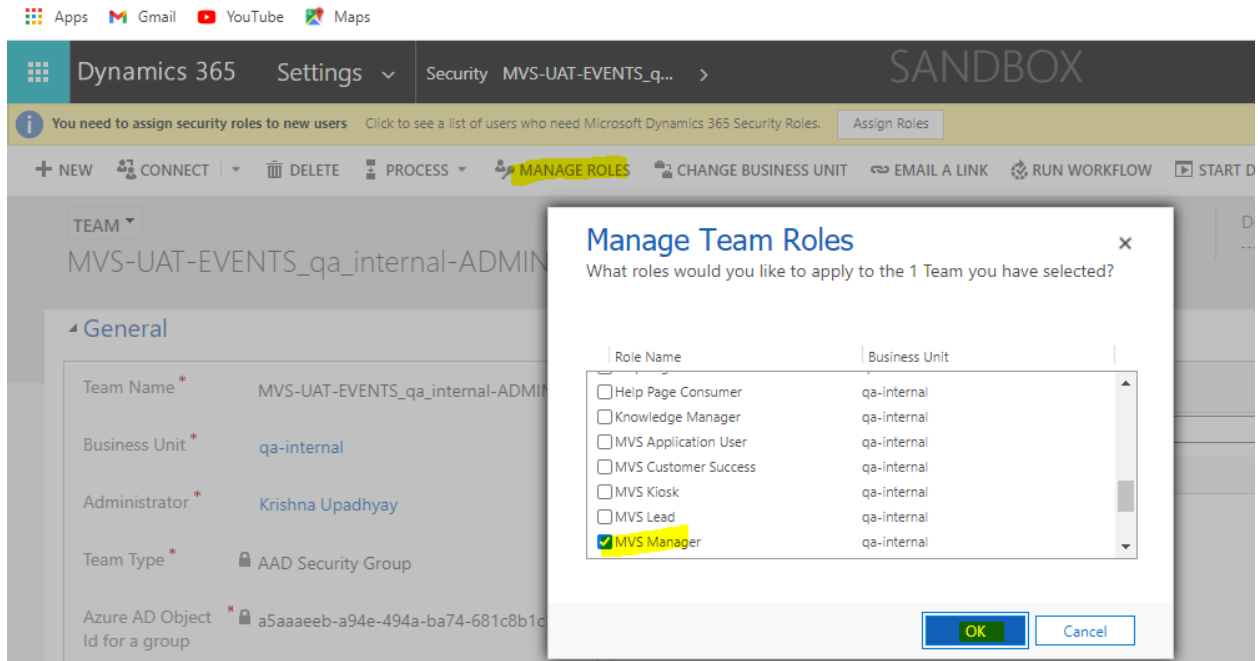


- create a business unit in my case i.e "qa-internal" and click on the save and close.

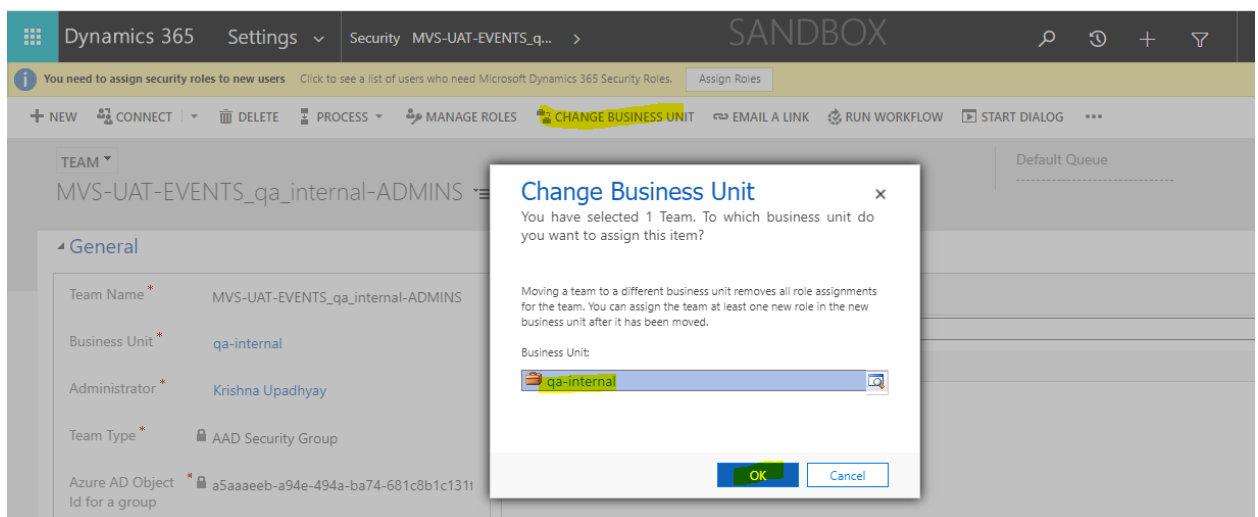
- now go the 'teams' which is already has sync with Azure AD groups (MVS-UAT-EVENTS\_qa\_internal-ADMINS) and select the team "All AAD Security Group Teams" and click on the "MVS-UAT-EVENTS\_qa\_internal-ADMINS" and click on the 'Manage Role' and assign the role "MVS application user".

