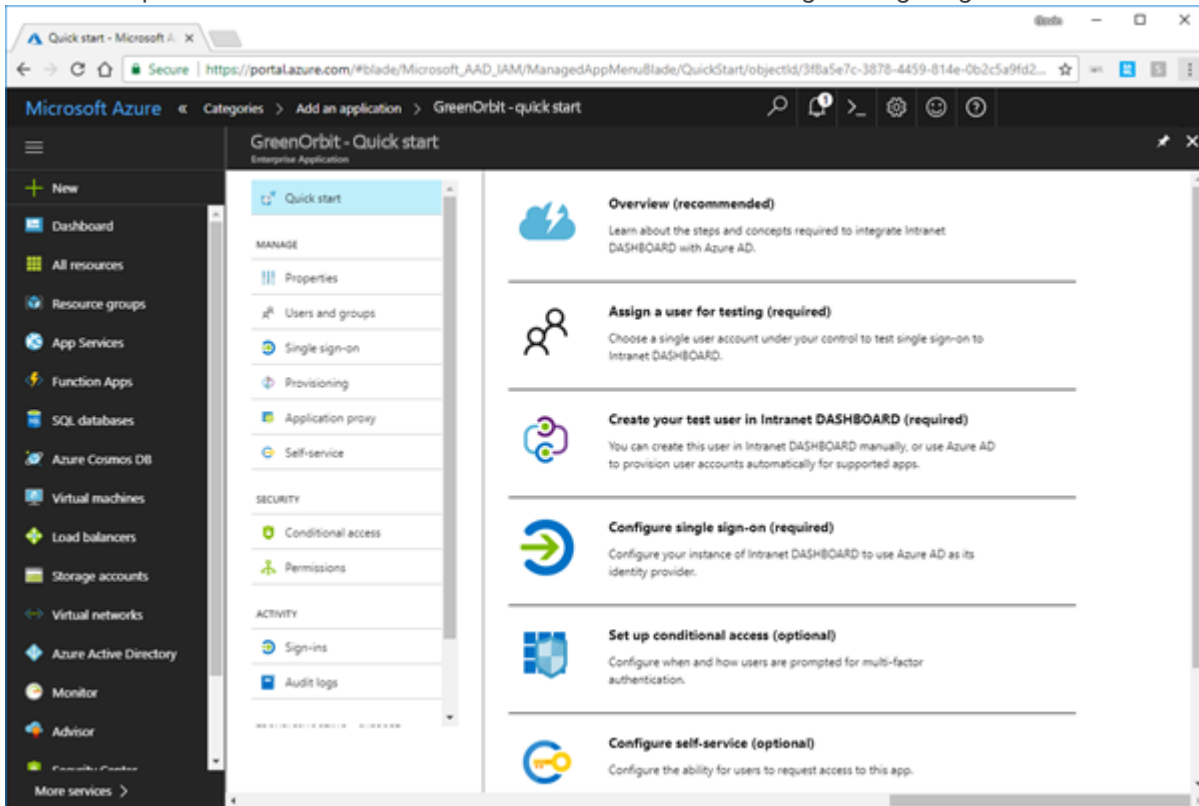
