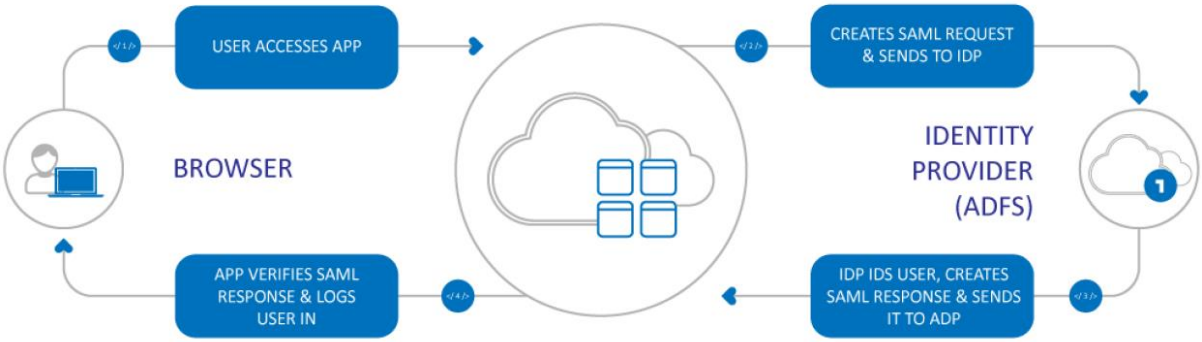
Setting up MEX SSO

SSO comes as a standard feature and takes the hassle out of having to remember different credentials for multiple applications and eliminates the need to individually log into each one every time you need to use it. MEX handles this in the back end allowing users to open up and instantly use all MEX applications with their credentials automatically activated.

How Single Sign On Works With MEX Applications

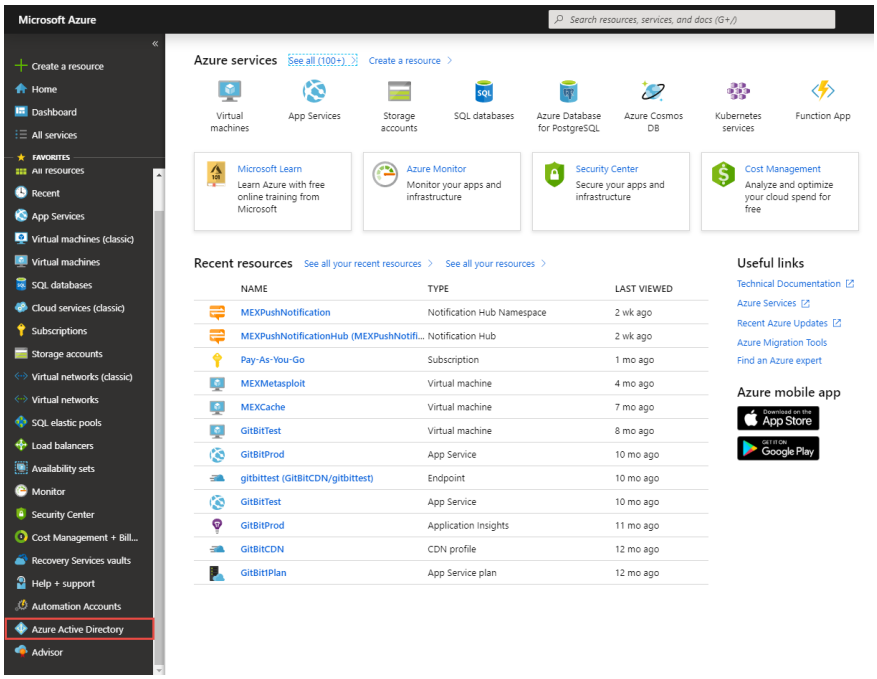
MEX SSO allows customers to specify an Identity Provider (such as ADFS) that MEX 15 can authenticate against, utilising your choice of either WS-Federation or SAML 2.0 protocols. This means that once a user has logged into the Identity Provider they will not need to enter any credentials again and MEX will know who they are.
Upon opening the MEX application, MEX will cross check their credentials within the MEX Database and if that user exists, grant them access. In the case where the user does not exist, a new user is created in MEX with the selected security group nominated in the setup of MEX SSO for new users. Here is a flow chart illustrating this process:



