For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.
Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td>1</td>
</tr>
<tr>
<td>General Requirements</td>
<td>1</td>
</tr>
<tr>
<td>Oracle Identity Cloud Service Integration and Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Utility Configuration Checklist</td>
<td>3</td>
</tr>
<tr>
<td>Oracle Identity Cloud Service User Experience</td>
<td>3</td>
</tr>
<tr>
<td>Oracle Identity Cloud Service Product Configuration Steps</td>
<td>10</td>
</tr>
<tr>
<td>Oracle Identity Cloud Service Testing Procedure</td>
<td>20</td>
</tr>
<tr>
<td>SAML Single Sign-On (SSO) Configuration</td>
<td>23</td>
</tr>
<tr>
<td>Utility Configuration Checklist</td>
<td>23</td>
</tr>
<tr>
<td>Supported SAML Single Sign-On Profiles</td>
<td>23</td>
</tr>
<tr>
<td>SAML Single Sign-On Assertion Requirements</td>
<td>25</td>
</tr>
<tr>
<td>Single Sign-On User Experience</td>
<td>27</td>
</tr>
<tr>
<td>SAML Single Sign-On Configuration Information</td>
<td>27</td>
</tr>
<tr>
<td>SAML Testing Procedures</td>
<td>28</td>
</tr>
<tr>
<td>Contacting Your Delivery Team</td>
<td>31</td>
</tr>
</tbody>
</table>
Getting Started

Authentication ensures that an individual is recognized and granted an appropriate level of access to Digital Self Service - Transactions.

General Requirements

Oracle Utilities supports the following:

- Single Sign-On (SSO) via OAuth if integrating with Oracle Identity Cloud Service.
- Security Assertion Markup Language (SAML) 2.0 if using another identity provider to implement SSO with utilities.

SSO makes it easier for customers to access their account online by allowing them to use one username and password to access any application integrated with an identity management service (IMS) without creating an additional account. With SSO, if customers attempt to access Digital Self Service - Transactions and are not currently logged into an integrated application, they are automatically directed to the IMS to sign in and are then returned to the content they were trying to view.
Oracle Identity Cloud Service Integration and Configuration

The mapping of web user IDs for Oracle Utilities Customer to Meter or Oracle Utilities Customer Care and Billing accounts is maintained by the Digital Self Service - Transactions system. The OAuth assertion only authenticates a web user ID, group, and identifying information.

Utility Configuration Checklist

The following steps are required to set up and configure Oracle Identity Cloud Service for single or multiple account authentication to Digital Self Service - Transactions.

1. Set up two Oracle Identity Cloud Service instances: Stage and Production. Also set up authentication services for Stage and Production.
2. Provide Oracle with client ID and client secrets to connect to these instances.
3. Provide Oracle with test login accounts for end-to-end testing on these instances.

Oracle Identity Cloud Service User Experience

Digital Self Service – Transactions’ built-in integration with Oracle Identify Cloud Service includes features that allow customers to create an account, reset their password, and login with valid account credentials through the Digital Self Service - Transactions interface, as opposed to an external identity provider’s interface. Use the following information to review Oracle Identity Cloud Service configuration options.

Registration

Digital Self Service – Transactions allows customers to create a web account to access their utility portal online.

Customers must complete fields that are required by Oracle Identity Cloud Service, including:
- First name
- Last name
- Email address
- A password that meets the configured password requirements

![Registration Form](image_url)

<table>
<thead>
<tr>
<th>Image Number</th>
<th>Configuration Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Registration Widget Name</strong></td>
</tr>
<tr>
<td></td>
<td>The title for the registration widget.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Create your web account</td>
</tr>
<tr>
<td>2</td>
<td><strong>Sub header</strong></td>
</tr>
<tr>
<td></td>
<td>The supporting text for the registration widget.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> To manage your account online, you must create a web account.</td>
</tr>
<tr>
<td>Image Number</td>
<td>Configuration Option</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td><strong>Password Policy</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Standard</td>
</tr>
<tr>
<td>4</td>
<td><strong>Unique Email as Web Username</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Email</td>
</tr>
<tr>
<td>Not Pictured</td>
<td>Resend Verification Email</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Pictured</td>
<td>Resend Verification Email Success</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Email verification has been resent. Please check your inbox.</td>
</tr>
</tbody>
</table>
Login

The login to Digital Self Service – Transactions requires a registered email address and password. Customers may also access a link to sign up for an account or a link to reset their password so they may complete these processes online.