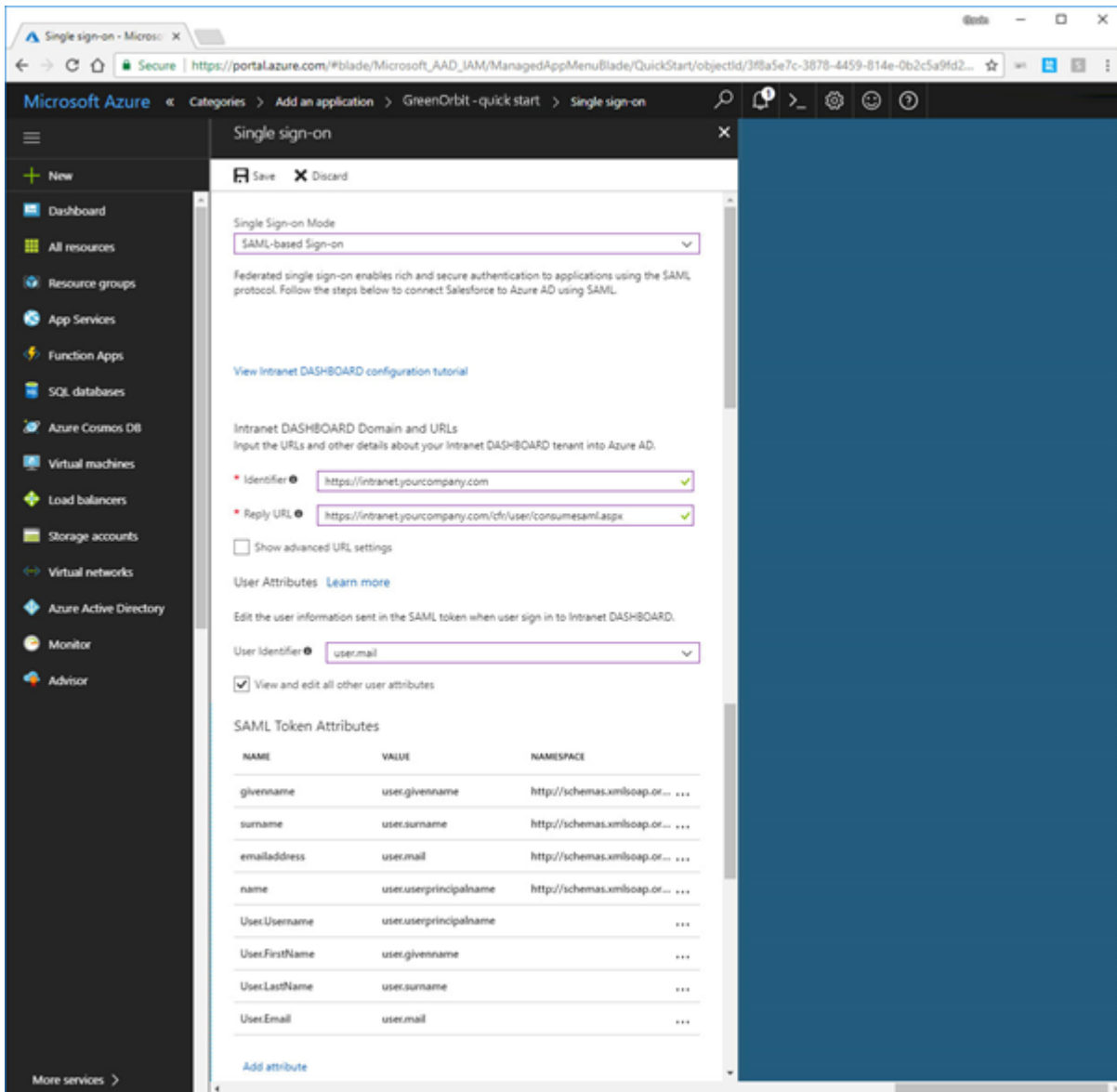