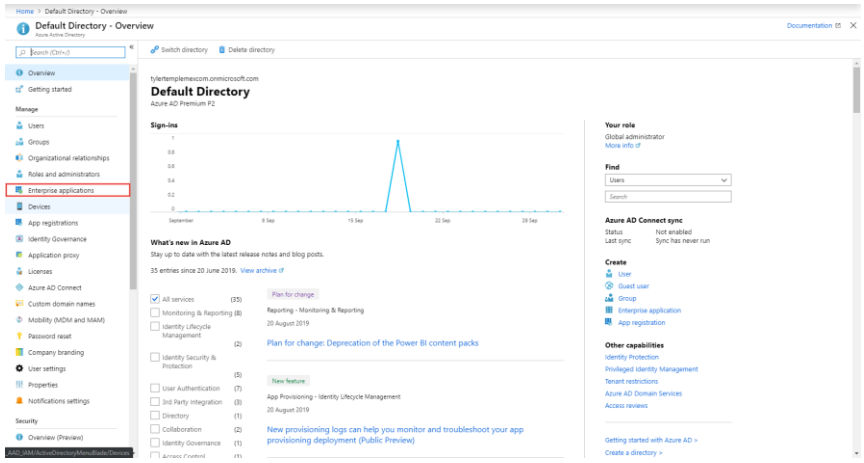
All MEX applications are compatible with the MEX SSO including **MEX**, **FleetMEX**, **MEX Ops** and the newly released **MEX Dashboard**.

Setting Up Azure SSO – Creating the Enterprise App

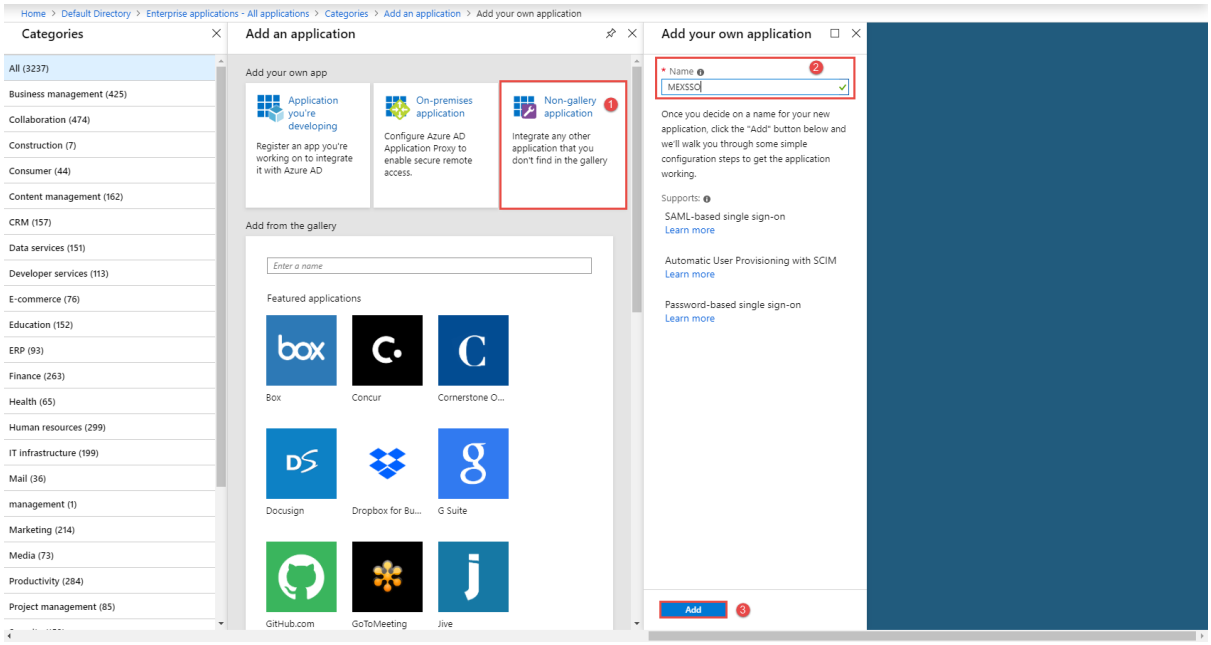
1. Select the option for **Azure Active Directory**



