Opower Customer Service Interface Single Sign-On Configuration Guide

You can use this documentation to implement Single Sign-On (SSO) with the Oracle Utilities Opower Customer Service Interface (CSI). With SSO, Customer Service Representatives (CSRs) can log into their utility CSR application with their existing utility user name and password, and then navigate to the CSI without creating an additional account or going through a separate authentication process. If CSRs attempt to access the CSI and are not already logged into it, they will be automatically directed to the utility site to sign in and returned to the CSI page they were trying to view.

General Requirements

Implementing SSO requires the use of standards-based communication between a federation server managed by the utility and one managed by Oracle Utilities. Oracle Utilities supports Security Assertion Markup Language (SAML) 2.0 to implement SSO with clients. If new versions are announced, Oracle Utilities will work to incorporate support for the last SAML versions in our product offering.

A utility's Oracle Cloud Infrastructure Identity and Access Management (IAM) environment acts as the Service Provider (SP) and the utility acts as the Identity Provider (IdP). This means that CSRs will log in on the utility application using their user name and password for the utility CSR application. They can then access the CSI without having to log in again.This table lists the utility requirements and limitations:

Supported SSO Profiles

Oracle Utilities requires Service Provider (SP)-initiated SSO. SP-initiated SSO allows users to bookmark pages. Also, if an Oracle Utilities session expires while a user still has a window open, SP-initiated SSO allows them to log in again and automatically return to the resource they are using. Performing SP-initiated SSO requires that the utility have a functional SSO URL that Oracle Utilities can access to begin the SSO process.

Oracle Utilities also supports Identity Provider (IdP)-initiated SSO. Clients must send Oracle Utilities a valid URL as a `RelayState` parameter. Oracle Utilities will provide the clients with appropriate URL for the CSI, which should be used as the default `RelayState`Parameter. Clients may also create links that take users to specific pages on the CSI by passing these URLs in the SAML `RelayState` parameter.

Whether a user attempts to access the CSI using IdP- or SP-initiated SSO, clients must ensure that their federation server only authenticates users that have permission to access the CSI. Oracle Utilities does not perform additional validation.

SAML Bindings - Identity Provider to Service Provider Binding

Oracle Utilities accepts SAML assertions from Identity Providers using the HTTP POST Binding method. This means all SAML assertions are sent as HTTP POST requests to the Oracle Utilities federation server. Oracle Utilities requires using HTTP POST and having the browser transmit the SAML assertion to the Oracle Utilities federation server. For this reason, Oracle Utilities does not support Artifact Binding for SAML 2.0.

SAML Bindings - Service Provider to Identity Provider Binding

Oracle Utilities supports either HTTP Redirect Binding or HTTP POST Binding when sending authentication requests to the Identity Provider. By default, Oracle Utilities will use HTTP Redirect Binding. This means that when Oracle Utilities begins the SP-initiated SSO process, Oracle Utilities will issue an HTTP Redirect to the user's browser directing them to the Identity Provider. The Identity Provider federation service will then receive an HTTP GET request from the consumer and initiate the authorization process. For similar reasons as above, Oracle Utilities does not support Artifact Binding on communication from Oracle Utilities to the Identity Provider.

SAML Assertion Requirements

Relay State

Identity Providers must send Oracle Utilities a `RelayState` parameter in the SAML Assertion sent to Oracle Utilities. In IdP-initiated SSO, clients can set up links that will take CSRs directly to any page they wish by sending the appropriate URL in the `RelayState`. Oracle Utilities will provide clients with the CSI URL to be used as a default `RelayState` parameter. The "Customer Service" page is an appropriate general page to send CSRs to once they log in. Clients must provide this "Customer Service" page URL or another valid URL as the `RelayState` URL when using IdP-initiated SSO.

In SP-initiated SSO, if Oracle Utilities sends a `RelayState` parameter to the Identity Provider, the Identity Provider must send the `RelayState` parameter back to Oracle Utilities without any modifications, as stated in the SAML 2.0 specification. When Oracle Utilities sends a `RelayState` parameter in SP-initiated SSO, it will be an alpha-numeric token that refers to saved state information on the Oracle Utilities federation server, and the `RelayState` will not be a URL.

SAML Data Elements - SAML Subject

The SAML Subject must contain a user identifier. Oracle Utilities will describe the exact value required for this field based on the implementation plan. Common user identifiers include CSR email IDs, employee IDs, or unique user names.

Security

Security for SAML is done through several mechanisms. First, SAML assertions sent using POST Binding from the Identity Provider must be digitally signed with the Identity Provider's private key using an XML signature. This is a requirement per the SAML specifications. Oracle Utilities will then verify the source with a corresponding public key. Assertions that fail this verification process will be rejected. This mechanism ensures that only assertions originating from the proper utility client are accepted. Furthermore, data is encrypted via HTTPS during transfer. In addition, the RelayState parameter does not include a full URL when it is passed from Oracle Utilities to the client and then back. Rather, it is a reference to the desired URL, which is stored on the Oracle Utilities federation server. This prevents unauthorized parties from tampering with the destination URL during transit.

Logout

Oracle Utilities does not currently support SAML Single Log Out. However, Oracle Utilities can redirect the CSR to a specific page after they click **Log Out** on the CSI.

SAML Configuration Information

When implementing SSO, most clients choose to contract with a federation server provider and configure settings through the provider's interface. Configuration details are provided below.

Oracle Utilities SAML Information

Oracle Utilities provides the utility with SAML metadata for production and staging servers. The metadata provided by Oracle Utilities includes the following information:

- Oracle Utilities SAML Entity ID
- Oracle Utilities Assertion Consumer Service URL
- Default Target URL (RelayState Value)

Information Required by Oracle Utilities from Utility

Oracle Utilities requires that a Utility defines their SAML specification or extracts a SAML metadata definition, and provides either resource to Oracle Utilities. Refer to your IdP third-party documentation for steps on completing a SAML metadata extraction. The information in the specification or metadata file must include the following:

- **Client SAML Entity ID**: This is the same concept as the Oracle Utilities entity ID.
- **Client Public Key**: Oracle Utilities requires the Public Key for the corresponding Private Key the utility is using to sign their SAML Assertions. SAML requires the Identity Provider to sign all Assertions submitted via POST with a Private Key. Oracle Utilities need the Public keys to verify the Assertions were sent by the utility client.
- **SAML Single Sign On Service URL**: Required for SP-initiated SSO. SP-initiated SSO is where the user visits the URL for the CSI before logging in at the client utility site. Oracle Utilities needs to redirect users to the utility to begin the sign in process and afterwards they will be returned to the URL on the CSI that they were

trying to access. This is done by sending SAML Messages to the partner's federation server to begin a user's SSO process. This value is the URL Oracle Utilities will use to begin SP-initiated SSO. Oracle Utilities uses Redirect Binding to access this URL.

- **Logout Redirect URL**: This is an optional parameter. It is the URL Oracle Utilities will redirect the user to after they click the **Log Out** link or make requests to the Oracle Utilities Logout URL.

Testing Procedures

SSO implementations are thoroughly tested by the client and Oracle Utilities before going live. Oracle Utilities has separate instances of our CSI specifically for integration testing. This is known as our "Staging Environment." Before going live with a client, the staging infrastructure is configured to accept SAML Assertions from the corresponding utility testing environment. The utility application and Federation server must similarly be configured to send SAML Assertions to the Oracle Utilities Federation server. Testers would then verify that users are able to successfully use SAML SSO to access the CSI. Once testing is complete, the configurations would be migrated to the production applications for both Oracle Utilities and the utility.
