1. Go to the Active Directory Tab in the Azure Management Portal
2. Click on Access Control Namespaces in options at the top of the page
3. Click “+ New” and select Access Control -> Quick Create to create a new ACS Namespace.
4. Enter the desired Namespace name and the Region. **Copy the full url to the ACS Namespace value into the AcsEndpoint appSetting value in the App.config of the sample application**. The value should look like [https://*yourname*.accesscontrol.windows.net](https://yourname.accesscontrol.windows.net) where “yourname” is replaced with the Namespace name you selected.
5. Once the new ACS Namespace is created, click Manage to go to the management portal for ACS.
6. Click on “Relying party applications” on the left menu. Then click add. You will need to fill in the

following pieces of data:

* 1. Name -> Enter a name for the Relying party.
  2. Realm -> Enter a URI. This will be the Scope or Audience parameter used with the token restriction. **Copy this value into the AcsScope appSetting value in the App.config of the sample application.**
  3. Token Format -> Pick SWT from the drop down.

1. Leave the rest of the fields at their default value and click Save to create the Relying Party Application.
2. Next click on “Rule groups” from the left menu. Then click the default rule group associated with the relying party application you just created. The name will start with “Default Rule Group for “ and end with the name you picked in 6a.
3. Click the Generate button above Rules.
4. Click Save to ensure that the token will have the nameidentifier claim in it. Otherwise you will get an error when trying to get a token from ACS about no output claims being generated.
5. Next click on “Certificates and Keys” from the left menu. Then click the add link above the Token Signing area. You will need to fill in the following pieces of data:
   1. Relying Party Application: make sure the name you used in 6a is selected.
   2. Type -> Choose Symmetric Key from the Drop Down
   3. Key -> Click the Generate button to generate a key. **Copy this value into the AcsSigningKey appSetting value in the App.config of the sample application.**
6. Leave the rest of the fields at their default values and click Save to create the symmetric token signing key.
7. Finally click on “Service Identities” from the left menu. Then click add. You will need to fill in the following pieces of data:
   1. Name -> this is the AcsAccountName used to authenticate the user to the ACS service to get a token. **Copy this value into AcsAccountName appSetting value in the App.config of the sample application.**
   2. Type -> from the drop down either pick Symmetric Key or password. If you pick password, fill in the Password field with a password. If you pick Symmetric Key, then click the Generate button to generate a password. **Whichever is used, copy this value into AcsAccountKey appSetting value in the App.config of the sample application.**
8. Click Save to store the new Service Identity. Note that this creates the credentials your test user users to authenticate to ACS with in order to get a token.