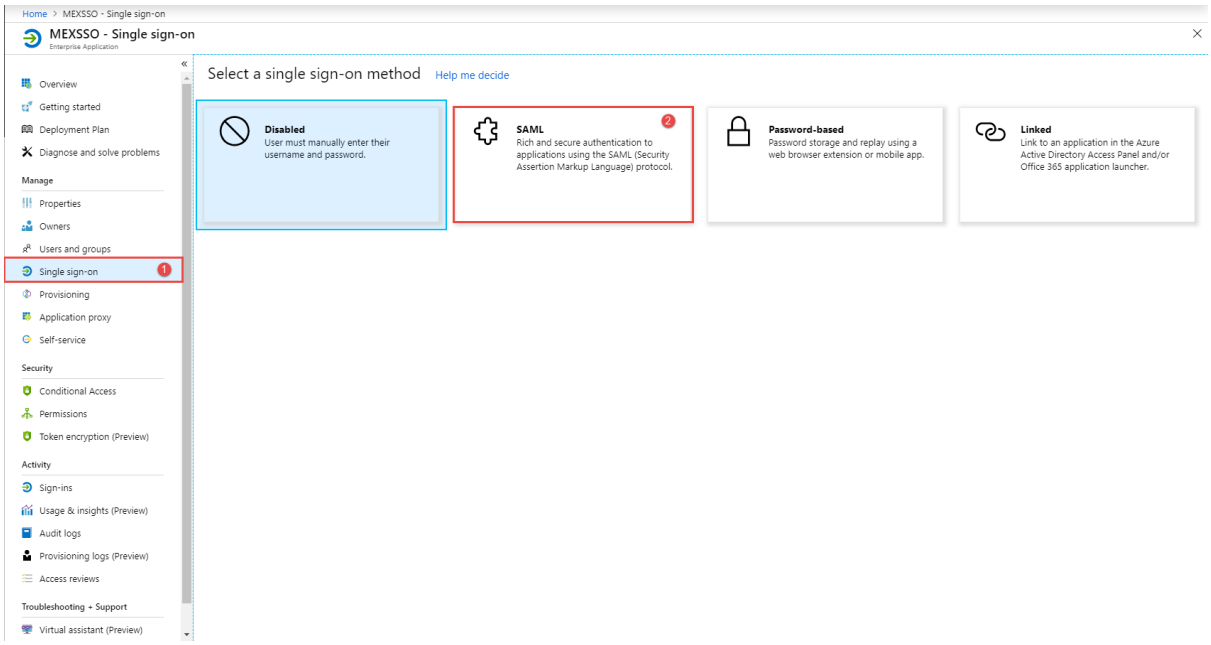
2. Select **Enterprise Applications**, then in the Enterprise application listing, select the **New Application** button



3. Creating the New application
    1. Select option for a **Non-gallery application**
    2. Assign a name for the SSO application (EG MEXSSO)
    3. Save