4. You will be presented with the Quick Start menu. Proceed to *Configure single sign-on*

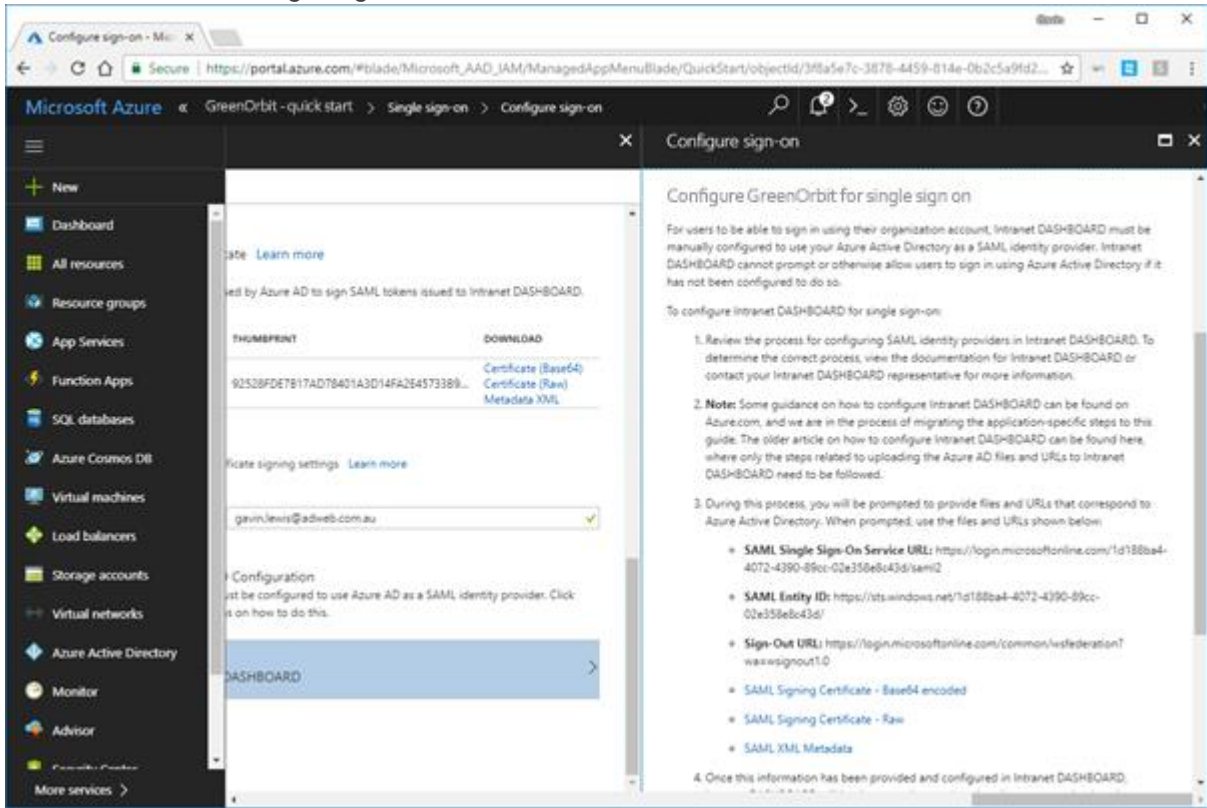


5. Select *SAML-based Sign-on* from the list and proceed to configure the options as presented below:
 - a. Intranet DASHBOARD Domain and URLs
 - i. Identifier: *https://intranet.yourcompany.com*
 - ii. Reply URL: *https://intranet.yourcompany.com/cfr/user/consumesaml.aspx*
 - b. User Attributes
 - i. User Identifier: *user.mail*
 - ii. View and edit all other user attributes: Yes
 - iii. SAML Token Attributes:

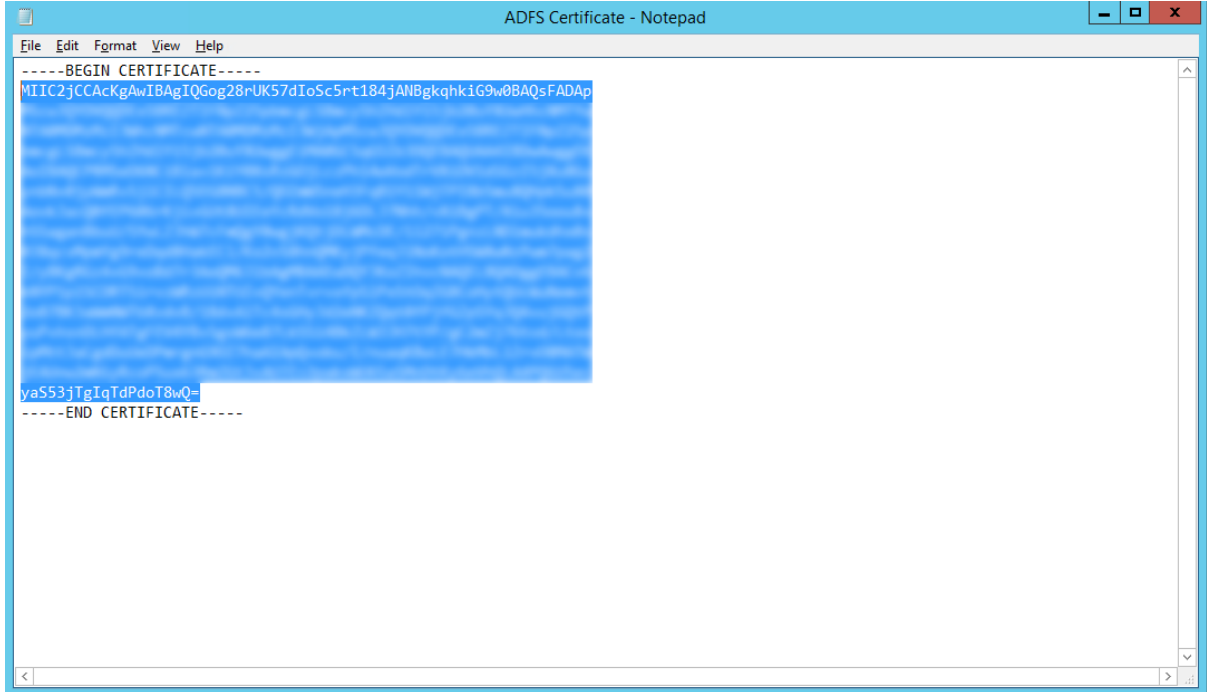
Name	Value
User.Username	user.userprincipalname
User.FirstName	user.givenname
User.LastName	user.surname
User.Email	user.mail



- Click **Save** and then select **Configure Intranet DASHBOARD**. Download a copy of the Base 64 certificate and take note of the **Single Sign-on Service URL**.