<table>
<thead>
<tr>
<th>Image Number</th>
<th>Configuration Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login ID</td>
</tr>
<tr>
<td></td>
<td>Customers can log in using a unique email address or username.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Email</td>
</tr>
<tr>
<td>2</td>
<td>Account Recovery Link</td>
</tr>
<tr>
<td></td>
<td>A link to allow the customer to reset their own password.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> The &quot;Can't access your account?&quot; link directs users to the account recovery widget.</td>
</tr>
<tr>
<td>3</td>
<td>Sign Up Link</td>
</tr>
<tr>
<td>Image Number</td>
<td>Configuration Option</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
|              | A link to allow the customer to sign up for a web account if they don't have an existing login.  
**Default:** Links to Registration Widget |
| Not Pictured | Redirect URL  
The destination after login.  
**Default:** Account Overview |

**Account Recovery**

An Account Recovery widget helps Digital Self Service – Transactions customers regain access to their account. A valid email address or username must be provided for the customer to receive the password recovery email. If the customer has forgotten their registered email address, or has multiple usernames associated with the same email address, they must contact customer service to regain access to their account.

![Can’t access your account?](image)
### Image Number

<table>
<thead>
<tr>
<th>Image Number</th>
<th>Configuration Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login ID</td>
</tr>
<tr>
<td></td>
<td>Customers can trigger a password reset notification based on their email address or username.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Email</td>
</tr>
<tr>
<td>Not Pictured</td>
<td>Destination URL</td>
</tr>
<tr>
<td></td>
<td>The destination after login.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> /dss/overview</td>
</tr>
</tbody>
</table>

### Edit Password

Customers can select to **Manage Web Account** to manage their web account. From the Web Login Details, customers can select the **Edit** password option to change their password directly within Digital Self Service - Transactions.

![Web login details](image)

### Notifications

Integration with Oracle Identity Cloud Service leverages email notifications at key steps in the customer journey. For example, after a user is created manually or using self-
registration, they will receive a welcome email. When they activate their account, they
will then receive an activation email.

Supported User Notifications & Templates

Self-Registration Email Verification: After successfully creating an account, this
notification is sent to the user to verify the email address.

Welcome Self-Registration User: After successfully creating an account, this
notification is sent to the user. The notification contains a link that the user clicks to
activate the account.

Password Recovery Request: This notification is sent to a user if the user requests a
password reset. This notification contains a URL that the user clicks to be redirected to
the Password Reset page. The user provides a password as part of the password
recovery process. After the activation process is complete, the user is logged in
automatically.

Password Change: This notification is sent to the end user to inform the user that the
password is changed successfully. This event is initiated by the end user.

User Account Locked: An end user is notified that their account in Oracle Identity
Cloud Service is locked.
**User Account Unlocked**: An end user is notified that their account in Oracle Identity Cloud Service is unlocked.

**User Exceeded the Maximum Number of Account Recovery Attempts**: After a user exceeds the maximum number of attempts to reset their password to recover their account, this notification is sent to the user’s primary email address.

**Resend Welcome**: This notification is sent when the user does not click the activate your account link in the Welcome notification. The notification contains a link that the end user clicks to activate the account.

**Oracle Identity Cloud Service Product Configuration Steps**

After reviewing all of the feature configuration options provided in the Oracle Identity Cloud Service User Experience section, you then complete the following configuration tasks using Oracle Identity Cloud Service.

**Note**: This documentation provides steps to complete these configuration tasks using Oracle Identity Cloud Service. Refer to your applicable product documentation for steps to complete the configuration using your version of Oracle Identity Cloud Service. Additionally, this documentation assumes that you have administrative access to Oracle Identity Cloud Service. For additional details on these tasks, refer to the applicable Oracle Identity Cloud Service Documentation.

