Manitou Single Sign-on - Manitou OAuth Setup

10/29/2025 10:33 am EDT

Web.config

OidcAuthority - This is the base website for the Open ID Connect integration of the Identity Provider. For Azure, it's https://login.microsoftonline.com/{tenant}/v2.0. The {tenant} can be found in your Azure application in the overview section. For Ping Identity it's https://auth.pingone.com/{id}/as. The whole URI can be found in your Ping Identity application in the configuration section as ISSUER. Both {tenant} and {id} are usually GUIDs.

OidcClientId - This is the client ID assigned to your application that was created in the IDP.

OidcClientSecret - This is the client secret assigned to your application that was created in the IDP.

OidcRedirectUri - This is the redirect URI you entered in your application that was created in the IDP. The redirect URI is where the IDP should redirect your browser after authentication has occurred. This would be like https://{webSite}/Manitou/Login?ws=1. Mine is https://dev-12.boldgroup.int/Manitou/Login?ws=1. This needs to be configured in your IDP application.

OidcUserIdTag - This is the property name that contains the user ID we use to create the Manitou user. It should uniquely identify the user. Mine is set to "preferred_username".

OidcNameTag - This is the property name that contains the user's name. Mine is set to "name".

OidcGroupTag - This is the property name that contains the user's groups. Mine is set to "groups".

OidcGroupMapping - This is what defines which groups are Manitou groups. It is '=' delimited '|' delimited values that map group IDs to Manitou Group names. Mine is set to "7df87dcc-3e4c-4d8b-9822-7d3268db967c=Data Entry|b3b6db15-3c29-43fb-bf01-72b58478174b=Admin|c7cf3e9c-637c-47ba-bc7c-15bf0ccb4ee3=Supervisor|f88fffbe-b462-4512-b743-0f8473b91c45=Operator". This maps group ID "7df87dcc-3e4c-4d8b-9822-7d3268db967c" to Manitou Group "Data Entry", group ID "b3b6db15-3c29-43fb-bf01-72b58478174b" to Manitou Group "Admin" and so forth. The order in that you enter is important and is honored. If an operator is associated with multiple groups in the list, Manitou will use the one it finds first in the list. The IDP should be setup to send group IDs instead of group names. However, you could have it send group names and still map the group names to Manitou Groups. Azure doesn't support sending group names so for Azure, you have to send group IDs.

Troubleshooting

On the web.config, there is a section that is commented out:

```
<!--<system.diagnostics>
  <trace autoflush="true" indentsize="4">
    <listeners>
      <add name="myListener"
        type="System.Diagnostics.TextWriterTraceListener"
        initializeData="OAuthTextWriterOutput.log" />
      <remove name="Default" />
    </listeners>
  </trace>
</system.diagnostics>-->
```

If you uncomment this and save it, then you will get log information in the file "OAuthTextWriterOutput.log" in the directory where OAuth is hosted in IIS. This will help you find the names of variables and help you set your OIDC "Tag" variables properly.

NOTE: If you uncomment this, then it should be commented back out when you are done, and delete the log file, as it contains personal information.