The screenshot shows the Microsoft Dynamics 365 Security settings page. The top navigation bar includes 'Dynamics 365', 'Settings', and 'Security'. A yellow banner at the top states: 'You need to assign security roles to new users. Click to see a list of users who need Microsoft Dynamics 365 Security Roles. Assign Roles'. Below this, the 'Security' section is active, and the 'Teams' feature is highlighted. The 'Teams' section includes a description: 'Add new teams and new members to existing teams. Modify the team description'. Below the 'Teams' section, there is a table of teams. The table has two columns: 'Team Name' and 'Business Unit...'. The first row shows 'MVS-UAT-EVENTS\_qa\_internal-ADMINS' with the business unit 'qa-internal'. The second row shows 'MVS-UAT-EVENTS\_uat\_internal-ADMINS' with the business unit 'uat-internal'.

Team Name	Business Unit...
MVS-UAT-EVENTS_qa_internal-ADMINS	qa-internal
MVS-UAT-EVENTS_uat_internal-ADMINS	uat-internal



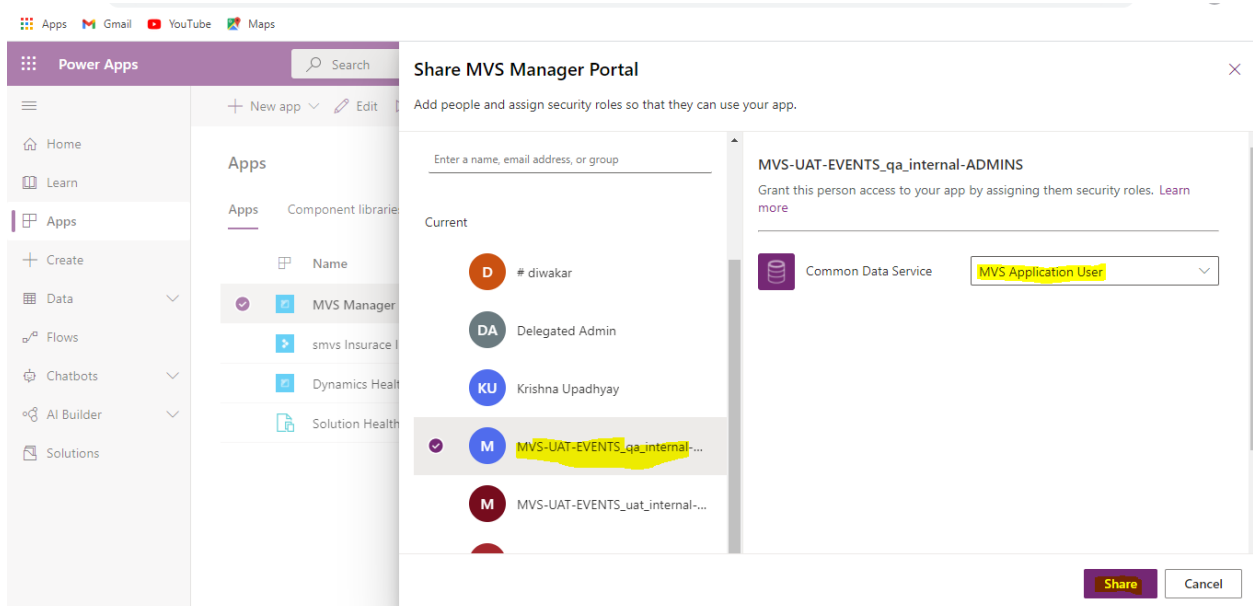
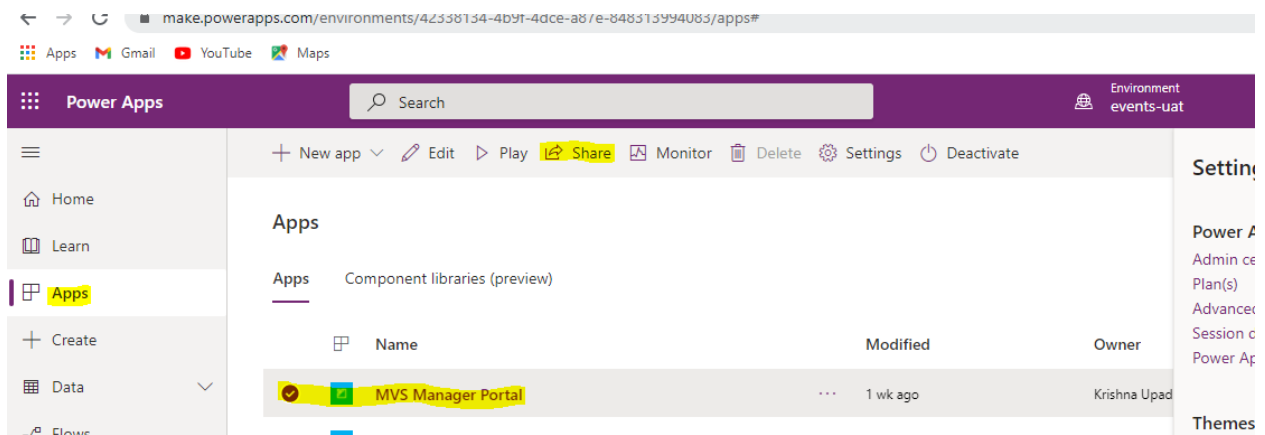
- now change the business unit to newly create "qa-internals by clicking on :CHANGE BUSINESS UINT" .