Configuration tasks include:

1. Application configuration
2. Create groups
3. Assign the application to your groups
4. Create users
5. Create a self-registration profile
6. Update password policy
7. Customize branding
8. Customize email templates
9. Create production Oracle Identity Cloud Service instance

Application Configuration

Within the context of the integration with Digital Self Service - Transactions, Oracle Identity Cloud Service acts as the Identity Provider (IDP). This means that Oracle Identity Cloud Service handles the full authentication process. It also supports different types of standard authentication solutions, including SAML and OAuth. The recommended integration approach with Digital Self Service - Transactions is OAuth.

Complete the following steps to configure Oracle Identity Cloud Service:

1. Navigate to the Oracle Identity Cloud Service Admin Console and select the Applications menu.

2. Add a new application and select Confidential Application from the list of applications.

3. Enter the following information in the new application wizard, and then click Next:
   - **Name**: For example, enter DSS-Test. You will need to provide this to your delivery team to complete the integration.
   - **Application URL**: This URL will be different for different Digital Self Service - Transactions clients and environments. For example, https://dss-utilityco-stage.opower.com

4. On the next page, select the Configure this application as a client now option and complete the following fields:
   - **Authorization**: Allowed Grant Types – enable Client Credentials and JWT Assertion
   - **Token Issuance Policy**: Grant the client access to Identity Cloud Service Admin APIs. Click Add and in the dialogue box, select the following:
     - **Me**
     - **Signin**
     - **Verify Email**
5. Click **Next**, and in the **Expose APIs to Other Applications** area, verify that **Skip for later** is selected.

6. Click **Next**, and under **Authorization**, verify that **Enforce Grants as Authorization** is not selected.

7. Click **Finish**, and make note of the Client ID and Client Secret that are generated. You will provide these to your delivery team to complete the integration.

8. After the application has been created in Oracle Identity Cloud Service, you activate the application. From the Admin Console, select **Applications** and then select **Activate** from the menu on the front of the application.

### Create Groups

Digital Self Service - Transactions requires different groups that grant different levels of access to Digital Self Service - Transactions. One group is used by utility customers (WSSUserGroup) and one group is used by utility staff for support and administration purposes (WSSCSRGroup).

WSSCSRGroup should be assigned to Customer Support Representatives who help customers answer questions about their accounts. See [Providing Customer Support](#) for additional information.

This table describes each group and their attributes:
<table>
<thead>
<tr>
<th>Group Name</th>
<th>Description</th>
<th>Users Can Request Access</th>
<th>Application Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSSUserGroup</td>
<td>Use this group for utility customers who have access to standard Digital Self Service - Transactions customer pages.</td>
<td>Yes</td>
<td>DSS Production</td>
</tr>
<tr>
<td>WSSCSRGroup</td>
<td>Use this group for utility customer service representatives who have access to a customer search and masquerading page.</td>
<td>No</td>
<td>DSS Production</td>
</tr>
</tbody>
</table>

To create the Digital Self Service - Transactions groups in Oracle Identity Cloud Service:

1. Navigate to the Oracle Identity Cloud Service Admin Console, and then select Groups.

2. Select Add and enter group information using the information in the table above for reference.

3. Create the remaining user groups following these steps. When you finish, you should see your new groups in the Oracle Identity Cloud Service Groups list.

Assign the Application to Groups

Assign the DSS-Production application to the groups you created. Assign the application by updating the group so that users within each group get proper access to Digital Self Service - Transactions.

To assign the application to a group:
1. Return to your Groups and then click the **Access** tab.

2. Click **Assign Applications**.

3. Search for your DSS application.

4. Click **Assign** and then click **OK** to save your changes.

**Create Users**

Once groups have been created, you may provision users and assign them to their respective group. Admin and CSR users will be manually created through the Oracle Identity Cloud Service Admin Console. External users can self-register for Digital Self Service - Transactions accounts. See [Create a Self-Registration Profile](#) for additional information.

You can create new users individually, or using a bulk import process.

**Creating Individual Users**

To create new users individually:

1. Log in to the Oracle Identity Cloud Service Admin Console, navigate to **Users** and select **Add**.

2. Enter the user’s personal information and click **Next**.

3. Assign the user to a specific group, such as WSSAdminGroup or WSSCSRGroup.

4. Click **Finish**.

**Bulk Importing Users**

You may also import multiple users using the bulk import process in Oracle Identity Cloud Service. To import users in bulk, download the import template from **Users -> Import -> Download sample file**. Then update the sample csv file with user information. When finished, you then import the file into Oracle Identity Cloud Service.

