We can connect with any directory

miniOrange provides user authentication from external directories like Microsoft Active Directory, Azure AD,AWS Cognito etc.

MiniOrange Directory

Microsoft AD

Azure AD

Prerequisites

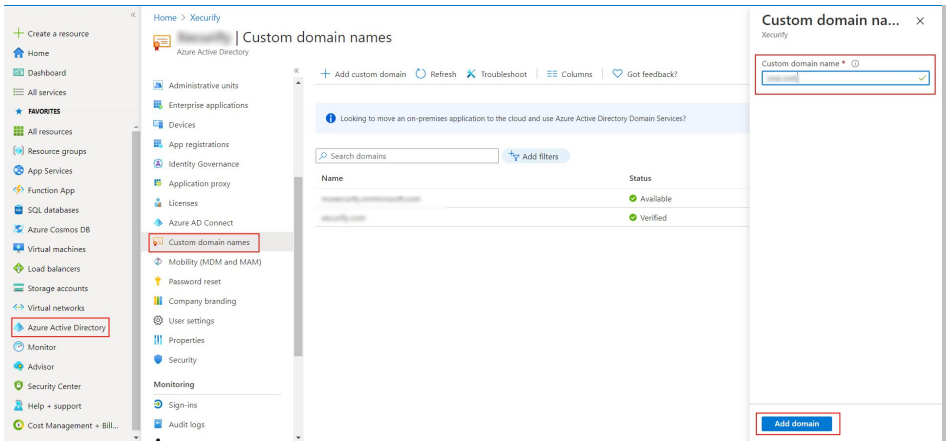
1. Sync On-Premise Active Directory with Azure Active Directory

NOTE: If you want to use your On-Premise Active Directory as a user store to Single Sign-On into Office 365 then follow the below steps to sync your AD and Azure AD.

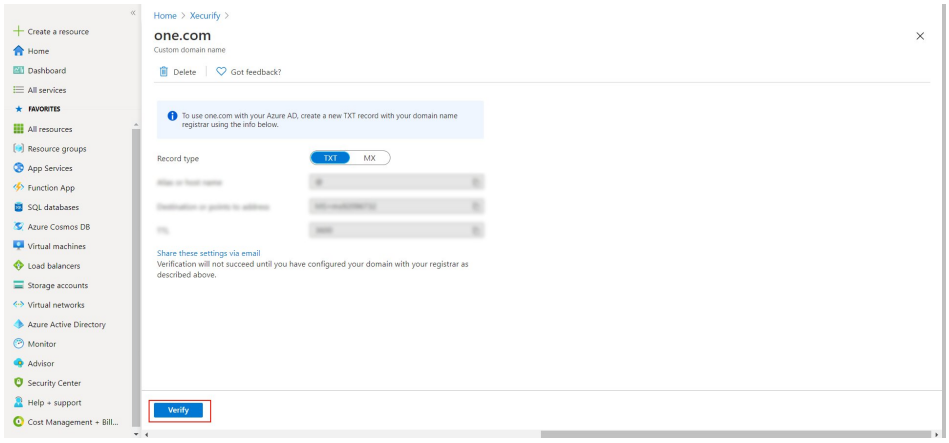
- Download the Azure AD Connect
- Run the Azure AD installer on your domain machine and follow the setup.

2. Verify your UPN Domain in Azure Portal

- In the Azure portal navigate to **Azure Active Directory >> Custom domain names** and click on **Add custom domain**.
- Enter the full domain name in the right pane that pops up and click on **Add domain**.



- A new window will open up with **TXT/MX** records for the domain. You will have to add the resented entry in your domain name registrar.



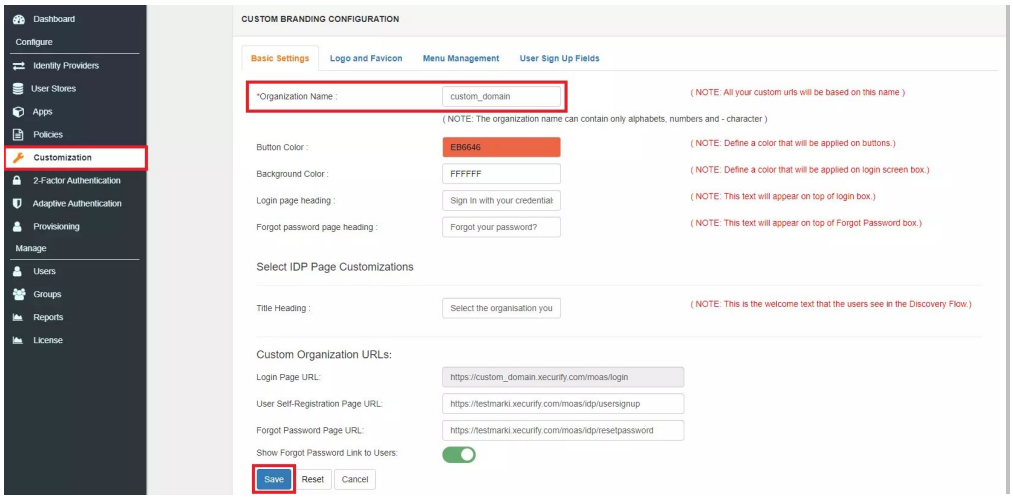
- Click on verify once you have added the entry

