



4. Add the and sections to the section.

5. Modify the section under the section, to match the following example.

- The *claimType* property should be the unique identifier of the user in Azure AD, and it should match a value in the *authenticationType* property in Cora Sequence., you can also use <https://schemas.microsoft.com/identity/claims/objectidentifier>.
- Make sure you configure the *originalIssuer* with the Tenant ID. For more information about Tenant IDs, see <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-token-and-claims>.
- If you experience any issues, see the Troubleshooting section in this article.

6. In the section, modify the following configurations in the section. Make sure you add the section under the section.

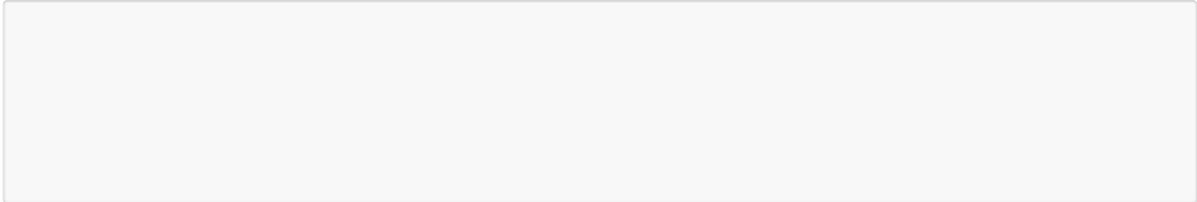
Configuration Attribute	Description
<i>ssoEnabled</i>	Specifies whether the application should configure the federation services to use the specified AD settings.
<i>tenantId</i>	Azure AD Tenant ID.
<i>wtRealm</i>	The application's App ID URI, which you can find in the properties section of the application you registered in Azure AD.

```
azureActiveDirectoryInstance="https://login.windows.net" />
```

7. Make sure that you configure the modules for the section under `web.config`. Add the following section to the `web.config` file.

8. Add the following to the `web.config`.

9. Add the following under the section.



10. For Flowtime and Process<sup>TOGO</sup> services, set the parameter to **None**.



11. In the Flowtime config file, in this section, change the *clientCredentialType* to **None**.

```
clientCredentialType="None" />
```

### Troubleshooting

If you experience an issue with denied access, set the diagnostic tool to information. You can view the full claim there, and retrieve all of the correct values.

```
initializeData="Information" />
```