Configure Claims-Based Authentication

Last Modified on 07/24/2023 11:35 am EDT

v8.3 and later

Overview

To authenticate users in Cora SeQuence using claims-based authentication, you need to modify the `web.config` file for each Cora SeQuence site (Windows Services are not required). There are two procedures to perform.

- IIS
- web.config file

Prerequisites

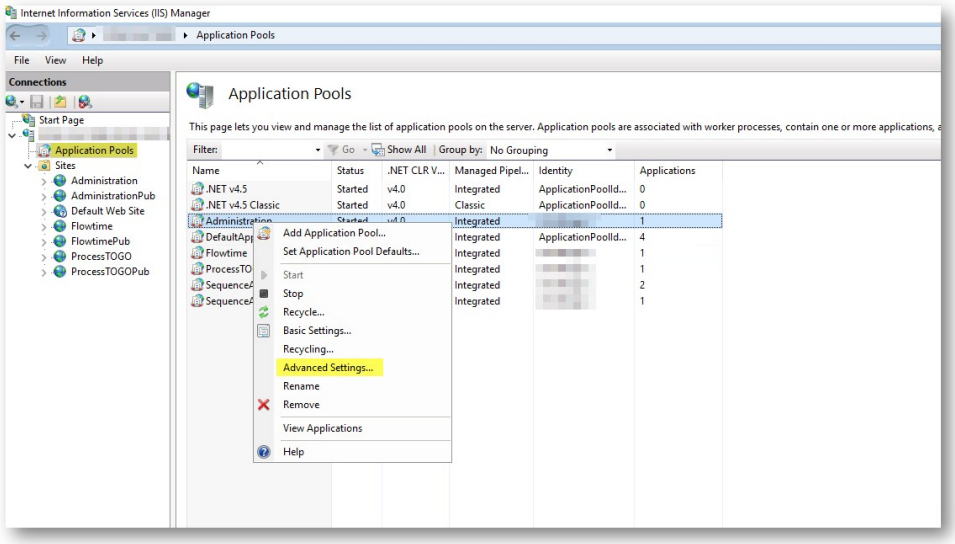
- You must configure all Cora SeQuence sites under HTTPS. For more information, see Configure HTTPS for Sequence Sites.
- Verify that your security token service (STS) supports SAML 2.0, and has a WS-Federation Endpoint.

IIS Procedure

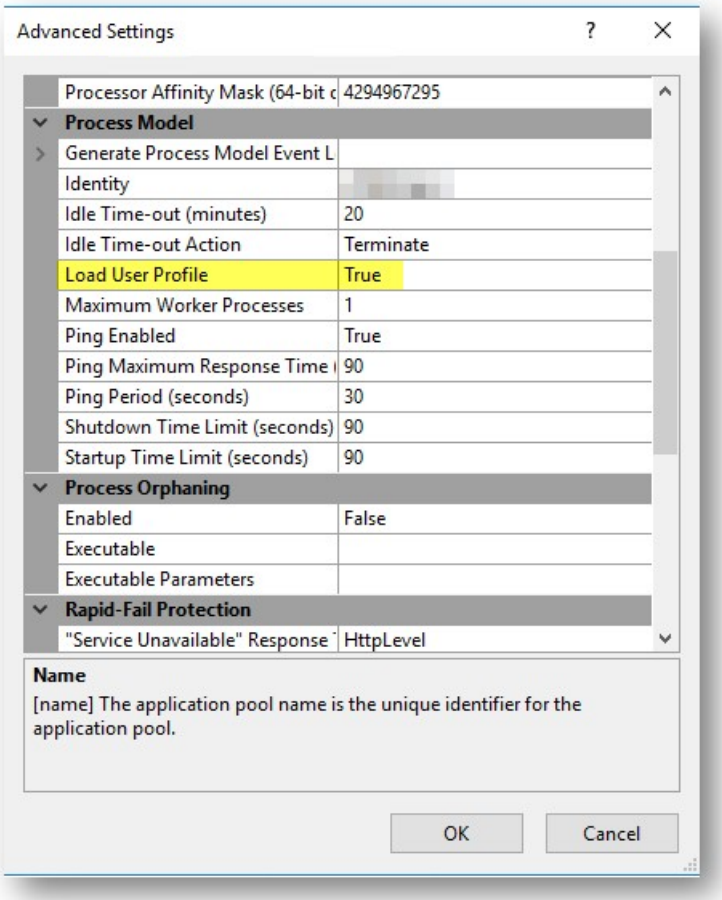
1. Configure the root level authentication for each Cora SeQuence site.

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

2. For the Default Document, add the `Default.aspx` file for each Cora SeQuence site. The `Default.aspx` file must be the only document.
3. In the Connections panel, select **Application Pools**.
4. Right-click the application pool used by your application and select **Advanced Settings**.