Follow the Step-by-Step Guide given below for Office 365 Single Sign-On (SSO)

1. Setup a Custom Branded URL in miniOrange Admin Console

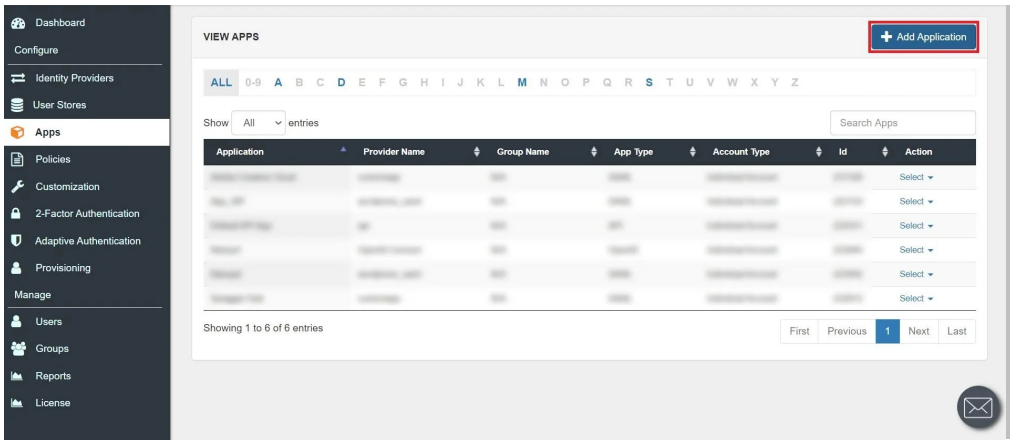
Single Sign-On into Office 365 requires a custom branded URL to be set. Access to miniOrange and connected resources will need to be through the custom branded URL in the format: **https://<custom_domain>.xecurify.com/moas**

- Login to miniOrange Admin Console.
- Click on **Customization** in the left menu of the dashboard.
- In **Basic Settings**, set the **Organization Name** as the custom_domain name.
- Click **Save**. Once that is set, the branded login URL would be of the format **https://<custom_domain>.xecurify.com/moas/login**

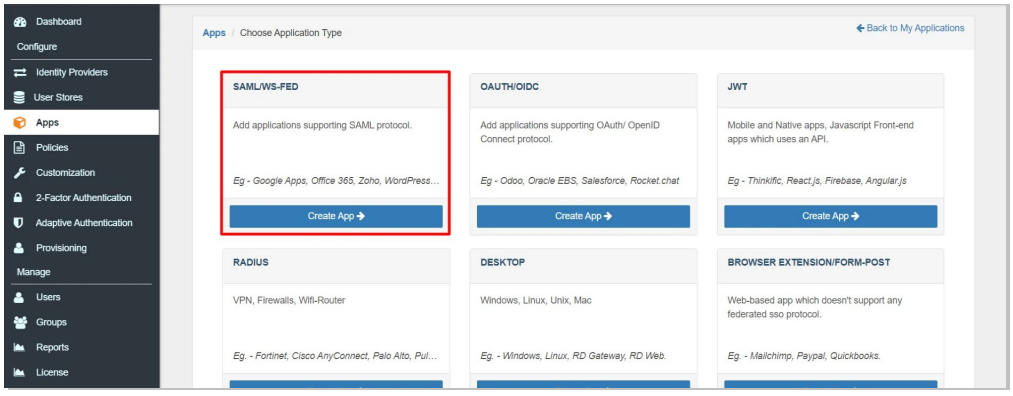


2. Configure Office 365 in miniOrange

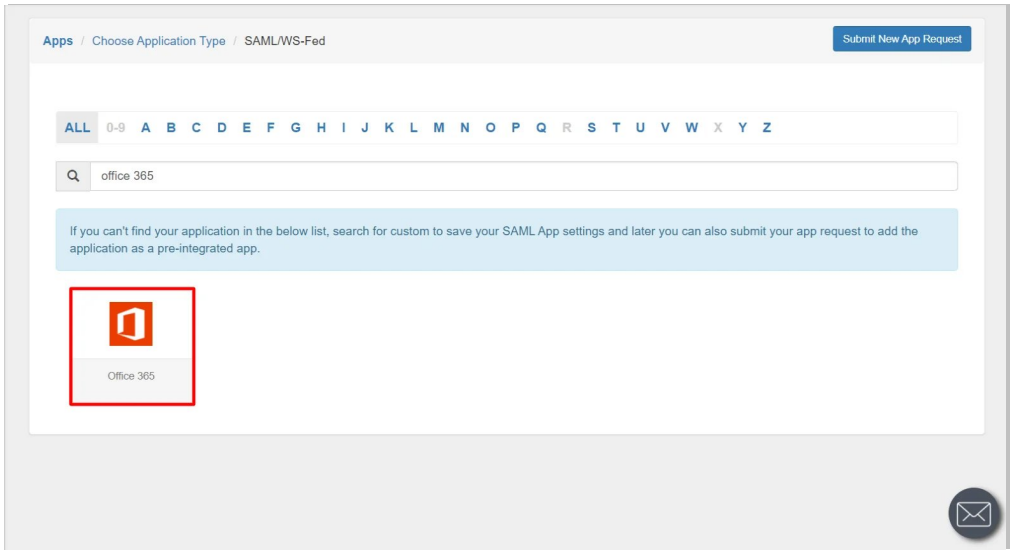
- Login into miniOrange Admin Console.
- Go to **Apps** and click on **Add Applicaton** button.