Users’ existing passwords can be retained from the source system if they are included hashed in the user import.

This table outlines the user attributes that Oracle Identity Cloud Service will pass to Digital Self Service - Transactions:
<table>
<thead>
<tr>
<th>Name</th>
<th>Format</th>
<th>Type</th>
<th>Value</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>Basic</td>
<td>User Attribute</td>
<td>Group Membership</td>
<td>All Groups</td>
</tr>
<tr>
<td>firstName</td>
<td>Basic</td>
<td>User Attribute</td>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>lastName</td>
<td>Basic</td>
<td>User Attribute</td>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>email</td>
<td>Basic</td>
<td>User Attribute</td>
<td>Primary Email</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>Basic</td>
<td>User Attribute</td>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>userID</td>
<td>Basic</td>
<td>User Attribute</td>
<td>Assigned User ID</td>
<td></td>
</tr>
</tbody>
</table>

Create a Self-Registration Profile

External utility customers can create their own web login to Digital Self Service - Transactions by completing the Self-Registration Profile. To enable this, you must create a self-registration page for users to enter their profile information.

This profile automatically assigns the user to the WSSUsersGroup. Once they have activated their account by validating their email address, they can link their web login with their utility account through the Digital Self Service - Transactions portal.

To create a self-registration page for external users:

1. Navigate to the Oracle Identity Cloud Service Admin Console. Select Settings, then select Self Registration, and then add a new profile.

2. Specify the following information, which are the only configurations supported by Digital Self Service:

   - **Profile Name**: DSS_Production_Self_Registration_Profile
   - **User Consent required**: No
- **Assign to Group**: WSSUserGroup
- **Allow Email Domains**: all

3. Select the self-registration profile, and then click the **Activate** option from the menu.

4. Make note of the profile ID that is generated. You will provide this to your delivery team to complete the integration.

After you create the self-registration profile, you can access it using the profile ID that was generated for the new profile.

The self-registration URL is as follows:

```
https://[idcs-instance]/ui/v1/signup?prifileid=[profile-id]
```

**Note**: Your customers will interact with the Digital Self Service - Transactions registration screen, not the Oracle Identity Cloud Service screen.

**Update the Password Policy**

You can change the password policy in Oracle Identity Cloud Service to suit your organization’s preferred password requirements. There are three types of password policies in Oracle Identity Cloud Service:

- Simple
- Standard
- Custom

To create a custom policy in Oracle Identity Cloud Service:

1. Navigate to the Oracle Identity Cloud Service Admin Console. From **Settings**, select **Password Policy** page.

2. Select **Change Your Password Policy**, and then choose **Custom password policy strength**.
3. Update the following password policy parameters:
   - Password length (min size)
   - Password length (max size)
   - Password expiration
   - Account lock threshold
   - Enable/disable auto unlock account
   - Auto unlock account duration
   - Previous passwords remembered
   - The password must contain characters settings
   - The password must not contain attributes

Customize Branding

Oracle Identity Cloud Service branding customizations include the application logo, company name, contact email addresses, and notification email address.

To update Oracle Identity Cloud Service branding:

1. Log in to the Oracle Identity Cloud Service Admin console. Navigate to **Settings**, and then select **Default Settings**.

2. Update the **Contact Email Addresses**. For example, enter: customerservice@UtilityCo.com

3. From **Settings**, select **Notifications**, and then update the **From Email Address**. For example, enter no-reply@UtilCo.com

4. From **Settings**, select **Branding** and then choose **custom branding**.

5. Update the **Company name**. For example, enter: UtilityCo

6. Upload the **company logo**, which is used in the console and email templates header and footer.
Customize Email Templates

Integration with Oracle Identity Cloud Service leverages email notifications at key steps in a customer’s journey. For example, after a user completes the sign-up steps online, they receive an email verification notification. When they have verified their email and successfully created an account, they receive a Welcome email.

Supported User Notifications and Templates

**Note:** To avoid any unintended issues, Oracle recommends disabling all other end-user notifications in Oracle Identity Cloud Service.

**Self-Registration Email Verification:** After successfully creating an account, this notification is sent to the user to verify the email address.

**Welcome Self-Registration User:** After successfully creating an account, this notification is sent to the user. The notification contains a link that the user clicks to activate the account.