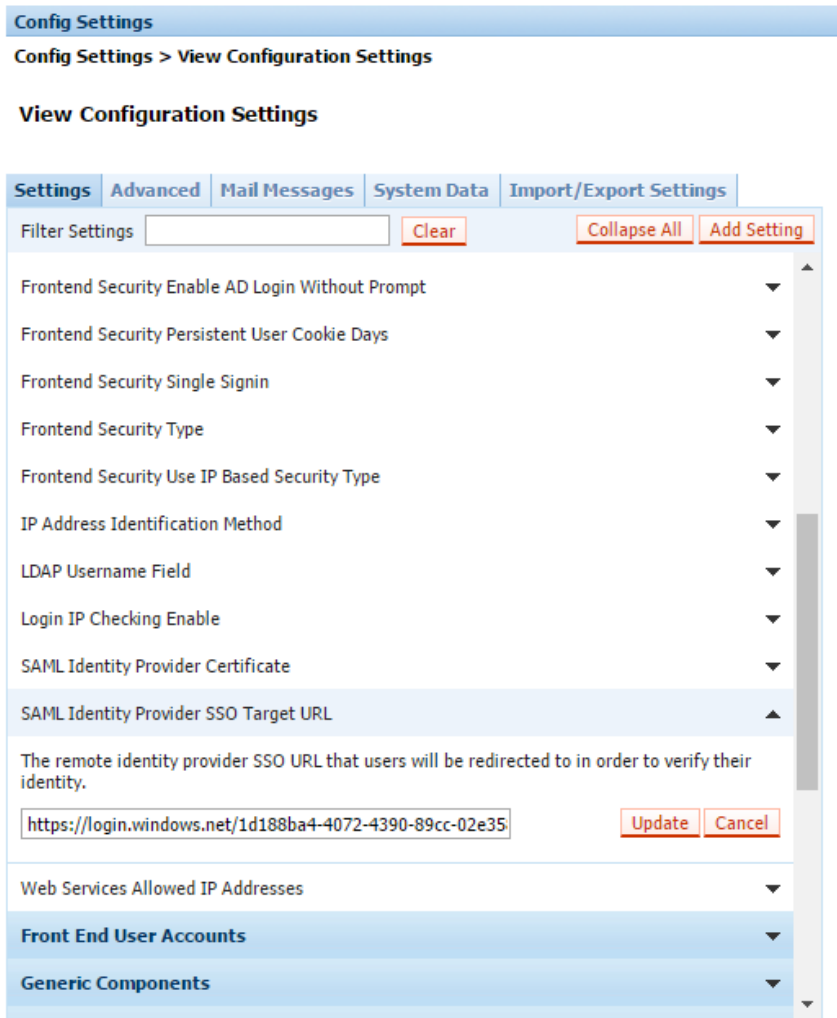


- Open a copy of your certificate that you downloaded in the previous step with your preferred text editor (such as notepad) and select the text between the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines.



- Now select the Config Setting *SAML Identity Provider SSO Target URL*, this is the *Single Sign-On Service URL* provided earlier in the application configuration. Get this URL and then put it into iD's config setting as:

`https://login.microsoftonline.com/<ApplicationID>/saml2`



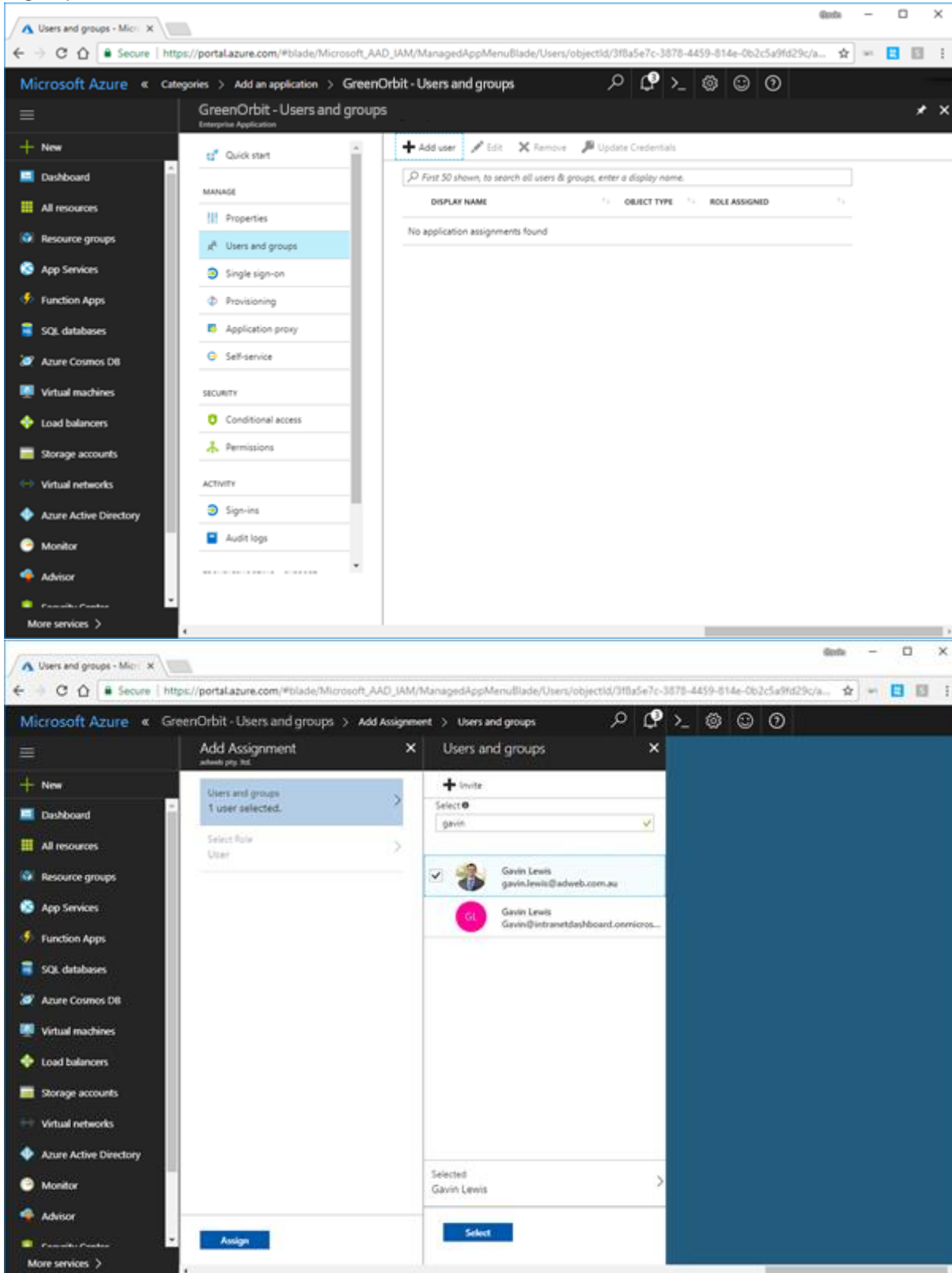
The screenshot shows the 'Config Settings' page with the following elements:

- Header: **Config Settings**
- Navigation: **Config Settings > View Configuration Settings**
- Section: **View Configuration Settings**
- Tabs: **Settings** (selected), **Advanced**, **Mail Messages**, **System Data**, **Import/Export Settings**
- Filter Settings: **Clear** **Collapse All** **Add Setting**
- Settings List:
 - Frontend Security Enable AD Login Without Prompt
 - Frontend Security Persistent User Cookie Days
 - Frontend Security Single Signin
 - Frontend Security Type
 - Frontend Security Use IP Based Security Type
 - IP Address Identification Method
 - LDAP Username Field
 - Login IP Checking Enable
 - SAML Identity Provider Certificate
 - SAML Identity Provider SSO Target URL** (highlighted)
- Description for SAML Identity Provider SSO Target URL: "The remote identity provider SSO URL that users will be redirected to in order to verify their identity."
- Input Field: **Update** **Cancel**
- Other settings: Web Services Allowed IP Addresses, **Front End User Accounts**, **Generic Components**

