

Document Name	SAML- SSO(Troubleshoot guide)
Authors	Mian Asad Hussain
Document Date	23-july-2019
Company	ITboost
Target Audience	End User, Development, Technical Support, Quality Assurance

## Introduction

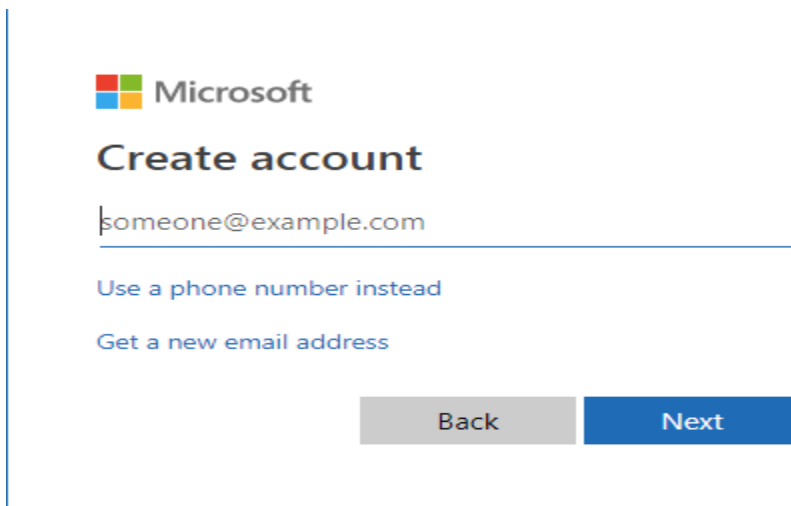
Sso (single-sign-on) is our latest feature of itboost. In this troubleshooting guide we will discuss the basic and main scenario that are necessary to follow.

Either in case of any concern when at some situation it could not easy to sort out from such type of situation then scenario are really helpful.

### **S.no 1 : if user is unable to create his microsoft azure account.**

When any new person go to microsoft azure and if he found any difficulty regarding creating his account, then he should follow the below steps.

1- go to the <https://portal.azure.com> and click to create new account



Microsoft

### Create account

someone@example.com

[Use a phone number instead](#)

[Get a new email address](#)

Back Next

2- create a password for yourself



← muhammad.umair@itboost.com

## Create a password

Enter the password you would like to use with your account.

.....|

☐ Show password

Next

3- enter the code here that you received on your email account



← muhammad.umair@itboost.com

## Verify email

Enter the code we sent to **muhammad.umair@itboost.com**. If you didn't get the email, check your junk folder or [try again](#).

Enter code

---



I would like information, tips, and offers about Microsoft products and services.

Choosing **Next** means that you agree to the [Privacy Statement](#) and [Microsoft Services Agreement](#).

Next

Microsoft account

## Verify your email address

To finish setting up your Microsoft account, we just need to make sure this email address is yours.

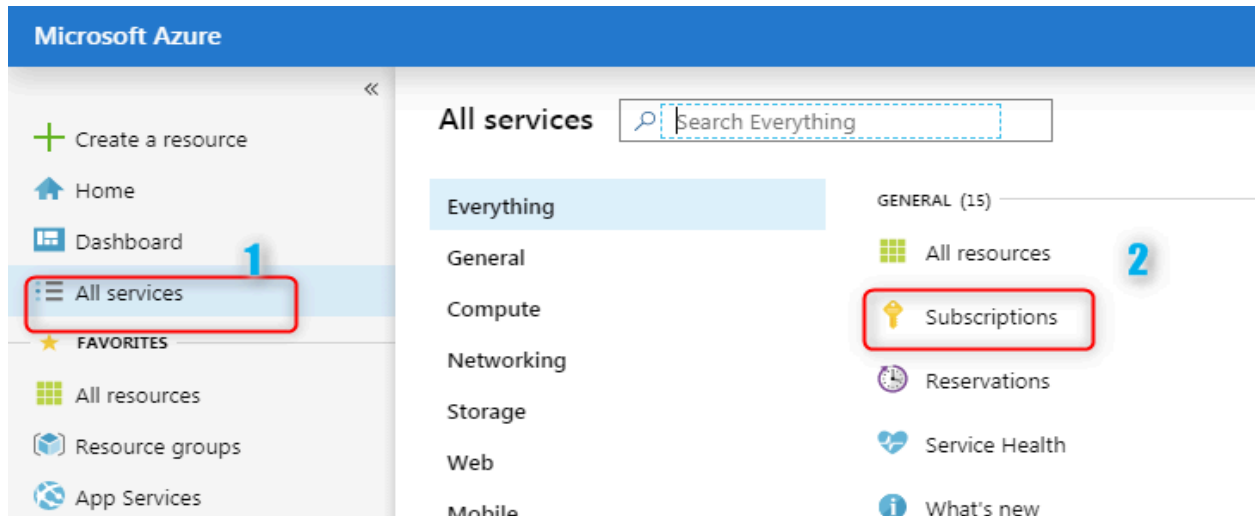
To verify your email address use this security code: **5677**

If you didn't request this code, you can safely ignore this email. Someone else might have typed your email address by mistake.