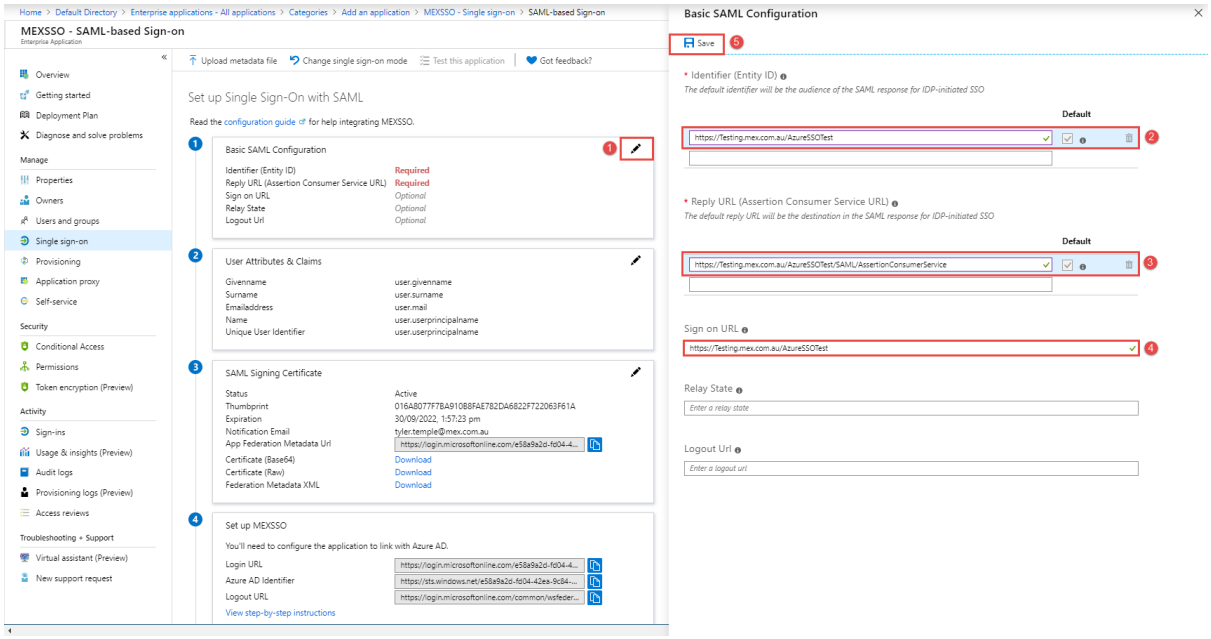


4. From the left-hand side, Select the **Single Sign-on** then **SAML** options



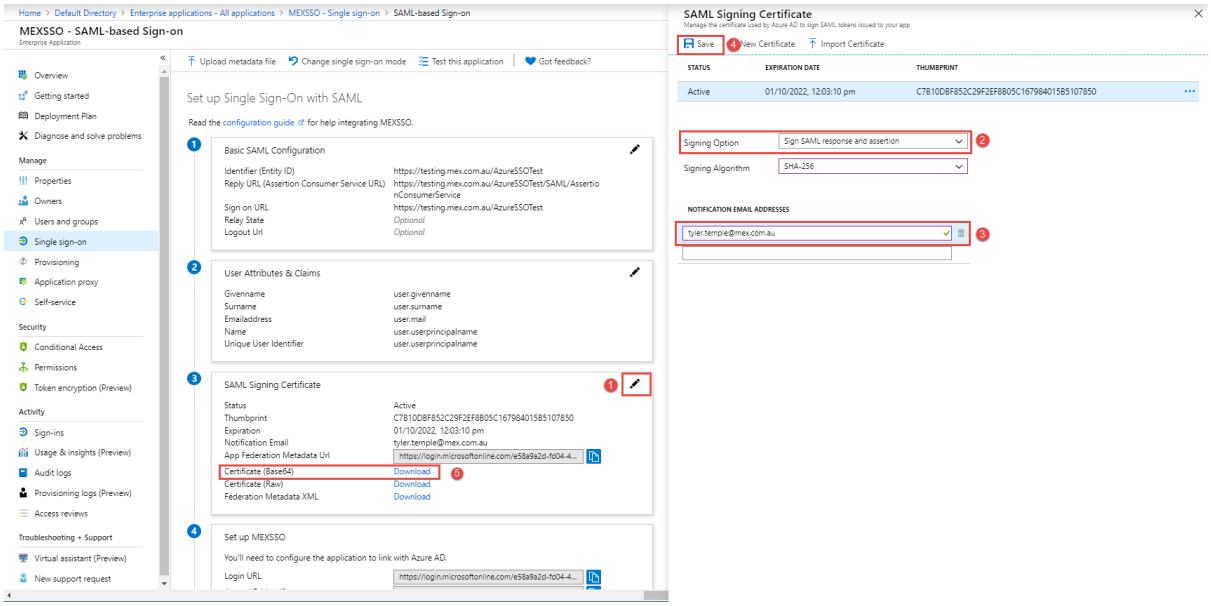
Setting Up Azure SSO – Apply SSO SAML Settings