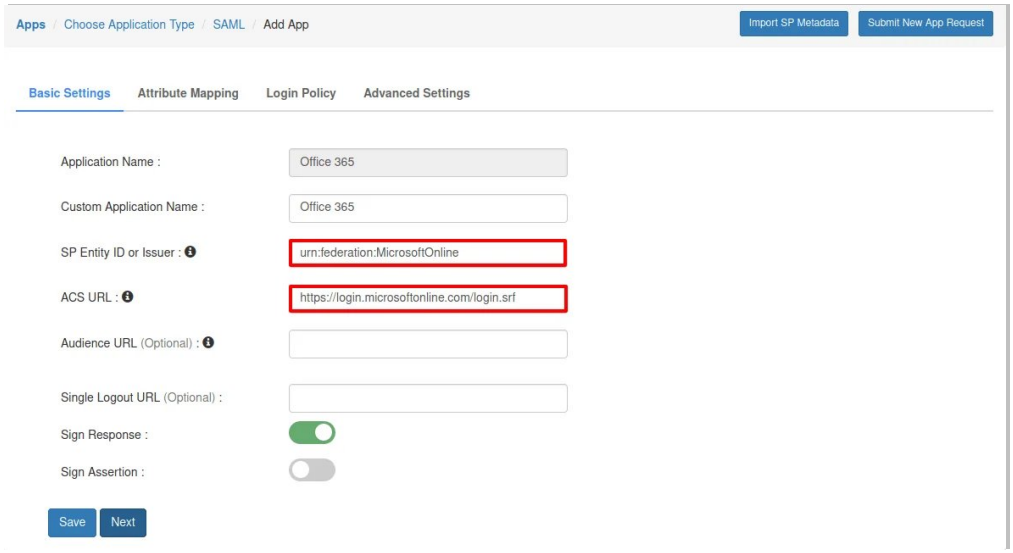
- In **Choose Application Type** click on **Create App** button in SAML/WS-FED application type.



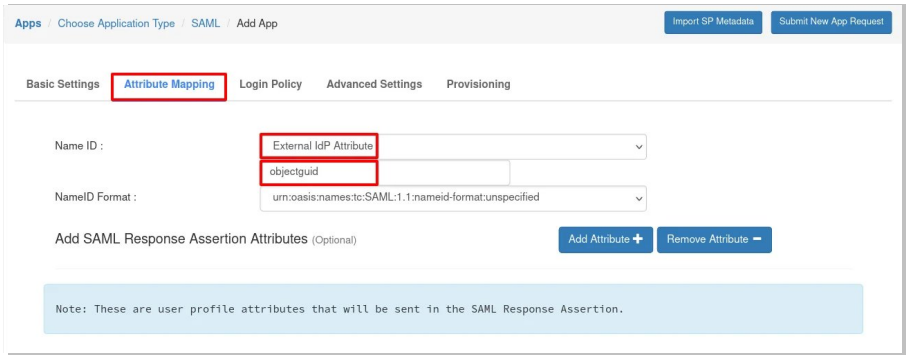
- In the next step, search for Office 365. Click on **Office 365** app.



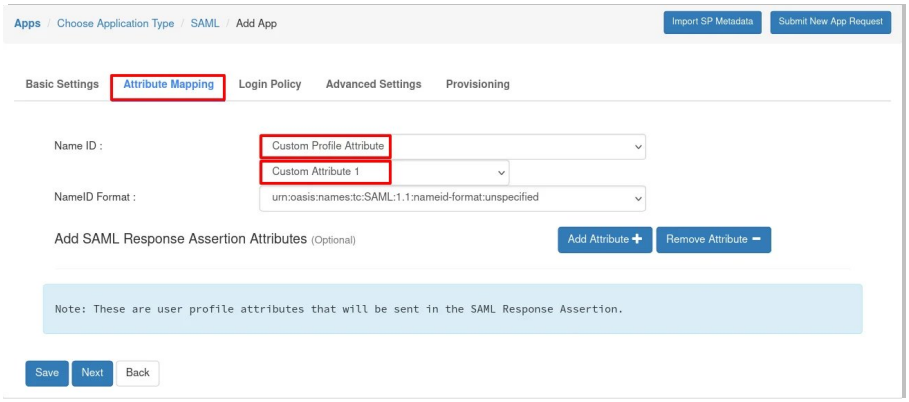
- Make sure the **SP Entity ID** or **Issuer** is: **urn:federation:MicrosoftOnline**
- Make sure the **ACS URL** is: **https://login.microsoftonline.com/login.srf**
- Click on **Next**.