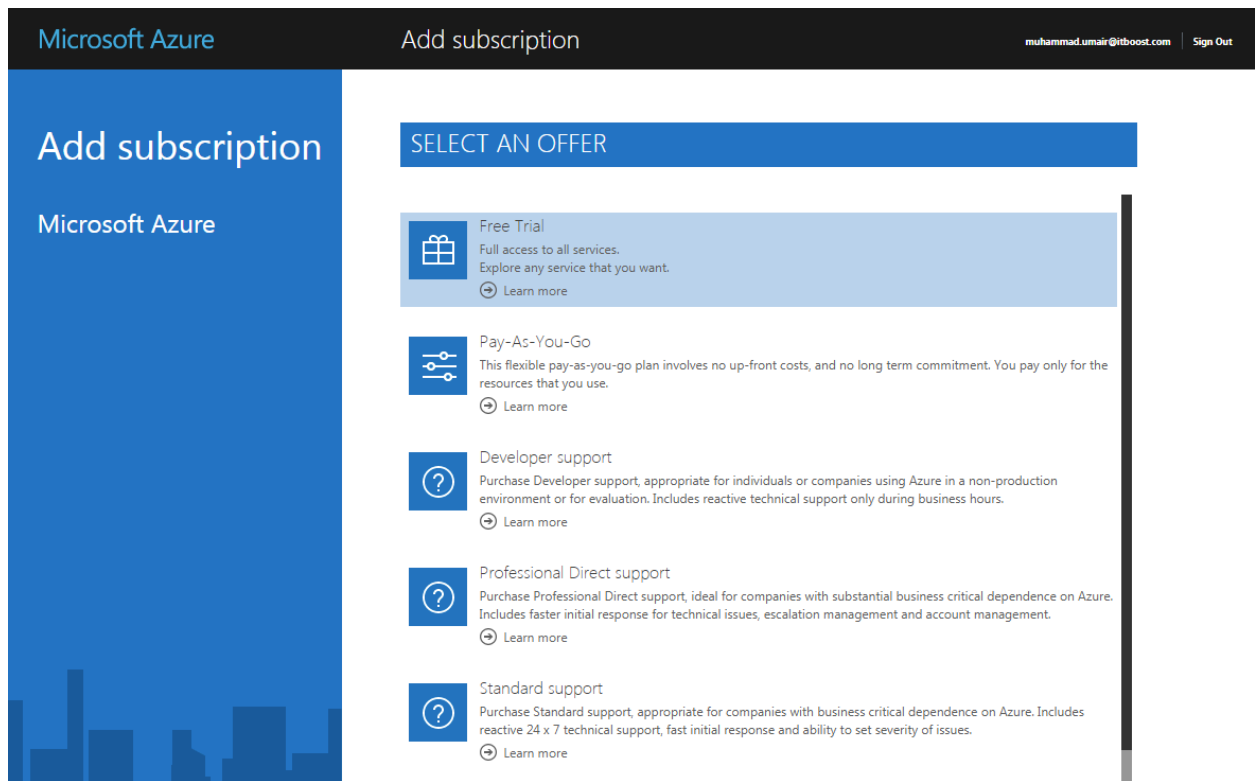
Thanks,  
The Microsoft account team

S.no 2 :How to assign default directory to your account.

1- Click on "**All services**" then click on "**subscription**"




2- add new subscription free trail



3- enter below your basic cred for sign up free trial, and click on "next" button.

## 1 About you

---

Country/Region 


Pakistan ▼

First name

muhammad

Last name

umair

Email address 

muhammad.umair@itboost.com

Phone

300-9675399

Next

4- it will send you code on your provided cell # and then enter the code , as in below screenshot, and click on verify the code.

## 2 Identity verification by phone

---



A text or phone call helps us make sure this is you.

Country code

Phone number

We delivered a code to your phone.