1. Setup the Basic SAML Configuration
    1. Select the Edit icon against **Basic SAML Configuration**
    2. In the **Identifier** field, set the URL used to access your MEX site
    3. In the **Reply URL** field, enter the MEX URL + **SAML/AssertionConsumerService**
    4. Set the **Sign on URL** to be the MEX URL as well
    5. Save your changes



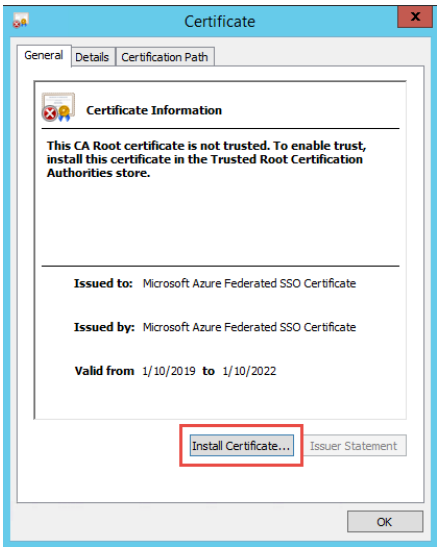
2. Review the User Attributes & Claims
    1. Select the edit icon under **User Attributes & Claims**
    2. In the User Attributes & Claims window, ensure **UserPrincipleName** is assigned to the email option (should be enabled by default)
    3. Assign any additional claims required.

3. Apply the default certificate
    1. Select Edit icon against the **SAML Signing Certificate** window
    2. Change the **Signing Option** to: **Sign SAML response and assertion**
    3. Optional: Edit the **Notification Email Address**, this user will be notified when the assigned certificate expires.
    4. Save changes
    5. Download a copy of the Certificate (xBase64) created



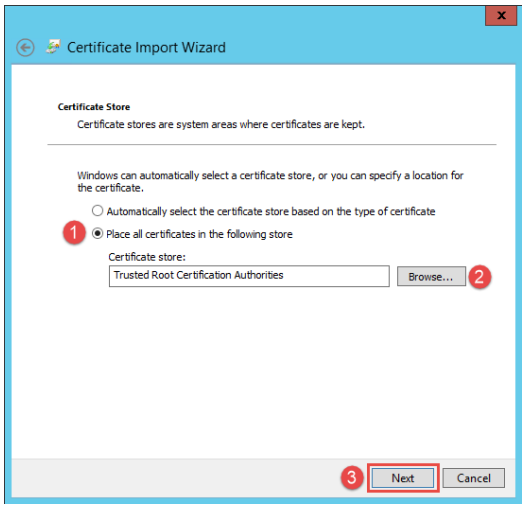
4. Installing the Certificate for **Hosted MEX Users**.
    1. If you are a hosted user please email the certificate downloaded in the previous step to Support@mex.com.au
    2. MEX Support will reply to the email once the certificate has been installed onto the hosting server.
    3. Once installed, we can continue with the setup of Azure SSO and move to the next step for Enabling SAML in Mex

5. Installing the Certificate for **Non-Hosted MEX Users**
    1. Transfer the Certificate downloaded to the Server machine running MEX
    2. As an Administrator user, open the certificate file and select the option to install