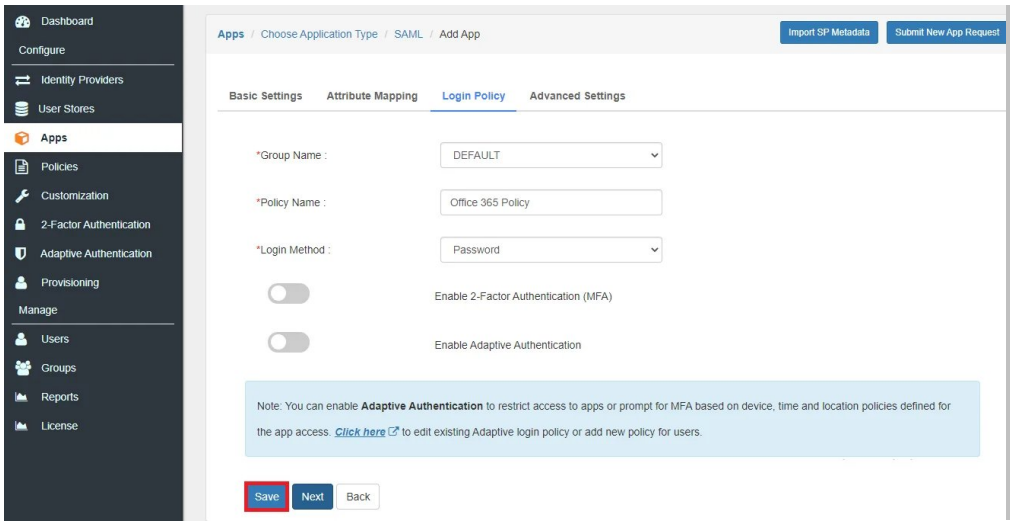
- Configure Name ID based on the User Store you are using:
    a. **Using Active Directory / miniOrange brokering service:** Select External IDP Attribute from the dropdown and add objectguid in the text-box that appears.



b. **Using miniOrange as a User Store:** Select Custom Profile Attribute and select a Custom Attribute from the drop-down.

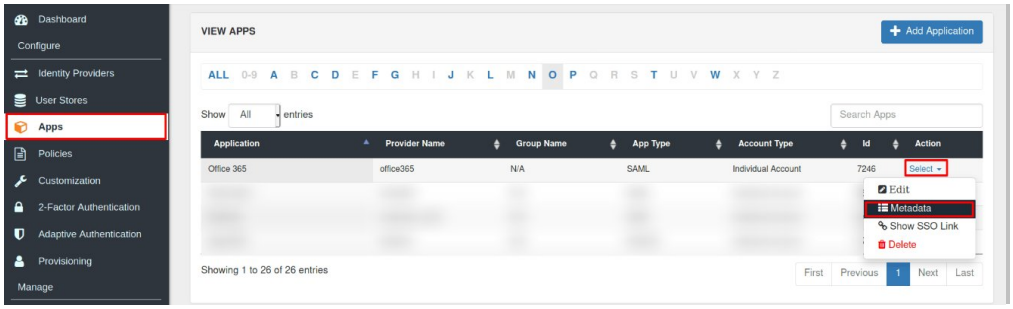


- Set the **login policy**. You can choose to enable 2FA for login or have users login using a standard username-password.
- Click on **Save** to configure Office 365.

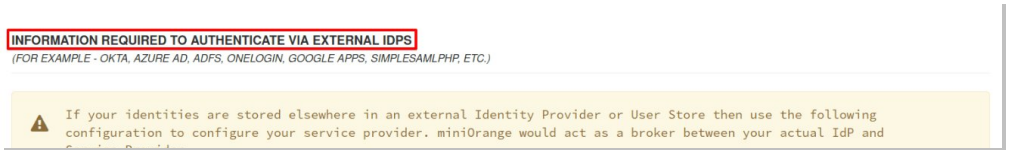


3. Configure Microsoft Online Services

- Click on **Select** dropdown and choose **Metadata**.



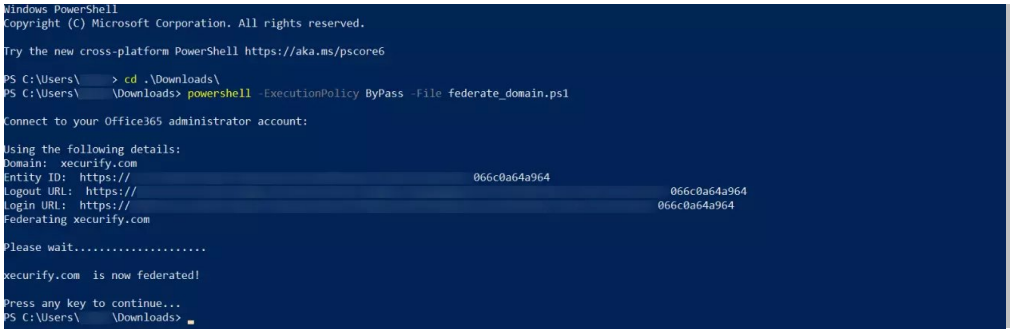
- Click on the **Download Federate Domain Script** button under **"INFORMATION REQUIRED TO AUTHENTICATE VIA EXTERNAL IDPS"**



- Enter the **domain name** that you want to federate and click on **Download**. **Note:** You cannot federate your default **"onmicrosoft.com"** domain. To federate your Office 365 tenant, you must add a custom domain to Office 365.