Verification code

**Note that: “ next step it will demand from you to enter your credit card credentials to pay for it, but do not need to do that because you are going To sign up with free account. Just ignore it”**

## 1 Identity verification by card



We ask for your credit card number to verify your identity and to keep out spam and bots.

**You won't be charged unless you upgrade.**



Card number

Expiration date

CVV [i](#)

Name on card

Address line 1

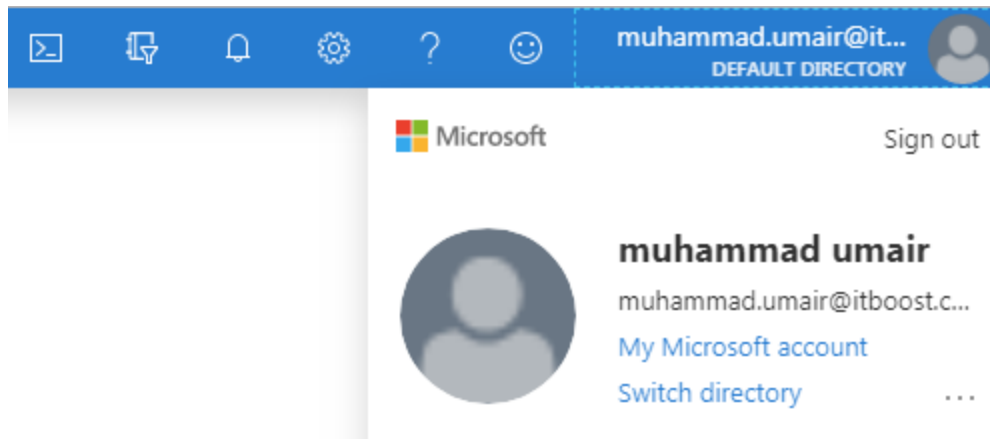
Address line 2

City

Postal Code

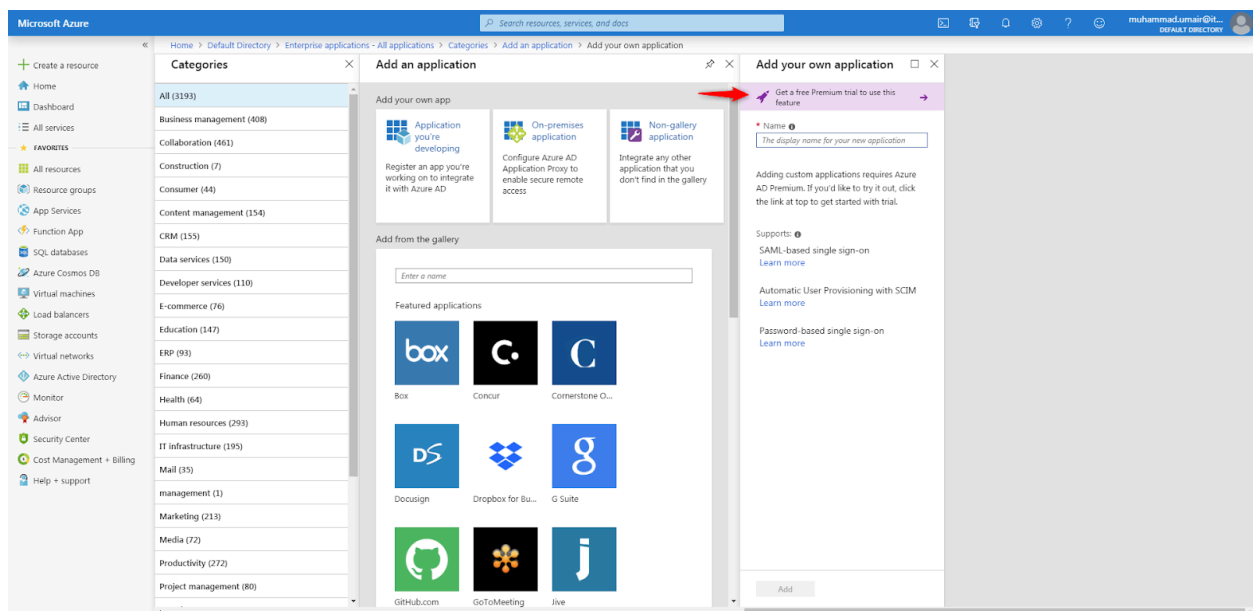
Next

5- logout and login again into Microsoft azure account.and you will have your default directory.



S.no 3 : if user is unable to create/add new application.

