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

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

Learn About Setting up SSO between Azure AD and Oracle Identity Cloud Service

When you move your PeopleSoft application to the cloud and provide access to the application through Microsoft Azure, then users have to sign in to Azure portal and also re-enter credentials to sign in to PeopleSoft applications.

Federated SSO makes the integration seamless and allows the users to authenticate only once to access multiple applications, without signing in separately to access each application.

Identity federation helps enterprises reduce cost, because user accounts don't need to be created and managed separately in each identity management system. The user-synchronization process ensures that identities are propagated to all the federated systems.

Before You Begin

Before you begin to run an application in Microsoft Azure connected to a database in Oracle Cloud, understand the networking architecture for connecting workloads deployed on Oracle Cloud and Microsoft Azure.

See *Learn about interconnecting Oracle Cloud with Microsoft Azure*.

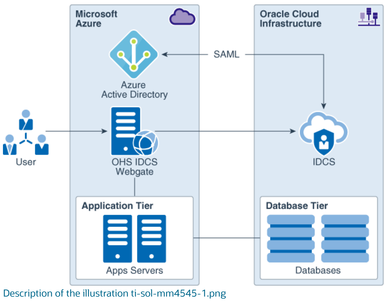
Architecture

This architecture diagram covers a pattern for setting up SSO with Oracle applications like PeopleSoft in which Oracle Identity Cloud Service acts as a bridge between the applications and Azure AD. This setup enables scenarios in which users can host Oracle Database in Oracle Cloud Infrastructure while using Azure AD as their identity provider.

In the diagram, the PeopleSoft application tier is in Azure and the database tier is in Oracle Cloud Infrastructure. Oracle HTTP Server (OHS) acts as a reverse proxy to the application tier, which means that all the requests to the end applications go through Oracle HTTP Server. Oracle Access Manager WebGate is an Oracle HTTP web server plugin that intercepts every request going to the end application and ensures that the user is logged in and authorized to access the application. Oracle Identity Cloud Service handles authentication for PeopleSoft. If a resource being accessed is protected (requires an authenticated session), the WebGate initiates OpenID Connect authentication flow with Oracle Identity Cloud Service through the user's browser.

Oracle Identity Cloud Service redirects users to Azure AD for authentication by using the SAML 2.0 protocol. Azure AD performs the authentication, and if it is successful, the user is redirected to the end application through Oracle Identity Cloud Service.

When you deploy PeopleSoft on Microsoft Azure, Oracle recommends that you deploy WebGate as a web-tier interface for the application servers. Configure appropriate security controls for traffic flow and ensure that only HTTP traffic from WebGate is accepted by PeopleSoft.

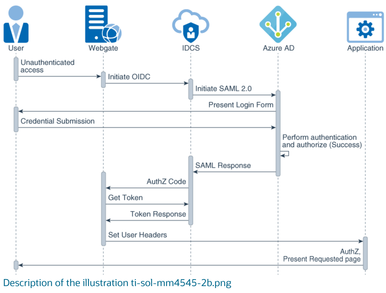


Description of the illustration ti-sol-mm4545-1.png

Authentication Flow

The WebGate is deployed on the same network infrastructure as Oracle's PeopleSoft. These two components must have network visibility into one another.

The following diagram shows the end user authentication flow when an application protected with WebGate and Oracle Identity Cloud Service is accessed.



Description of the illustration ti-sol-mm4545-2b.png

The architecture can be scaled out for high availability (HA) and failover by adding multiple Oracle HTTP Server hosts in front of an application and having a load balancer. To scale out an application deployment, follow the Azure HA and failover guidelines.

The following steps explain the authentication flow between the different components:

1. In a web browser, a user requests access to PeopleSoft through WebGate.
2. WebGate intercepts the request, verifies if the user hasn't signed in previously, and then redirects the browser to Oracle Identity Cloud Service.
3. Upon successful authentication, Oracle Identity Cloud Service issues a Security Assertion Markup Language (SAML) Request to initiate authentication by Azure AD.
4. Azure AD presents the sign-in page.
5. The user provides the credentials needed to sign in to the application.
6. Azure AD verifies authorization and generates the SAML token, and sends it to Oracle Identity Cloud Service.
7. Oracle Identity Cloud Service identifies the user and issues authorization token to WebGate via a browser. WebGate gets this token via a server-server call.
8. WebGate validates the token, adds header variables in the request and forwards the request to PeopleSoft.
9. PeopleSoft receives the header variables, identifies the user, and starts the PeopleSoft user session.

About Required Services, Products and Roles

An Oracle Identity Cloud Service administrator must be able to access the Oracle Identity Cloud Service console to configure and activate applications.

You must have access to the following services and products:

- Oracle Identity Cloud Service
- Oracle Cloud Infrastructure
- A fully functional Oracle's PeopleSoft instance deployed on Microsoft Azure
- Microsoft Azure

These are the roles needed for each service.

Service Name: Role	Required to...
Server administrator	Configure PeopleSoft and change security settings
Identity domain administrator: Security administrator	Register an application
Azure contributor or greater privileged account	Get Azure subscription
Application administrator or Global administrator	Handle configuration and set up on the Azure side

See *Learn how to get Oracle Cloud services for Oracle Solutions* to get the cloud services you need.

Previous Page
Next Page