Configure Cora SeQuence Single Sign-on for Use with Azure Active Directory

Last Modified on 01/30/2018 5:41 am EST

v8.3 and later

Overview

To authenticate users in Cora SeQuence using claims, you need to modify the `web.config` file for each Cora SeQuence component, and IIS.

Prerequisites

- Copy the `PNMsoft.Sequence.AzureService.dll` file from the GAC to the admin bin folder (the folder where you installed the Cora SeQuence Administration site).
- You must configure all Cora SeQuence sites under HTTPS. For more information, see Configure HTTPS for Cora SeQuence Sites.
- Make sure that the application URL matches the Reply URL in the Azure AD application.
- Verify that you added and configured each Cora SeQuence site in the Azure AD portal. For more information, see Set Required Permissions for Azure AD to Integrate with Cora SeQuence Sites.

Procedure

1. In IIS, configure the root level authentication for each Cora SeQuence site.

Setting	Value
Anonymous Authentication	Enabled
ASP.NET Impersonation	Enabled
Windows Authentication	Disabled

2. In IIS, for the Default Document, add the `Default.aspx` file for each Cora SeQuence site. Set the `Default.aspx` file as the first document, if there are other documents.
3. Add the following under the section group declaration

```
            .
            .
            .

            .
            .
            .

0a1a1b90c1c5dca1" />

            .
            .
            .

  .
  .
  .
```

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
ssoEnabled	Specifies whether the application should configure the federation services to use the specified AD settings.
tenantId	Azure AD Tenant ID.
wtRealm	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 . 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[TOGO] services, set the parameter to **None**.

11. In the Flowtime config file, in the 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" />
```