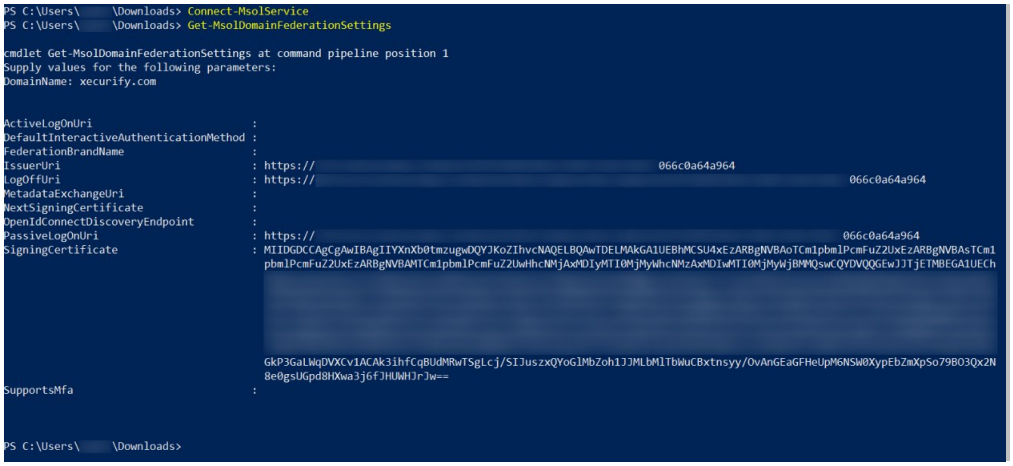
- After downloading the script, **Open PowerShell** run the federate_domain script using:

```
cd ./Downloads powershell -ExecutionPolicy ByPass -File federate_domai
n.ps1
```



- Your domain is now federated. Use the commands below to check your federation settings:

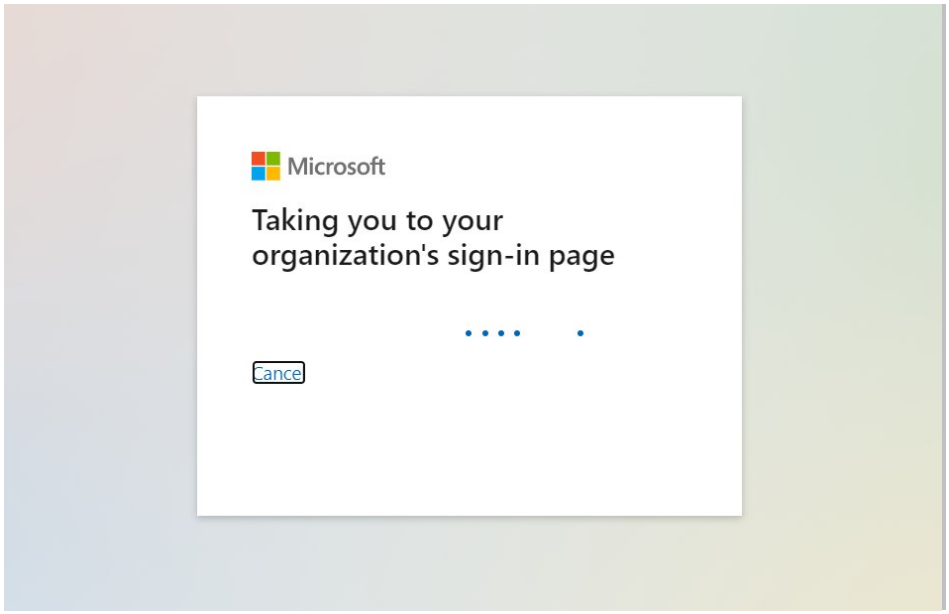
```
Connect-MsolService Get-MsolDomainFederationService
```



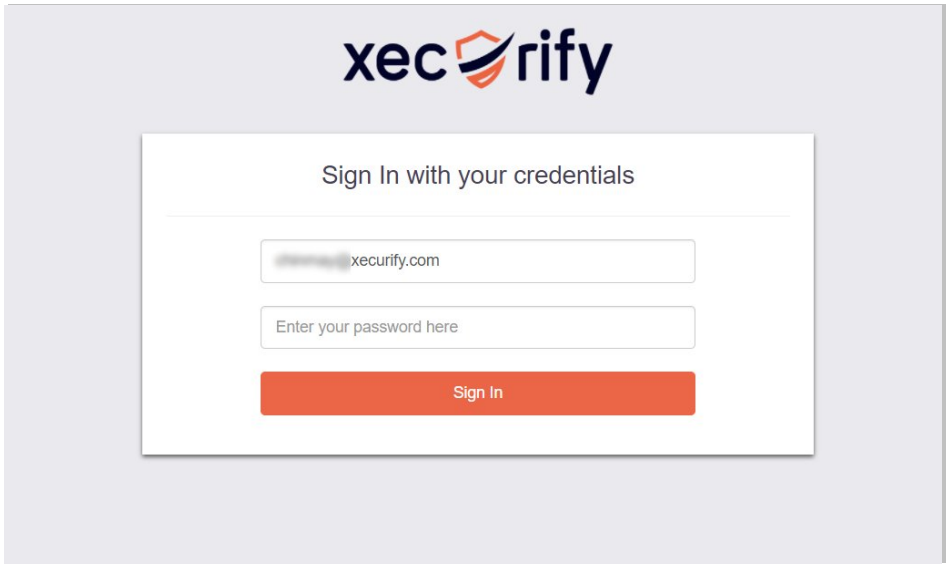
Step 6: Now sign in to your Office 365 account with miniOrange IdP by either of the two steps:

1. Using SP initiated login :-

- Go to Office 365 Login and click on sign-in
- You will be redirected to Microsoft Online portal. Here you have to enter the UPN of the user.(It should contain the domain that is federated with miniOrange)
- Now you will be redirected to miniOrange IdP Sign On Page.

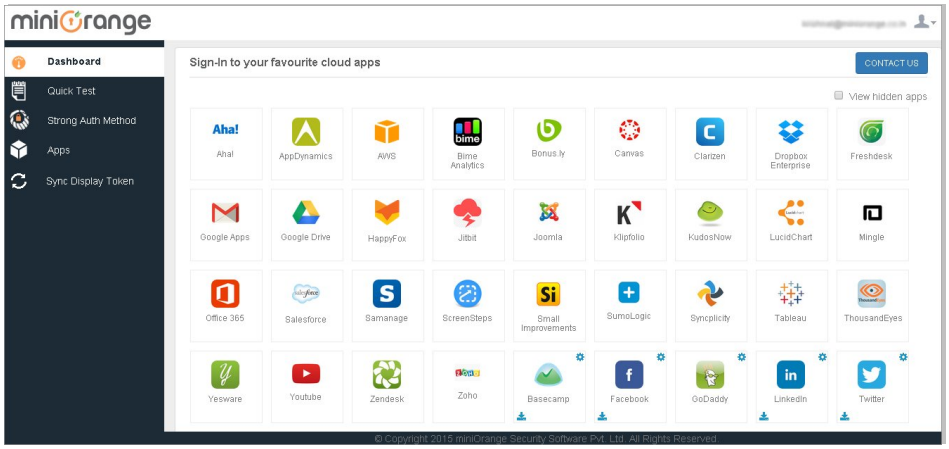


- Enter your login credential and click on Login. You will be automatically logged in to your Office 365 account.



2. Using IdP initiated login :-

- Login to your **miniOrange Self Service Console** as an End User and click on the **Office 365** icon on your **Dashboard**.
- Once you click on Office 365 you don't need to enter credentials again you will be redirected to Office 365 account.



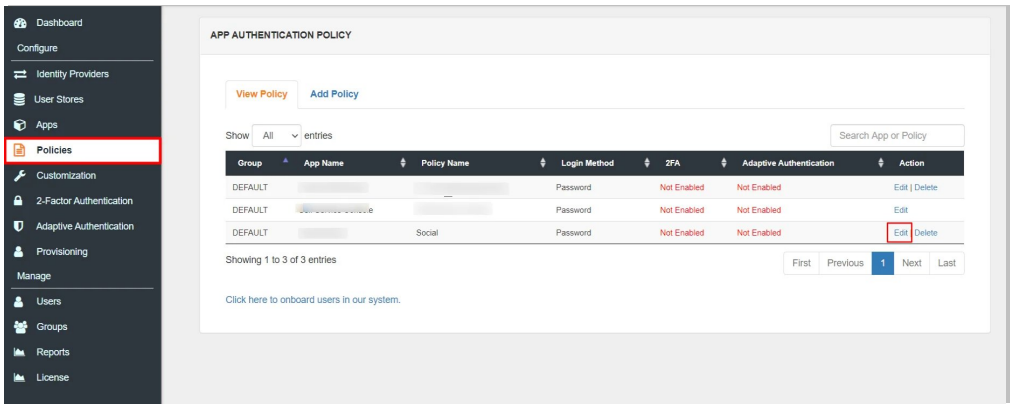
Step 7: Adaptive Authentication with Office 365