**Password Recovery Request:** This notification is sent to a user if the user requests a password reset. This notification contains a URL that the user clicks to be redirected to the Password Reset page. The user provides a password as part of the password recovery process. After the activation process is complete, the user is logged in automatically.

**Password Change:** This notification is sent to the end user to inform the user that the password is changed successfully. This event is initiated by the end user.

**User Account Locked:** An end user is notified that their account in Oracle Identity Cloud Service is locked.

**User Account Unlocked:** An end user is notified that their account in Oracle Identity Cloud Service is unlocked.

**User Exceeded the Maximum Number of Account Recovery Attempts:** After a user exceeds the maximum number of attempts to reset their password to recover their account, this notification is sent to the user’s primary email address.
Resend Welcome: This notification is sent when the user does not click the activate your account link in the Welcome notification. The notification contains a link that the end user clicks to activate the account.

To customize email templates:

1. Log in to the Oracle Identity Cloud Service Admin Console.
2. Navigate to Settings, then select Notifications, and then select the Email Templates tab.
3. Select the email template, and then update email subject and email body as needed.

By default, notifications will be sent from no-reply@oracle.com. The From Address can be customized to a utility email address; however, you must be able to verify the email address which will be used.

To modify the from email address:

1. Log in to the Oracle Identity Cloud Service Admin Console.
2. Navigate to Settings, then select Notifications, and then choose the Domain or Email option.
   a. Choosing Domain will send a validation email to the postmaster account of the email’s domain.
   b. Choosing Email will send a validation email to the email that you provide.

Create a Production Oracle Identity Cloud Service Instance

Two Oracle Identity Cloud Service instances are required for your Digital Self Service - Transactions integration. This separates users and configurations for production and non-production environments.

The first instance that is provisioned as part of your cloud tenancy is the Primary instance. This will be used as your pre-production environment. You must also provision a secondary instance for your production environment.

Before you can create your secondary instance, you must meet the following prerequisites:
- You must have the Identity instance creation cloud account role.
- Your secondary instance should be within the same data region as your primary instance.
- You should be familiar with the Oracle Identity Cloud Service pricing model. In this scenario, you will provision a Standard version of Oracle Identity Cloud Service.

To provision secondary instance, complete these steps:

1. Log in to the Oracle Identity Cloud Service Console. For example, [customer ID].oraclecloud.com/mycloud/cloudportal/gettingStarted
2. Select Create Instance from the Cloud dashboard and then select Identity Cloud Service.
3. Update following fields and then click Create:
   - **Name:** idcsprod
   - **License Type:** Oracle Identity Standard Cloud Service
   - **Initial Administrator Details:** enter IDCS instance administrator information (email, first name and last name)

### Oracle Identity Cloud Service Testing Procedure

Oracle Utilities follows thorough testing procedures for Oracle Identity Cloud Service implementations. Oracle Utilities has separate instances of Digital Self Service - Transactions and federation servers specifically for integration testing. This is known as our staging environment. This infrastructure is completely separate from the production Oracle Utilities infrastructure.

Before going live with a utility, the Oracle Utilities staging infrastructure is configured to accept OAuth responses from the corresponding utility testing environment. The client application and federation server must similarly be configured to complete an authentication handshake with the Oracle Utilities federation server.

In order to verify a successful connection and assist with troubleshooting, Oracle Utilities needs the ability to log in to the utility’s staging environment. Oracle Utilities also requires at least one valid login on the utility’s stage environment. For implementations where accounts are passed in via OAuth, account mappings must be created in the
utility's identity system with matching active accounts in the stage environments being used for testing.

After testing is complete, the configurations are migrated to the production applications for both Oracle Utilities and the utility. To verify these connections, Oracle Utilities also needs a test account on production.

The stage and production test accounts should be available for the life of the program for continuous verification of end-to-end authentication functionality.
SAML Single Sign-On (SSO) Configuration

The mapping of web user IDs for Oracle Utilities Customer to Meter or Oracle Utilities Customer Care and Billing accounts is maintained by the Digital Self Service - Transactions system. The SAML assertion only authenticates a web user ID, group, and identifying information.