Its normally happens when you are signed up with a free account, and login into azure And you want to add a new application , but you are forced to get premium trail like given in the following screenshot.



1: click on this premium account to activate it. And it will redirect to you on activation page as given below.



## Add your own application

Get a free Premium trial to use this feature

\* Name ⓘ

The display name for your new application

Adding custom applications requires Azure AD Premium. If you'd like to try Premium, click the link at top to get started with a free trial.

Supports: ⓘ

- SAML-based single sign-on  
[Learn more](#)
- Automatic User Provisioning  
[Learn more](#)
- Password-based single sign-on  
[Learn more](#)

Add

## Activate

Browse available plans and features

Consumption of MFA, P2, and SaaS challenges. In addition to Azure Active Directory Premium P2 the suite includes Microsoft Intune and Azure Rights Management.

[More information](#)

^ Free trial

Enterprise Mobility + Security E5 provides a comprehensive solution enabling you to effectively manage devices, identity and access in your organization. The suite includes Microsoft Intune, as well as Azure AD Premium P2 and Azure Rights Management. [Learn more about features](#)

The trial includes 250 licenses and will be active for 90 days beginning on the activation date. If you wish to upgrade to a paid version, you will need to purchase Enterprise Mobility + Security E5 or its individual components. [Learn more about pricing](#)

Enterprise Mobility + Security E5 is licensed separately from Azure Services. By confirming this activation you agree to the [Microsoft Online Subscription Agreement](#) and the [Privacy Statement](#).

Activate

## Azure AD Premium P2

With Azure Active Directory Premium P2 you can gain access to advanced security features, richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

[More information](#)

^ Free trial

Azure Active Directory Premium P2 enhances your directory with additional features that include multi-factor authentication, policy driven management and end-user self-service. [Learn more about features](#)

The trial includes 100 licenses and will be active for 30 days beginning on the activation date. If you wish to upgrade to a paid version, you will need to purchase Azure Active Directory Premium P2. [Learn more about pricing](#)

Azure Active Directory Premium P2 is licensed separately from Azure Services. By confirming this activation you agree to the [Microsoft Online Subscription Agreement](#) and the [Privacy Statement](#).

Activate

2- activate these trial and logout and login again. after that you can be able to add new app, as shown below

## Add your own application ☐

\* Name 



Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: 

SAML-based single sign-on

[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)

Add

S.no 4 : SSO cred must be same both in azure and itboost for configure successfully.

Below a comparison screen shot is given, that is indicate that the cred same in azure created app(idp) are the same in itboost .

If users want to configure azure successfully with itboost , then cred must be same.

LOGIN METHOD

ENFORCE LOGIN

SSO

IDP ID  
Azure

ENTITY ID  
new

CERTIFICATE  
Ohgh p1jkTjVw+agzwnHKpyJd -----END CERTIFICATE-----

SP META DATA URL  
https://betabk.itboost.com/login/metadata.xml/

LOGIN URL  
https://login.microsoftonline.com/d9504996-7ad2-4a05-bl

LOGOUT URL  
https://login.microsoftonline.com/common/wsfederation?v

REPLY URL  
https://betabk.itboost.com/login/sso-assert

SAVEDELETECLOSE

1

Basic SAML Configuration

Identifier (Entity ID)  
Reply URL (Assertion Consumer Service URL)  
Sign on URL  
Relay State  
Logout Url

new  
https://betabk.itboost.com/login/sso-assert  
https://betabk.itboost.com/login/sso-assert  
Optional  
Optional

2

User Attributes & Claims

Givenname  
Surname  
Emailaddress  
Name  
Unique User Identifier

user.givenname  
user.surname  
user.mail  
user.userprincipalname  
user.userprincipalname

3

SAML Signing Certificate

Status  
Thumbprint  
Expiration  
Notification Email  
App Federation Metadata Url  
Certificate (Base64)  
Certificate (Raw)  
Federation Metadata XML

Active  
9038D3F9D6EA69F6D2C643E6DCCDBE3AEB68B5BC  
7/23/2022, 11:59:47 AM  
muhammad.umair@itboost.com  
https://login.microsoftonline.com/d9504996-7ad2-...  
Download  
Download  
Download

4

Set up new\_app\_adding

You'll need to configure the application to link with Azure AD.

Login URL  
Azure AD Identifier  
Logout URL

https://login.microsoftonline.com/d9504996-7ad2-...  
https://sts.windows.net/d9504996-7ad2-4a05-bb08-...  
https://login.microsoftonline.com/common/wsfede...

