Set up SSO between Azure AD and Oracle Identity Cloud Service for PeopleSoft

Technologies: IAM
Service Categories: Multicloud, Networking
Released: Jan 10, 2020

Configure SSO

This section provides steps for configuring SSO for PeopleSoft applications and Azure AD.

Before You Begin

Before you begin to set up SSO between Azure AD and Oracle Identity Cloud Service:

- Make sure that an Oracle Identity Cloud Service tenancy is available.
- You should know how to install Oracle HTTP server and deploy the WebGate to the Oracle HTTP server instance directory.
- You should have access to Microsoft Azure and have privileges to install and configure applications.

Integrate Identity Cloud Service and PeopleSoft Using Oracle HTTP Server and OpenID Connect

You can integrate your application with Oracle Identity Cloud Service for authentication purposes through industry-standard protocols and layers, such as OpenID Connect and HTTP Server.

1. Create or use an existing virtual machine (VM) in Microsoft Azure.
2. Select a certified OS for Oracle HTTP Server 12.2.1.3 installation.
3. Select the appropriate networking components to enable Oracle HTTP Server to reach the PeopleSoft application tier. Follow the standard Azure methods and security best practices for running a VM and application installations.
4. Install Oracle HTTP Server and create an Oracle HTTP Server instance. Follow Azure security best practices to open Oracle HTTP Server HTTP ports.
5. Apply the latest WebGate bundle patch and deploy the WebGate to the Oracle HTTP Server instance directory.
6. Register an application in Oracle Identity Cloud Service. Log in to the Oracle Identity Cloud Service console and create a trusted application. For example, you can name the application as **Webgate-App**.
7. Go to the **Configuration** tab to configure the application as a client. Note down the **Client ID** and **Client Secret** values so that you can use these values while configuring the WebGate.
   a. In **Client Configuration**, enter the following values:
      - Redirect URL:
        `https://<host:port>/oauth/callback`. This value should match the value in the WebGate `cloud.config` file for the **`callbackPrefix`** parameter.
      - Logout URL:
        `https://<host:port>/test/oauth/logout`. This is the URL configured for the authentication method **`oauth+logout`** in the WebGate `config.policy` file.
      - Post Logout URL:
        Oracle HTTP Server URL to the PeopleSoft home page
   b. Navigate to **Resources** and configure the application as a resource server by selecting **Register Resource**. For **Secondary Audiences**, enter `host:port` of the Oracle HTTP Server instance where WebGate is configured (or, in a high availability setup, enter the load balancer URL).
   c. Save to activate the application.

Configure WebGate to Interact With Oracle Identity Cloud Service for PeopleSoft

Configure WebGate to interact with Oracle Identity Cloud Service using the the `cloud.policy` file in the WebGate folder.

You can refer to the following sample `cloud.policy` file for protecting PeopleSoft applications with a single WebGate.

Copy

```
{
 "cloudgatePolicy":
{
 "comment" : "Sample Cloud Policy file to protect the application with the same WebGate",
 "disableAuthorize" : false,
 "webtierPolicy" :
 [
 {
  "policyName" : "default",
  "resourceFilters" : [
   {
    "comment" : "Test Application OAuth+Logout Filter",
    "type" : "text",
    "filter" : "/test/oauth/logout",
    "method" : "oauth+logout"
   },
  {
   "comment" : "PeopleSoft",
   "type" : "regex",
   "filter" : "/psc/.*",
   "method" : "oauth",
   "authorize" : true,
   "scope" : "",
   "idcsscope" : "",
   "headers" : [{"test_header" : "$subject.user.name"}]
  },
  {
   "comment" : "PeopleSoft",
   "type" : "regex",
   "filter" : "/psp/.*",
   "method" : "oauth",
   "authorize" : true,
   "scope" : "",
   "idcsscope" : "",
   "headers" : [{"header2" : "$subject.user.name"}]
  },
  {
   "comment" : "PeopleSoft",
   "type" : "regex",
   "filter" : "/ps/.*",
   "method" : "oauth",
   "authorize" : true,
   "scope" : "",
   "idcsscope" : "",
   "headers" : [{"test_header" : "$subject.user.name"}]
  },
  {
   "comment" : "PeopleSoft",
   "type" : "regex",
   "filter" : "/cs/.*",
   "method" : "oauth",
   "authorize" : true,
   "scope" : "",
   "idcsscope" : "",
   "headers" : [{"test_header" : "$subject.user.name"}]
  },
  {
   "comment" : "Test Application OAuth Filter",
   "type" : "regex",
   "filter" : "/cgi-bin/.*",
   "method" : "oauth",
   "authorize" : true,
   "scope" : "",
   "idcsscope" : "",
   "headers" : [{"test_header" : "$subject.user.name"}]
  }
 ]
}
]
}
}
```

Set User Headers for PeopleSoft

By default, the header value `OAM_REMOTE_USER` is set by the WebGate to the Oracle Identity Cloud Service username. The WebGate doesn't support fetching the Oracle Identity Cloud Service username and setting it as a custom header in `cloud.policy` file. If an application can use `OAM_REMOTE_USER`, then no additional changes are required.

PeopleSoft can be configured to consume the `OAM_REMOTE_USER` header set by the WebGate.

If you want to set a different header, for example PSUSER, add the following line to the Oracle HTTP Server instance `httpd.conf` file:

Copy

```
RequestHeader set PSUSER "%{OAM_REMOTE_USER}e"
```

Save the file and then restart the Oracle HTTP Server instance.