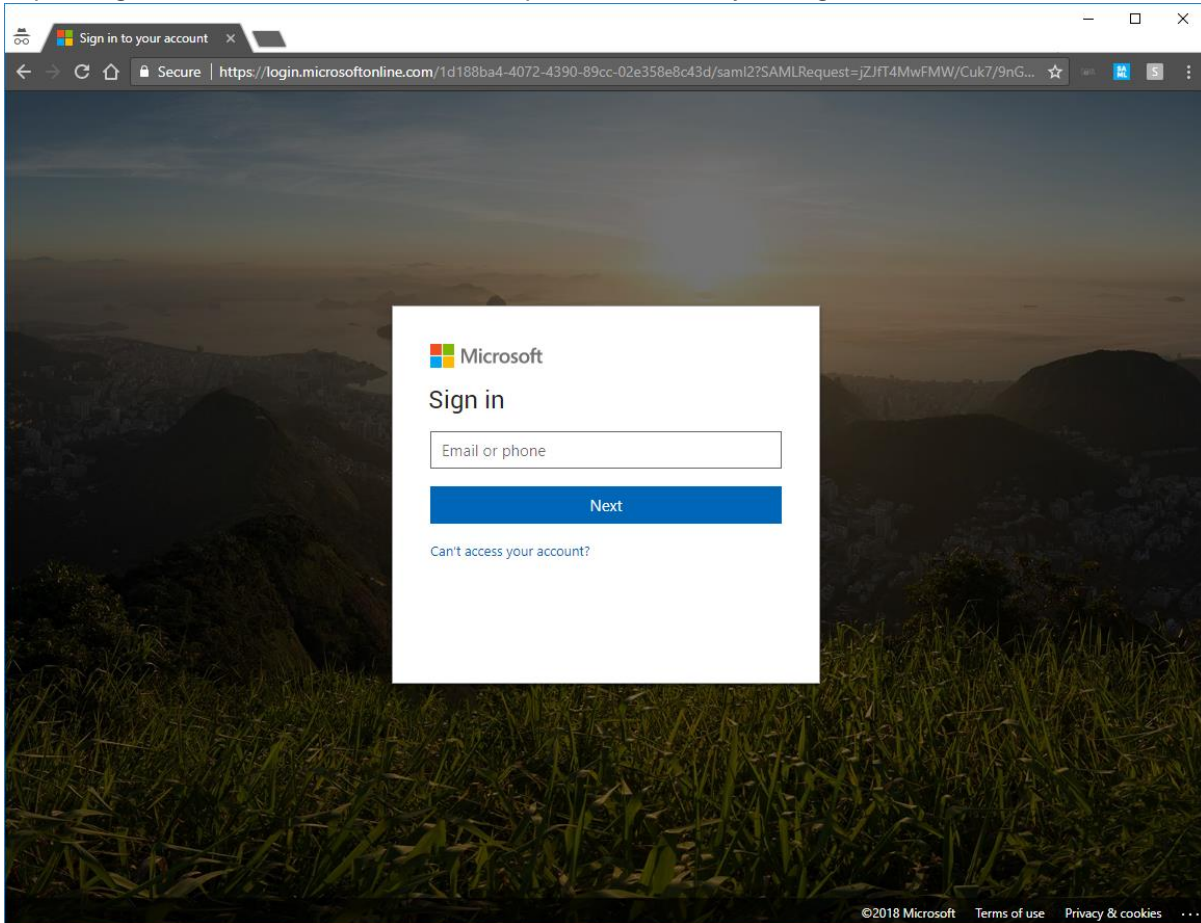
- If you haven't already done so, also change the Frontend Security Type to *Login using SAML*. Follow the guide on our help site to learn how to do this:

<http://help.intranetdashboard.com/systemadmin/Security/ChangingtheFrontendSecurityType.html>

- Now choose the *Users and Groups* item from the horizontal navigation. Select the Users or Groups who you want to grant access to the intranet and then select *Add user* then select and assign the users or groups who will have access to 2.



12. Now when accessing your intranet address, eg <https://intranet.yourcompany.com> you'll be redirected to authenticate by O365 prior to being logged into the site. Your authentication experience may vary depending on how O365/Azure has been implemented within your organization.





ADDITIONAL INFORMATION

If you have been unsuccessful configuring O365/Azure AD to act as an SAML Identity Provider for GO, please reach out to our support team at support@greenorbit.com.