S.no 5 :certificate must be copied and pasted into itboost properly.

Some time when users download the certificate and paste it in sso (azure) in itboost Then it might be possible that , he can avoid the “**beginning ,ending**”

Of the certificate.

In this scenario the sso will integrate successfully but , on login time user will unable to login so it must need to follow the below steps.

1- download the certificate

2- open it in “**notepad**”

3- press “**ctrl + A**” to select all and paste it in itboost sso(azure)



```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQHKQpxL7EhYpNp3tTjAK8zANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylNaWNyb3NvZnQxcmUgRmVkbG9uZGVkFNTTy8DZXJ0aWZpY2F0ZTAeFw0xOTA3MjMwNjU5
NDdaFw0yMjA3MjMwNjU5NDdaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRIcmF0ZWQg
U1NPIENlcnRpZmljYXRIMjIwMjMwNjU5NDdaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRIcmF0ZWQg
c8SPdJHx9E6viO3kVsjXNVFo9AEHaymKMgCxtKdmOODrMGFMHB7q7tDychJrnhN5dPmMXRO9dPGI
pqCgilly95RAskL4oNahBzHvQeGnuZsjX7MN9RIGWOzVYHTsXkb0ul3HlfCsQO1vqMGr6+vk8K7ox
hceE1jAnLROp886sTPnxvYGkxoe2vBQkb4Xkpi4xZXG12R3Rnogje3NmzmFTtZ5V7Uf7K0H8//
wHwi7peTYAP8/3xsWvOdBxV04sOA0Y8Rm2zg9EzLYbDbY4ObXU7hJNgNGhRx214JtfS3N9xVadR
aEVeWoyXNREiu2et9T41hh8q7QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBELZExYvwPAiRekvMt
yK4mlATqgVb5GmD4eTDrIBYmQtHgyOquqVU5sQanhGSjNbFs+jOWXy3if05Q4uS8ZoxOp0nRISH2
ZTK0E6I9TMN7pUcIqjVIHHH9TPli8B4w5RVOavO4kZR38/hdn95W86iQ222czzS/WRtNngdPGZL
bnUgnD7st0HjvPAD1R8HyxkKG3TineIQVWcdZAJxrS6XklIQGhEFOsH+g+KU83wjwglS9uh8REX+
lQ7H/UMARh1LLbspQqhMNips04lcORbwdtE7K7Abym7Umr7Jc2PlJ1E8AnUdzwVzJuK48cAiOhgh
p1jktJVw+agzwnHKpyjd
-----END CERTIFICATE-----
```

S.no 6 : in itboost, login methods sso, it should be mandatory that all fields have accepts the cred, without filling any mandatory filled It must not be integrated.

In the following screenshot we did not give the identity id only , except this all other mandatory fields are filled, but it is not allowing to configure It should must work in this way.