To support SAML logout behavior for customers, the utility must provide Oracle with a logout URL. When a customer logs out of Digital Self Service - Transactions, they are redirected to the logout URL provided by the utility, which then redirects to a customer login page. This redirection occurs after the customer is logged out from the utility’s Identity Provider.

Utility Configuration Checklist

SSO relies on standards-based communication between a federation server managed by the utility and the server managed by Oracle Utilities. The following steps are required to set up and configure SSO for single or multiple account SSO.

1. Set up two SAML 2.0 Identity Provider federated servers: Stage and Production. Also set up authentication services for Stage and Production.

2. Provide Oracle Utilities with SAML metadata to connect to these servers.

3. Provide Oracle Utilities with test login accounts for end-to-end testing on these servers. If necessary, provide Oracle Utilities with VPN access to the Stage login page. If your test site is behind a firewall, be sure to whitelist the Oracle Utilities IP address. Contact your Delivery Team if you need a copy of the IP address.

Supported SAML Single Sign-On 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. Utilities may create links that take users to specific pages on Digital Self Service - Transactions by passing these URLs in the SAML RelayState parameter. Utilities must send Oracle Utilities a valid URL as a RelayState parameter. Oracle Utilities will provide utilities with the appropriate URL for Digital Self Service - Transactions, which should be used as the default RelayState parameter.

Whether user access attempts employ IdP-initiated or SP-initiated SSO, utilities must ensure that their federation server only authenticates users that have permission to access Digital Self Service - Transactions.

For further information on SAML SSO profiles, see the Security Assertion Markup Language (SAML) V2.0 Technical Overview.

SAML Bindings

Identity Provider to Service Provider Binding

Oracle Utilities accepts SAML assertions from IdPs using the HTTP POST binding method. This means that all SAML assertions are sent as HTTP POST requests to the Oracle Utilities federation server. The SAML specification also allows assertions to be sent using HTTP artifact binding, which requires direct server to server communication and is more complex to configure. Oracle Utilities recommends using HTTP POST and having the browser transmit the SAML assertion to the Oracle Utilities federation server. Oracle Utilities does not support artifact binding for SAML 2.0.

Service Provider to Identity Provider Binding

Oracle Utilities supports either HTTP redirect binding, or HTTP POST binding when sending authentication requests to the IdP. By default, Oracle Utilities uses HTTP redirect binding. This means that when Oracle Utilities begins the SP-initiated SSO process, Oracle Utilities issues 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. Oracle Utilities does not support artifact binding on communication from Oracle Utilities to the Identity Provider.
SAML Single Sign-On Assertion Requirements

The SAML assertion for an SSO implementation requires a RelayState parameter, as well as specific data elements and security information. Many of these requirements are the same for both single and multiple account SSO. The main differences are in the required data elements, which are identified in the following sections.

RelayState Parameter

Identity Providers must send Oracle Utilities a RelayState parameter in the SAML assertion sent to Oracle Utilities. In IdP-initiated SSO, utilities can set up links that will take users directly to a specific page by sending the appropriate URL in the RelayState. Oracle Utilities will provide utilities with our Dashboard URL to be used as a default RelayState parameter. The Dashboard is an appropriate general page to send customers to once they log in. Utilities must use this Dashboard 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

The required SAML data elements include the SAML subject and the SAML attribute. The elements of the SAML attributes can vary slightly depending on your implementation.

Warning: Ensure that carriage return characters are not included in SAML responses. Inclusion of carriage returns can cause errors such as signature mismatches.

SAML Subject

The SAML subject must contain an anonymous user identifier, such as a GUID, that is used for the login process. This identifier must not contain any personally identifiable
information (PII). Additionally, the user identifier must uniquely identify users in the identity management system and must remain static upon creation. In other words, modifications to the user identifier referenced in the SAML subject are not supported.

**SAML Attributes for All Account Types**

The following attributes are included for all account types.

- **groups:** This required attribute controls the user landing page for groups of users. The allowed values include:
  - **WSSUserGroup:** Use this group for utility customers who have access to standard Digital Self Service - Transactions customer pages.
  - **WSSCSRGroup:** Use this group for utility customer service representatives who have access to a customer search and masquerading page.

- **firstName:** This required attribute is the user’s first name, which can be displayed to the user, such as in welcome messages for a logged in user.