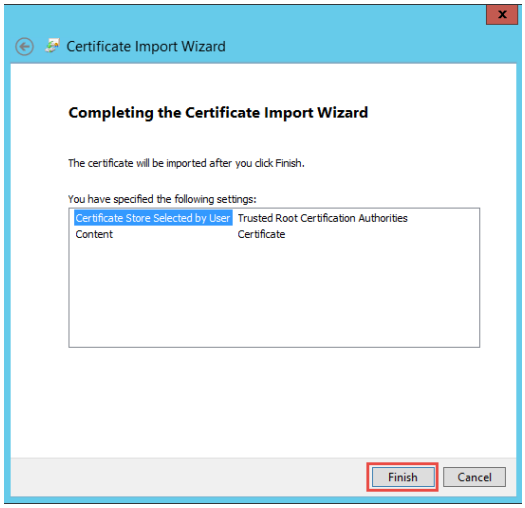


3. Set the **Store location** as **Local Machine**

4. Select where to store the certificate
    1. Choose the option **Place all certificates in the following store**
    2. Click on **Browse** and Select the **Trusted Root Certification Authorities**



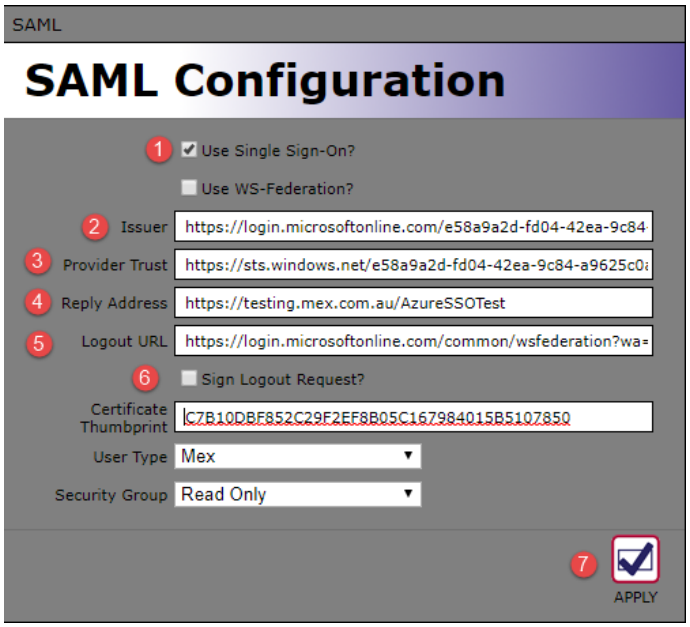
5. Review details and finish the installation



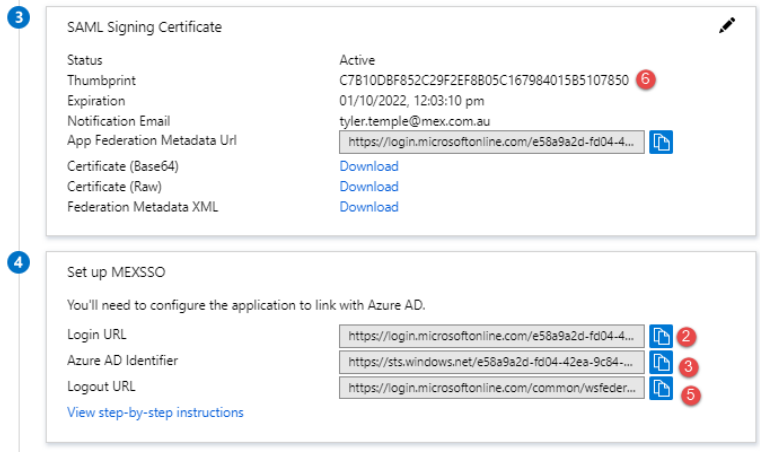
Setting Up Azure SSO – Enabling SAML in Mex

The next step will require navigating to the SAML setup in MEX itself. While still logged into the Azure Portal, open a new browser tab and enter the MEX URL followed by '/SAML/', in this example the URL will be: http://testing.mex.com.au/AzureSSOTest/SAML/

The Data asked to be assigned is coming from the 'Set Up MEX SSO' window in the Azure Portal