LOGIN METHOD

ENFORCE LOGIN

SSO

IDP ID\*

Azure

LOGIN URL\*

https://login.microsoftonline.com/d9504996-7ad2-4a05-bl

ENTITY ID\*

LOGOUT URL\*

https://login.microsoftonline.com/common/wsfederation?v

CERTIFICATE\*

-----BEGIN CERTIFICATE-----MIIC8DCCAdigAwIBAgIQHk

REPLY URL\*

https://betabk.itboost.com/login/sso-assert

SP META DATA URL\*

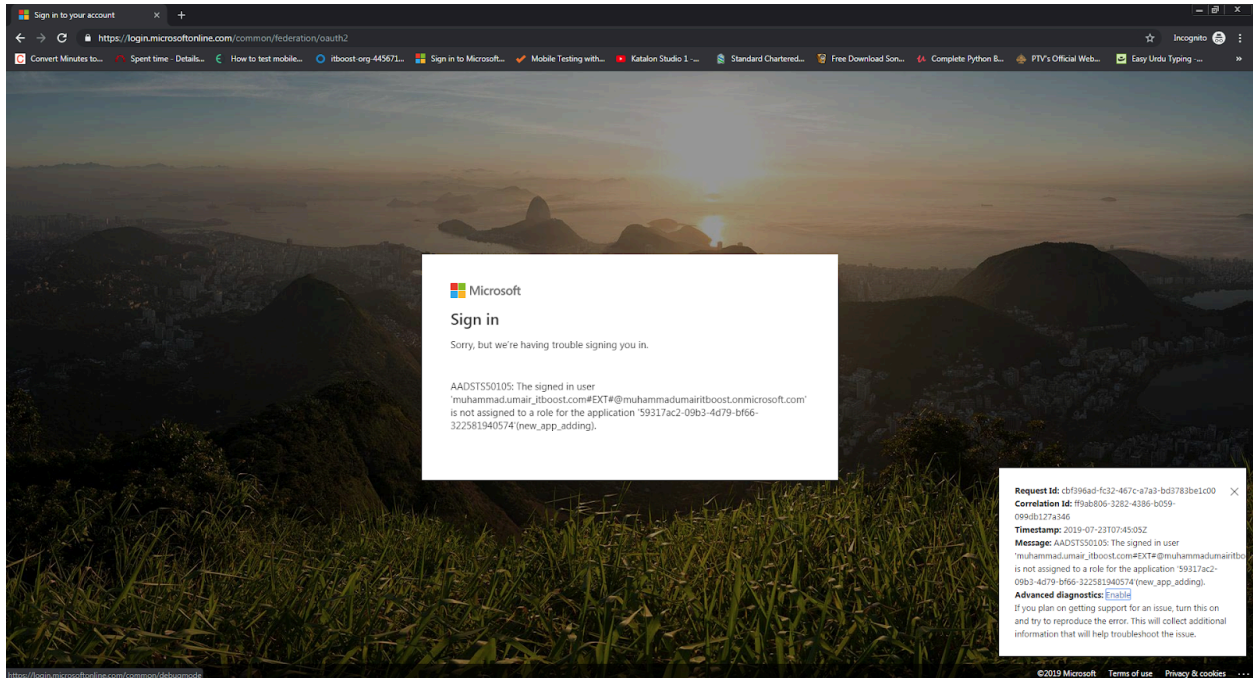
https://betabk.itboost.com/login/metadata.xml/

SAVE

DELETE

CLOSE

S.no 7 : error show on login with sso.if user in azure not assign to any app.



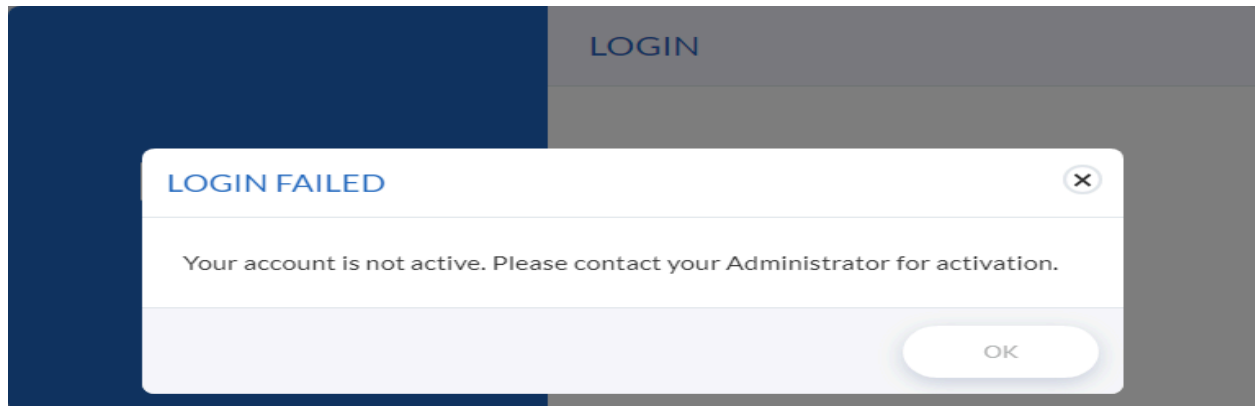
In the above screen shot an error message is shown, it happens when your user is not created in itboost / not assigned to app in azure .

So it must be confirmed that user must be created in (itboost + azure and assign to app).

**S.no 8 :** if user face a problem with his account showing as “not active”.

Its generally happens when your itboost created account is inactive, you have an account on both sides (idp + itboost) , but your account is not active in itboost and user try to login through sso .

At that time a following pop up appear.