- **lastName:** This required attribute is the user’s last name, which can be displayed to the user, such as in welcome messages for a logged in user.

- **email:** This required attribute is the user’s email address.

- **username:** This required attribute is the user’s username, which is used to sign in to and access their account.

**Security Requirements**

Security for SAML is achieved 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 XML signature. This is a requirement per the SAML specifications. Oracle Utilities will then verify the source with the corresponding public key. Assertions that fail this verification process are 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 utility and then back, but it is a reference to the desired URL. This prevents unauthorized parties from tampering with the destination URL during transit.
Single Sign-On User Experience

The user experience can be customized when implementing SAML SSO by controlling how the utility website initiates SSO and how users are directed to the Oracle Utilities website.

Users can begin at the utility website. After users log in, they can be presented with links that take them to Digital Self Service - Transactions using SSO. These links can be customized to link to any page on Digital Self Service - Transactions.

**Note:** If the landing page is configured to be based on a user’s group role, (See "SAML Attributes for All Account Types" on page 26) the link to the main page for Digital Self Service - Transactions uses the syntax

http://[host]:
[port]/webcenter/portal/system/DSSLandingPage

where **host** and **port** are the applicable host IP address and port number for the portal.

SAML Single Sign-On Configuration Information

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

Oracle Utilities Opower SAML Information

**Production Information**

- **Oracle Utilities Opower SAML Entity ID:** sso.opower.com
- **Oracle Utilities Opower Assertion Consumer Service URL:**
  https://sso.opower.com/sp/ACS.saml2
- **Default Target URL (RelayState Value):** To be provided by Oracle Utilities.
Staging Information

- **Oracle Utilities Opower SAML Entity ID**: sso-stage.opower.com
- **Oracle Utilities Opower Assertion Consumer Service URL**: https://sso-stage.opower.com/sp/ACS.saml2
- **Default Target URL (RelayState Value)**: To be provided by Oracle Utilities.

Information Required by Oracle Utilities from the Utility

- **Utility SAML Entity ID**: The URL to the client IdP SAML endpoint, which is the client-side counterpart to the Oracle Utilities Opower entity ID.
- **Utility 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 needs the public keys to verify the assertions were sent by the utility.
- **SAML Single Sign-On Service URL**: Required for SP-initiated SSO, in which the user visits the URL for Digital Self Service - Transactions before logging in at the client utility website. 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 Digital Self Service - Transactions 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.
- **Logout Redirect URL**: The logout URL logs out of the utility’s IdP and redirects to the utility’s login page. Oracle Utilities redirects the user to after they click the logout link.

SAML Testing Procedures

Oracle Utilities follows thorough testing procedures for SSO SAML implementations. Oracle Utilities has separate instances of Digital Self Service - Transactions and federation servers specifically for integration testing. This is known as our staging environment. This infrastructure is completely separate from the production Oracle Utilities infrastructure.

Before going live with a utility, the Oracle Utilities staging infrastructure is configured to accept SAML assertions from the corresponding utility testing environment. The client
application and federation server must similarly be configured to send SAML assertions to the Oracle Utilities federation server.

In order to verify a successful connection and assist with troubleshooting, Oracle Utilities needs the ability to log in to the utility’s staging environment. This may require VPN access if the utility stage environment is located behind a firewall. Oracle Utilities also requires at least one valid login on the utility’s stage environment. For implementations where accounts are passed in the SAML assertion, account mappings must be created in the utility’s identity system with matching active accounts in the stage environments being used for testing.

After testing is complete, the configurations are migrated to the production applications for both Oracle Utilities and the utility. To verify these connections, Oracle Utilities also needs a test account on production.

The stage and production test accounts should be available for the life of the program for continuous verification of end-to-end SSO functionality.
Contacting Your Delivery Team

Your Oracle Utilities Delivery Team is the group responsible for setting up, configuring, launching, or expanding your Oracle Utilities Opower program. Contact your Delivery Team if you have any questions about your program products and implementation.

To contact your Delivery Team:

1. Log in to Inside Opower (https://inside.opower.com). This is your portal for questions and information related to your program.

2. Go to the **Community** tab to see who is on your Delivery Team.

3. Contact any of the team members using the information provided.

If you need to report an issue or get technical support, contact **My Oracle Support**.