1. Against each field, set the following
    1. Tick field to **Use Single Sign-On**
    2. Set **Issuer** equal to the **Login URL** from the Azure Portal
    3. Set the **Provider Trust** to the **Azure AD Identifier**
    4. The **Reply Address** is the URL used to access MEX
    5. **Logout URL** will be the same **Logout URL** from Azure
    6. Set the **Certificate Thumbprint** equal to the **Thumbprint** in Azure



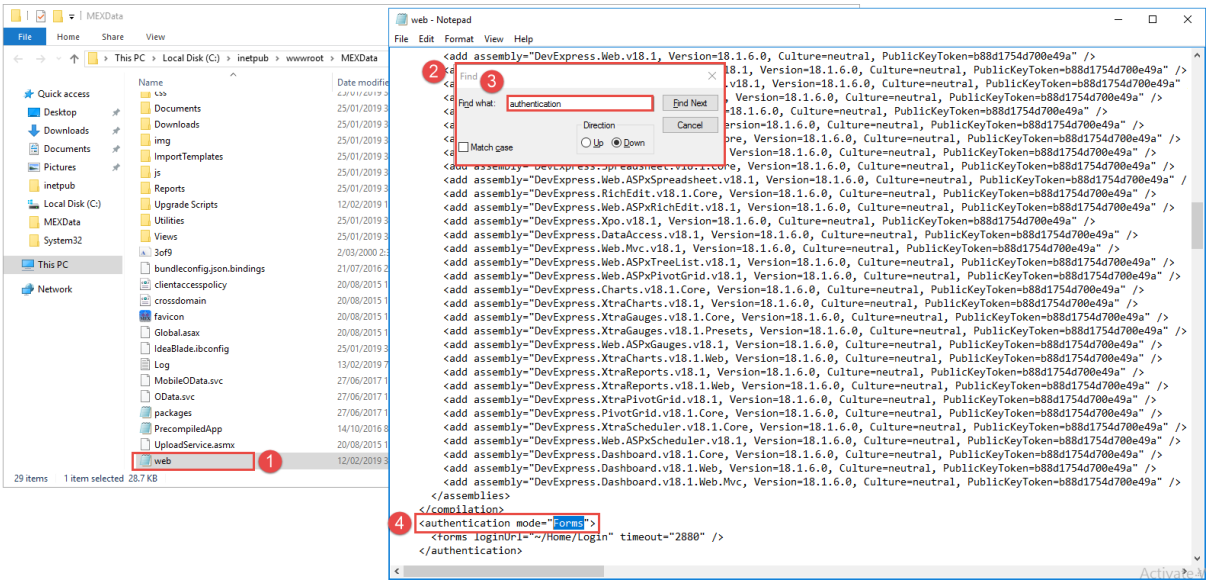
SAML Configuration Data Sources

Setting Up SSO – Update MEX Web Config

The next stage is to update the MEX config settings to allow the SSO functionality.

1. Navigate to the MEXData web files, and open the **web.config** file in Notepad.
2. Open the Search tool with the keyboard command **'Ctrl + F'**
3. Search the word **'Authentication'**
4. Replace the value on the first search result from **'Windows'** to **'Forms'**
5. Save the document and close out of it.

Note: *If hosted by MEX, please contact MEX at cloud.admin@mex.com.au to get this changed*