7.1: Restricting access to Office 365 with IP Blocking

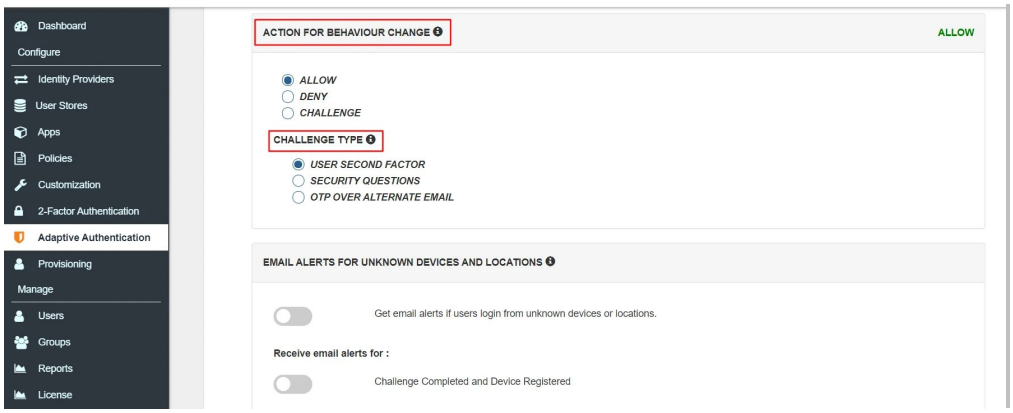
You can use adaptive authentication with Office 365 Single Sign-On (SSO) to improve the security and functionality of Single Sign-On. You can allow a IP Address in certain range for SSO or you can deny it based your requirements and you can also challenge the user to verify his authenticity. Adaptive authentication manages the user authentication bases on different factors such as Device ID, Location, Time of Access, IP Address and many more.

You can configure Adaptive Authentication with IP Blocking in following way:

- Login to **Self Service Console >> Adaptive Authentication**.
- Add a **Policy Name** for your Adaptive Authentication Policy.



- Select your **Action for behaviour Change** and **Challenge Type** for user from the **Action for behaviour Change** Section.



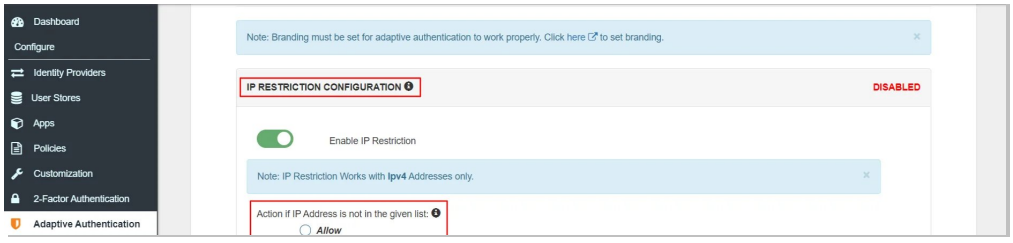
Action for behaviour Change Options :

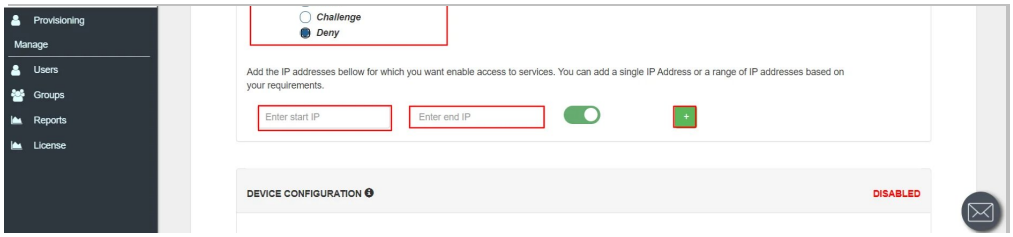
Attribute	Description
Allow	Allow user to authenticate and use services if Adaptive authentication condition is true.
Challenge	Challenege users with one of the three methods mentioned below for verifying user authenticity.
Deny	Deny user authentications and access to services if Adaptive authentication condition is true.

Challenge Type Options :

Attribute	Description
User second Factor	The User needs to authenticate using the second factor he has opted or assigned for such as • OTP over SMS • PUSH Notofication • OTP over Email • And 12 more methods.
KBA (Knowledge-based authentication)	The System will ask user for 2 of 3 questions he has configured in his Self Service Console. Only after right answer to both questions user is allowed to proceed further.
OTP over Alternate Email	User will recieve a OTP on the alternate email he has configured threw Self Service Conolse. Once user provides the correct OTP he is allowed to proceed further.

- Now Enable **Enable IP Restriction** option from the **IP RESTRICTION CONFIGURATION** section to configure custom IP range.





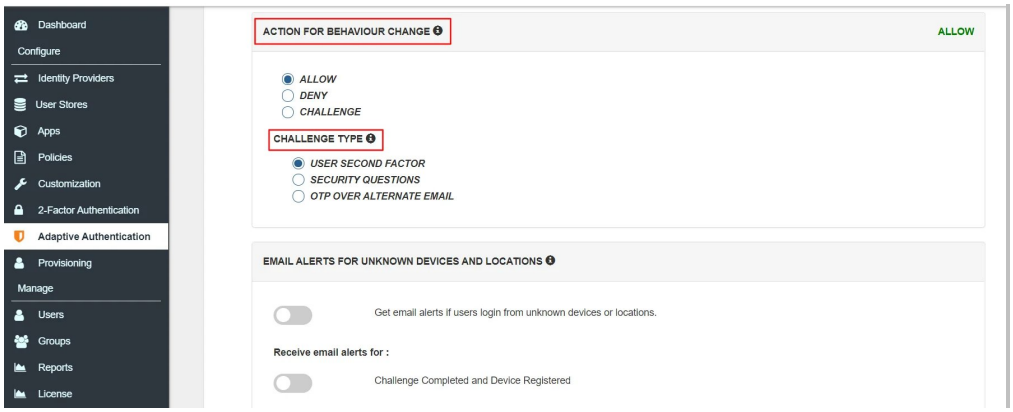
- Select the **Action** you want to perform if the IP address is out of the range. i.e Allow, Challenge & Deny.
- Specify the IP Address range for which you want above setting to reflect. You can add more than one IP Address ranges by clicking on following button **+**.
- Scroll to the end and click on **save**.