5. In the Process Model section, set the **Load User Profile** attribute to **True**.



web.config File Procedure

1. Add the `system.identityModel` and `system.identityModel.services` section declarations to the `<configSections>` section.

```
<section name="system.identityModel" type="System.IdentityModel.Configuration.SystemIdentityModelSecti
on, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089"/>
<section name="system.identityModel.services" type="System.IdentityModel.Services.Configuration.SystemI
dentityModelServicesSection, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyTok
en=B77A5C561934E089"/>
```

2. Replace the `<authentication>` section under the `<sequence.engine>` section, with the code sample in this step.
    a. For *claimType*, use one of the claim types provided by your STS, which you can match with one of the following Cora SeQuence employees table.
        i. Domain/User Name
        ii. User Name
        iii. Email
    b. For *authenticationType*, use one of the following (depending on your selection from the previous sub-step.
        i.
        ii.
        iii.
    c. Enter a unique name for the *originalIssuer* attribute.

```
<authentication impersonate="false">
  <providers>
    <add type="PNMsoft.Sequence.Security.ClaimsIdentityAuthenticationProvider, PNMsoft.Sequence.Ide
ntityModel.v8, Version=8.0.0.0, Culture=neutral, PublicKeyToken=0a1a1b90c1c5dca1" />
  </providers>
  <claims enabled="true">
    <IdentityClaims>
      <add claimType="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
originalIssuer="https://sts.windows.net/yourTenantID/" authenticationType="" />
    </IdentityClaims>
  </claims>
</authentication>
```

3. Make sure that you configure the modules for the `<system.identityModel>` section under the main `<system.webServer>` `<modules>`.

```
<add name="SessionAuthenticationModule" type="System.IdentityModel.Services.SessionAuthenticationMod
ule, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
preCondition="managedHandler" />
<add name="WSFederationAuthenticationModule" type="System.IdentityModel.Services.WSFederationAuthe
nticationModule, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5
61934e089" preCondition="managedHandler" />
```

4. Add the following under the main `<configuration>` node.

```
<location path="Authentication/Federation">
      <system.web>
          <httpHandlers>
              <add verb="GET, POST" path="SignIn.axd" type="PNMsoft.Sequence.IdentityModel.Web.Feder
ationSignInHttpHandler, PNMsoft.Sequence.IdentityModel, Version=8.0.0.0, Culture=neutral, PublicKeyToken=
0a1a1b90c1c5dca1" />
          </httpHandlers>
      </system.web>
      <system.webServer>
          <handlers>
              <add name="Authentication" verb="GET, POST" path="Authenticate.axd" type="PNMsoft.Sequ
ence.Web.WSFederationAuthenticationHttpHandler, PNMsoft.Sequence.IdentityModel.v8, Version=8.0.0.0, Cul
ture=neutral, PublicKeyToken=0a1a1b90c1c5dca1" />
          </handlers>
      </system.webServer>
</location>
<location path="FederationMetadata">
      <system.web>
          <authorization>
              <allow users="*" />
          </authorization>
</system.web>
</location>
```

5. Add the following under the `<configuration>` `</configuration>` section.
   - For `<audienceUris><add value=>` use the URL of the Sequence site you are configuring.
   - For `<trustedIssuers><add...>` use the following information.
     - `<thumbprint>` is the thumbprint of your STS token signing certificate. Make sure there are no spaces, there are no coding errors, and that it is plain text.
     - `<name>` is the value you used for `<originalIssuer>` in step 4c.
   - For `<federationConfiguration><wsFederation>`, use the following information.
     - `<issuer>` is the sign-in URL of your STS (where users are directed to log in).
     - `<realm>` and `<reply>` is the URL of the Sequence site you are configuring.
6. Configure Administration and Flowtime, and the Process^{TOGO} identity issuer setup using the following

settings.

Administration and Flowtime

```
<system.identityModel>
 <identityConfiguration>
  <audienceUris>
        <add value="XXXXX" />
  </audienceUris>
  <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, System.I
dentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
         <trustedIssuers>
              <add thumbprint="XXXXX" name=" XXXXX " />
         </trustedIssuers>
  </issuerNameRegistry>
  <certificateValidation certificateValidationMode="None" />
 </identityConfiguration>
   </system.identityModel>
   <system.identityModel.services>
 <federationConfiguration>
  <cookieHandler requireSsl="true" />
  <wsFederation passiveRedirectEnabled="true" issuer="XXXXX" realm="XXXXX" reply=" XXXXX " requireHtt
ps="true" />
 </federationConfiguration>
</system.identityModel.services>
```

Process[TOGO]

```
<system.identityModel>
 <identityConfiguration>
  <audienceUris>
        <add value="XXXXX" />
  </audienceUris>
  <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, System.I
dentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">
         <trustedIssuers>
              <add thumbprint="XXXXX" name=" XXXXX " />
         </trustedIssuers>
  </issuerNameRegistry>
  <certificateValidation certificateValidationMode="None" />
 </identityConfiguration>
   </system.identityModel>
   <system.identityModel.services>
 <federationConfiguration>
  <cookieHandler requireSsl="true" name="SequenceSessionId" hideFromScript="false" />
  <wsFederation passiveRedirectEnabled="true" issuer="XXXXX" realm="XXXXX" reply=" XXXXX " requireHtt
ps="true" />
 </federationConfiguration>
</system.identityModel.services>
```

7. Under the `<system.web>` section, replace each of the following sections wherever they exist.

```
<authentication mode="None"/>
<identity impersonate="true" />
<authorization>
       <deny users="?" />
</authorization>
```