Now we have successfully create the business unit, assign the role and change the business unit.

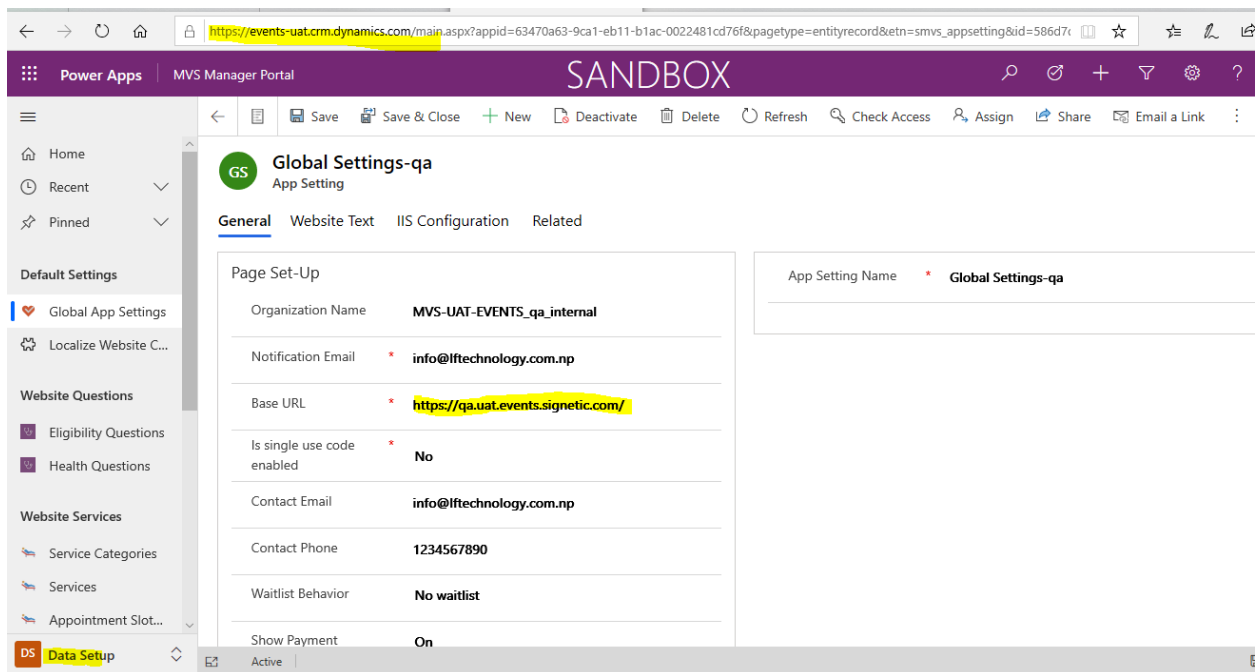
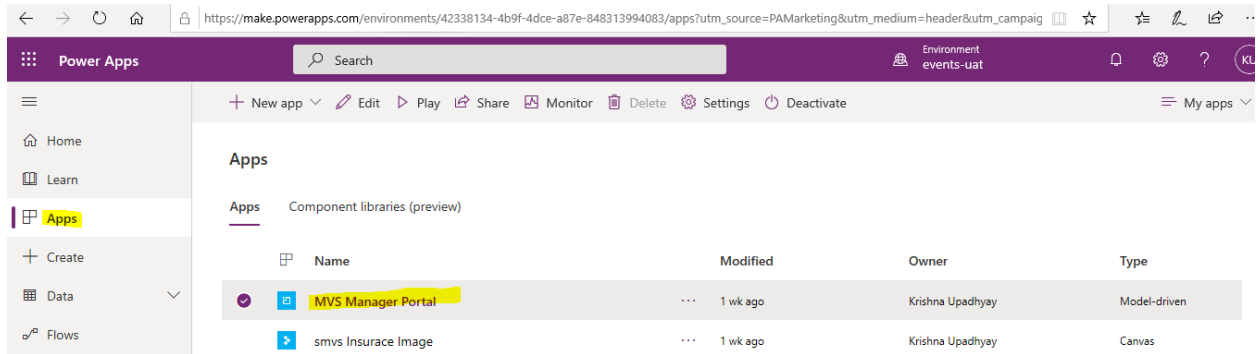