7.2: Adaptive Authentication with Limiting number of devices.

Using Adaptive Authentication you can also restrict the number of devices the end user can access the Services on. You can allow end users to access services on a fixed no. of devices. The end users wii be able to access services provided by us on this fixed no. of devices.

You can cofigure Adaptive Authentication with Device Restriction in follwing way

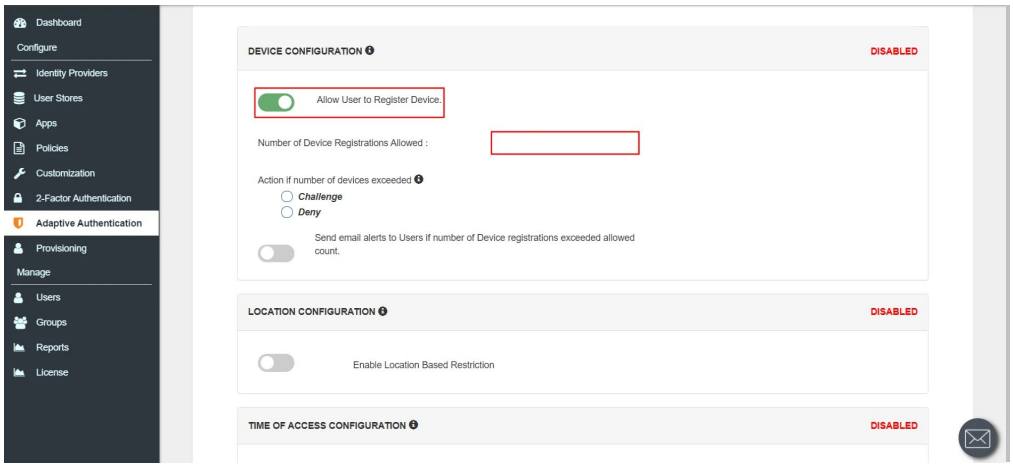
- Login to **Self Service Console >> Adaptive Authentication**.
- Add a **Policy Name** for your Adaptive Authentication Policy.
- Select your **Action for behaviour Change** and **Challenge Type** for user from the **Action for behaviour Change** Section.



- Scroll down to **Device Configuration** section and enable **Allow User to Register Device** option to allow users to register their devices.
- Enter the **Number of Devices** which are allowed to register in field next to **Number of Device Registrations Allowed**
- Choose **Action** if number of devices exceeded (This will override your setting for **Action for Behaviour Change.**)
    - **Challenge**: The user needs to verify himself using any of the three methods mentioned in table in step 7.1

- **Deny** : Deny users access to the system

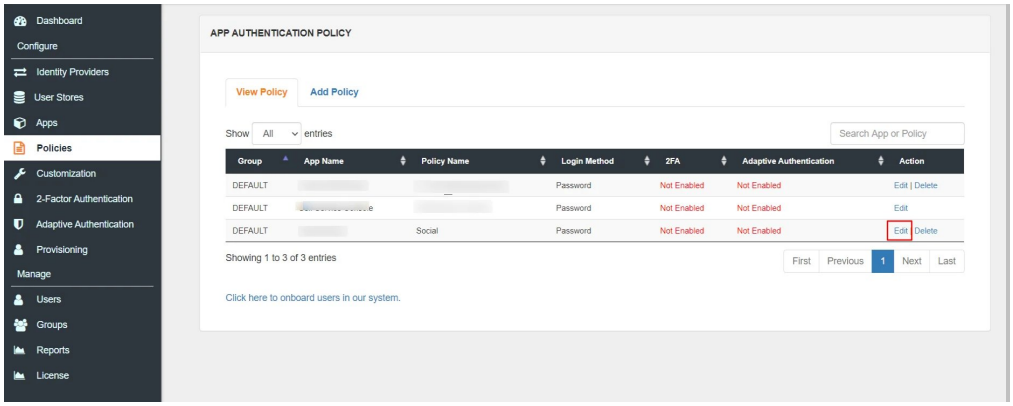
- Enable option **Send email alerts to Users if number of Device registrations exceeded allowed count** if you want to alert the user about no of devices exceeding the limit. Save the configuration.



7.3: Add Adaptive Authentication policy to Office 365.

- Login to **Self Service Console >> Policies**.

- Click on **Edit** option for predefined SAML app policy.



- Set your application name in the **Application** and select password as **Login Method.**

- Enable **Adaptive Authentication** on Policy page and select the required **restriction method** as an option.

- From **Select Login Policy** dropdown select the policy we created in last step and click on save.