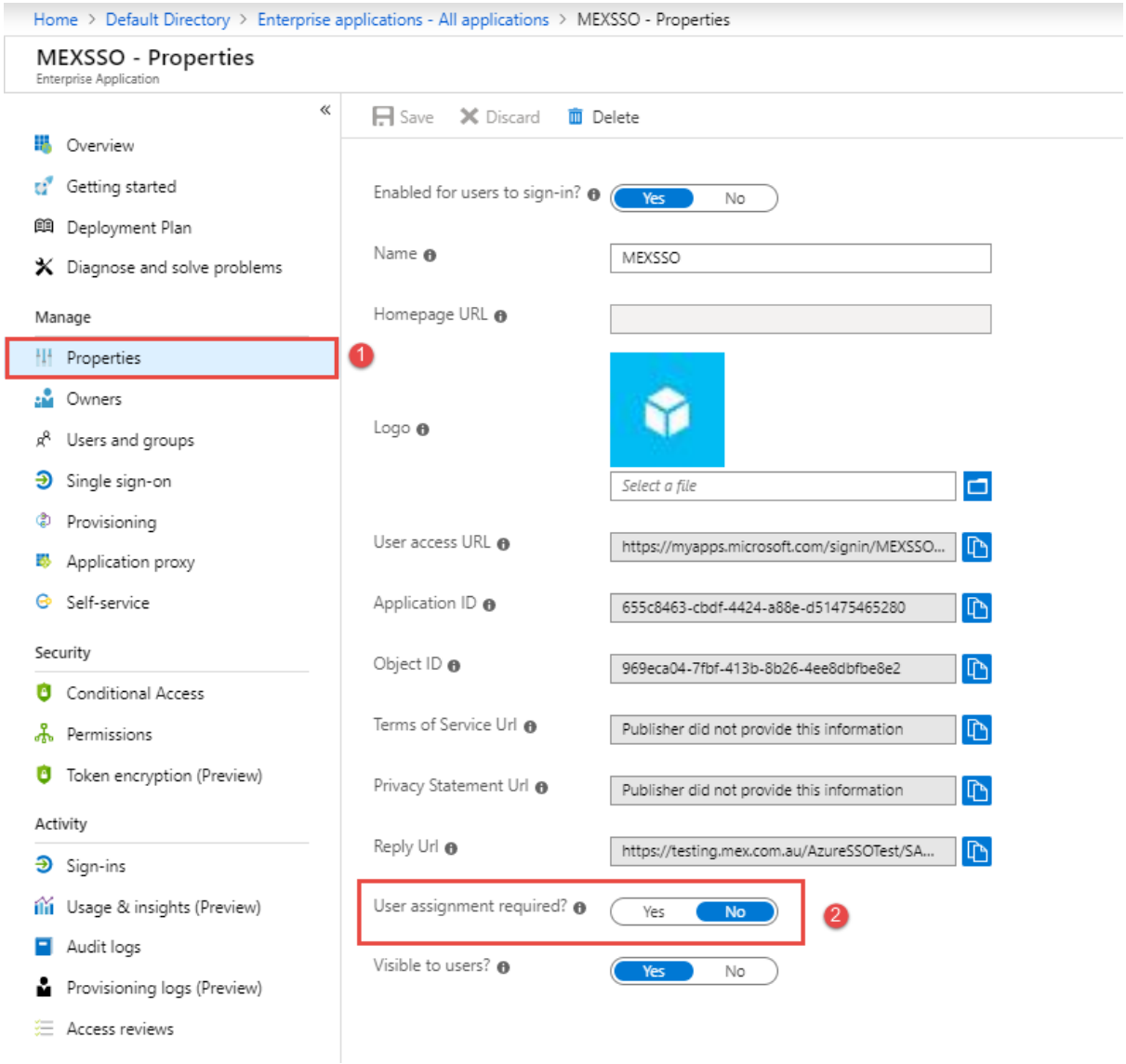


Setting Up Azure SSO – Setting User Access

The last action to complete is setting up Azure user's access to MEX, this can be set up to allow all azure users access, or set up to require access to be applied on a per user basis.

To allow all users:

1. Navigate to the properties of the MEX SSO Enterprise app
2. Change the option for 'User Assignment Required' to No



To allow individual users:

Alternatively, if you are required to apply access to SSO functionality per each user, we can ignore the steps above and leave the ‘User Assignment Required?’ field remaining on Yes. Instead we can apply each user’s level of access from the ‘Users and groups’ module.

1. Navigate to ‘Users and groups’ module
2. Select ‘Add User’ button
3. Select to add by ‘Users and groups’
4. Select User on the right-hand side to allow access
5. Selected users will be listed here
6. Click the select button to save them with access to use SSO