**6. Share the manager portal to the groups: Go to the power apps and click on the "APPS" and select the "MVS Manager Portal" and click on the 'share' with group "MVS-UAT-EVENTS\_qa\_internal-ADMINS" and select the role 'MVS application user'.**

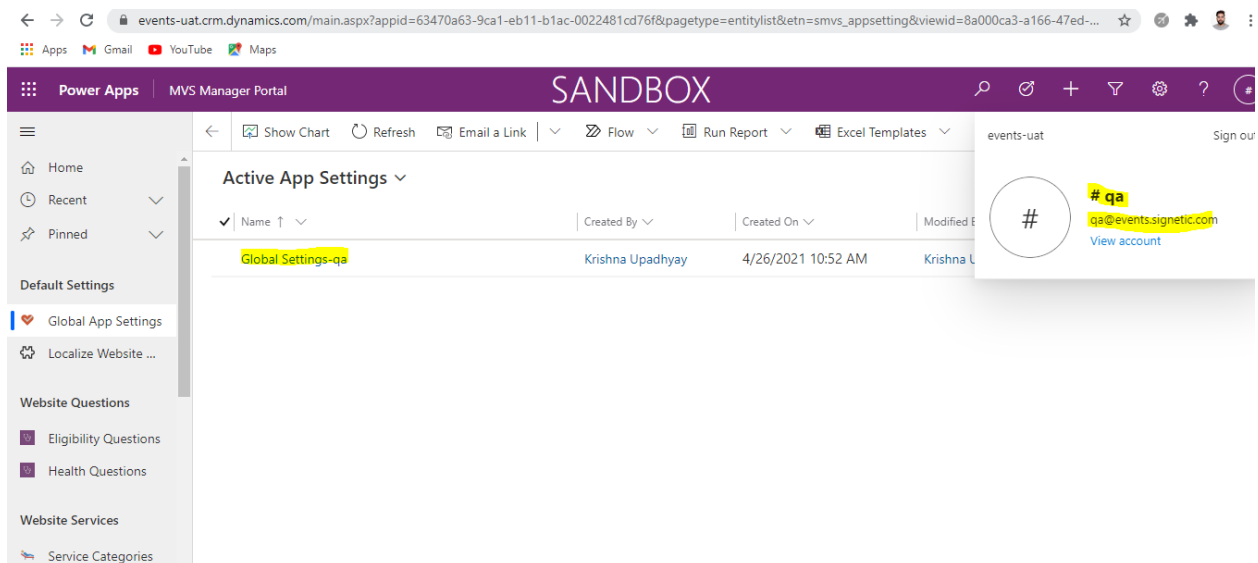


- now setups the data for group "MVS-UAT-EVENTS\_qa\_internal-ADMINS" with **base url** : <https://qa.uat.events.signetic.com> by click on the "MVS Manager