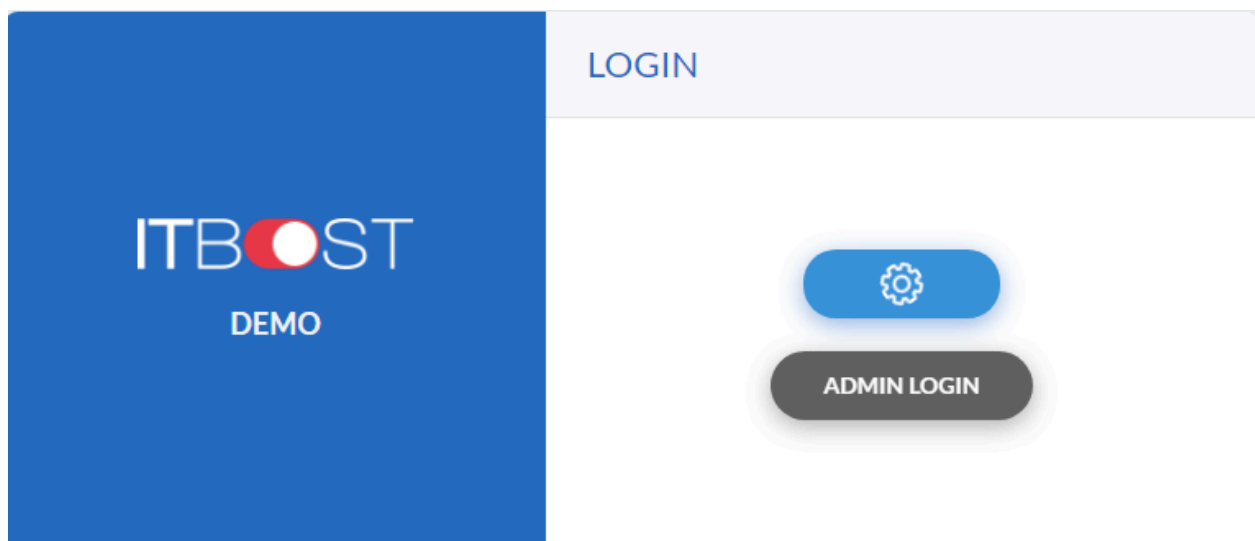


Handle this situation is simple

- 1- login into itboost with your admin user.
- 2- go to user list.
- 3- active the user account you want to login through sso . and after that you will login successfully.

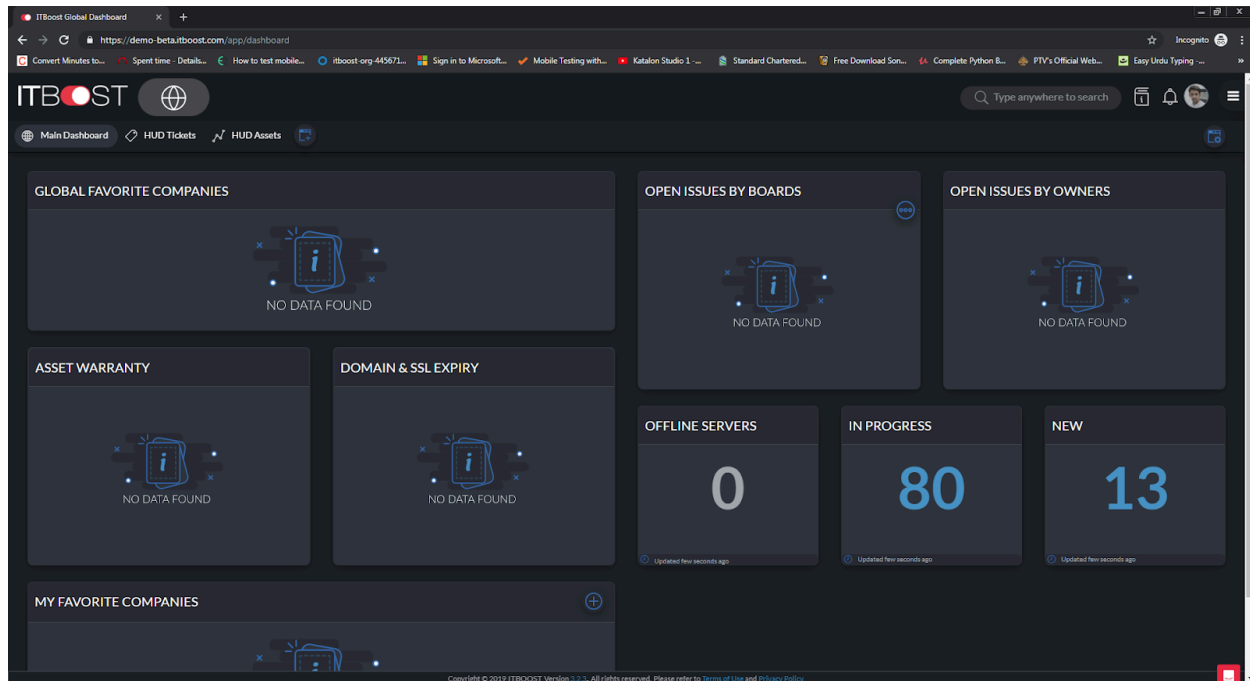
**S.no 9 : when user login through sso, the sso trigger option is scrolling only and admin login option must be disable.**

When user select sso method for login and select sso option , after entering his/her azure cred, when login page is loading on that page  
Scorller must be scrolling on sso option and admin login option must be shown as disable. As shown below,.