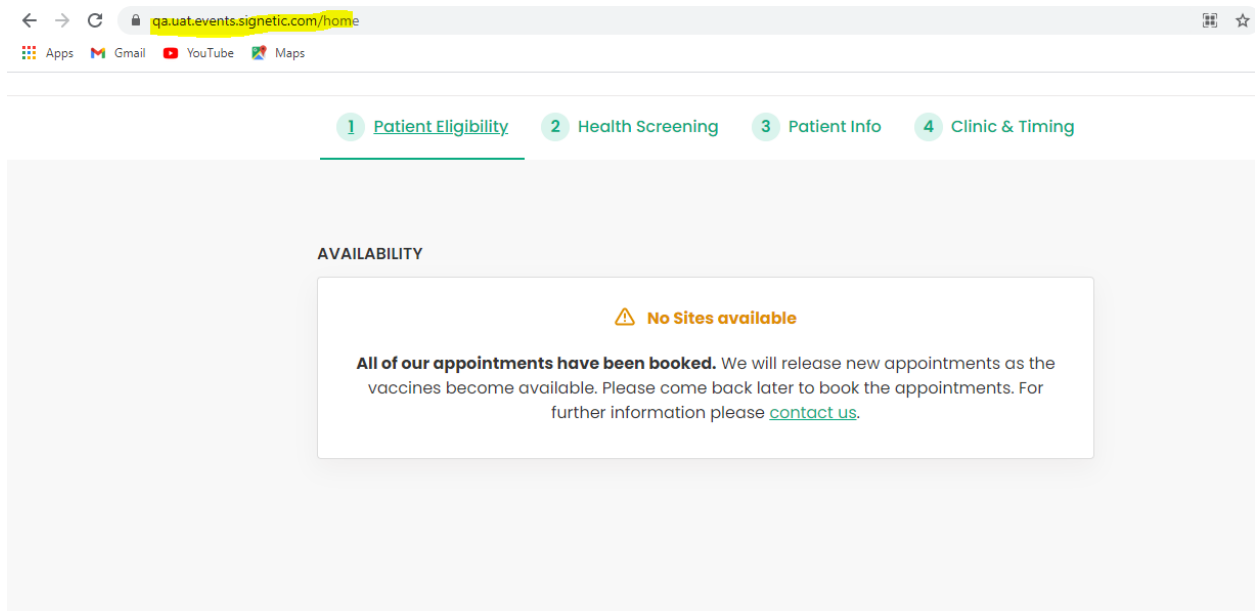
## Portal"



- login to the power-apps by 'qa' user and now you can access the "MVS Manager portal" from it.



**7. Now the multi-tenant has been deployed access url i.e <https://qa.uat.events.signetic.com> to verify.**



- Verify the backend by sending get request to front-end.

GET https://api.uat.e... X GET https://api.uat.e... GET Untitled Request Postman Echo + ... No Environment

https://api.uat.events.signetic.com/api/appSetting Save

GET https://api.uat.events.signetic.com/api/appSetting ...

Params Authorization Headers (7) Body Pre-request Script Tests Settings

Headers 6 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	Origin	https://qa.uat.events.signetic.com			
	Key	Value	Description		

Body Cookies Headers (9) Test Results Status: 200 OK Time: 1663 ms Size: 3.49 KB Save Re

Pretty Raw Preview Visualize JSON

```

6   "smvs_baseurl": "https://qa.uat.events.signetic.com/",
7   "smvs_issiteunderconstruction": false,
8   "smvs_isnoinsuranceallowed": false,
9   "smvs_is_credit_card_accepted": false,
10  "smvs_is_single_use_code_enabled": false,
11  "smvs_organizationname": "MVS-UAT-EVENTS_qa_internal",
12  "smvs_contactphone": "1234567890",
13  "ownerid value": "42b5472d-20a4-eb11-b1ac-0022481cd76f".

```

**We have successfully setups the multi-tenets and builds the apps in power apps.**