S.no 10 : after sso login the user role must be the same as in itboost.

The role that is assigned to user in itboost(tv user,admin,non admin,external) , after login through sso the remain same As shown in the screenshot



S.no 11 : “Reply url” in itboost accepted in azure app as “reply url & sign on url”.

Reply url given in itboost sso , first not editable, not able to delete only this field. This field save at back end and generated from db.

Its purpose is to copy this “reply url” and past it single sign on of related app, then It get configured.



LOGIN METHOD

ENFORCE LOGIN

SSO

IDP ID\*

Azure

LOGIN URL\*

https://login.microsoftonline.com/d9504996-7ad2-4a05-b

ENTITY ID\*

new

LOGOUT URL\*

https://login.microsoftonline.com/common/ws federation?v

CERTIFICATE\*

-----BEGIN CERTIFICATE-----MIIC8DCCAdigAwIBAgIQHk

REPLY URL\*

https://betabk.itboost.com/login/sso-assert

SP META DATA URL\*

https://betabk.itboost.com/login/metadata.xml/

SAVE

DELETE

CLOSE

Upload metadata file

Change single sign-on mode

Test this application

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating new\_app\_adding.

1

Basic SAML Configuration

Identifier (Entity ID)

new

Reply URL (Assertion Consumer Service URL)

https://betabk.itboost.com/login/sso-assert

Sign on URL

https://betabk.itboost.com/login/sso-assert

Relay State

Optional

Logout Url

Optional

S.no 12 : user types in azure.

There are two types of user in

- **Member**
- **Guest**

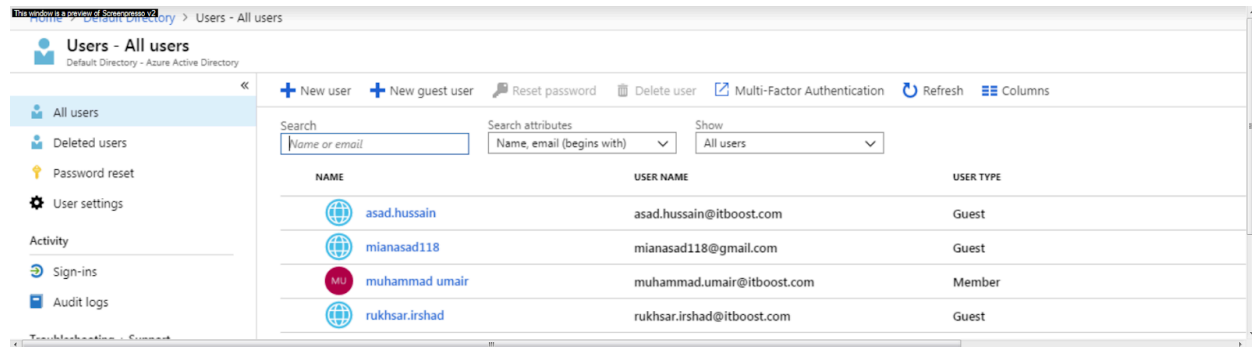
### Member:

Member users are those users that are sign up in azure ,and they have default directory.

### Guest:

Guest are those user they are created / added by member user.

**Note: both member and guest user type cannot changes in azure.**



**S.no 13 : How Free trial is different from Premium account and what are the things to consider for premium accounts.**

The answer is very simple , when user first time sign up into azure , user sign as with free trial, and initial he does not have (azure active directory) that have other possible option.

For this he subscribe free trial period.

The second thing is that , user can login to itboost when he has application in Azure, for that after subscription of free plan, he tries to add application , User forced to activate premium account when he activate that premium account Then he is able to add application.

That's why he activate the premium account. And he is able to add application.

**Note : how to subscribe free trial and activate premium account procedure is mentioned above.**

**S.no 12 : “Other” option available in idp drop down in itboost, and its purpose.**

"Others" this option is for those IDPs which provides mandatory fields(Login URL, Entity ID, Logout URL, Certificate) to integrate SSO in itboost and can be used for Single Sign on.