Oracle Utilities Opower Digital Self Service - Transactions Authentication

Configuration Guide

F12826-32

Last Updated: November 20, 2023

Oracle Utilities Opower Digital Self Service - Transactions Authentication Configuration Guide

F12826-32

Contents

Getting Started

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

Note: Previous versions of this documentation provided configuration steps using Oracle Identity Cloud Service. Authentication for Digital Self Service - Transactions is supported through Oracle Cloud Infrastructure Identity and Access Management. If you require configuration steps that cover the previously supported Identity Cloud Service, contact your Oracle Utilities Delivery Team.

General Requirements

Digital Self Service - Transactions supports the following authentication approaches:

- Authentication using OAuth if integrating with Oracle Cloud Infrastructure Identity and Access Management.
- Single Sign-On (SSO), using OpenID Connect if integrating with Oracle Cloud Infrastructure Identity and Access Management, or Security Assertion Markup Language (SAML) 2.0 if using another identity provider to implement SSO with utilities.

Accessing Your Digital Self Service - Transactions Cloud Service

The following information assumes that you have completed your Digital Self Service - Transactions Initial Configurations including Linking Services to a Cloud Account described in the Oracle Utilities Opower Digital Self Service - Transactions Configuration Guide.

Oracle Cloud Infrastructure Identity and Access Management provides identity and access management functionality for the Oracle Utilities Cloud Services and supports SSO and identity federation capabilities.

In Identity and Access Management, an Identity Domain is enabled with each Digital Self Service - Transactions subscription to access non-production Digital Self Service - Transactions environments in OAuth mode. Once provisioned, the Identity Domain is administered exclusively by the client.

A security administrator uses the Identity Domain to manage applications and users, who are given access to a one or more application environments. The security administrator can also assign other users to an administrative role in the Identity Domain and delegate user management privileges.

- If you intend to support authentication to Digital Self Service - Transactions utilizing OAuth with Oracle Cloud Infrastructure Identity and Access Management, no further action is required to access your pre-production environments. Review the configuration options at "Oracle Cloud Infrastructure Identity and Access Management Product Configuration Steps" on page 16.
- If you intend to support authentication to Digital Self Service - Transactions in single sign-on mode, follow the steps for "Single Sign-On (SSO) Configuration" on page 35Identity and Access Management.

Oracle Cloud Infrastructure Identity and Access Management 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.

Oracle Cloud Infrastructure Identity and Access Management User Experience

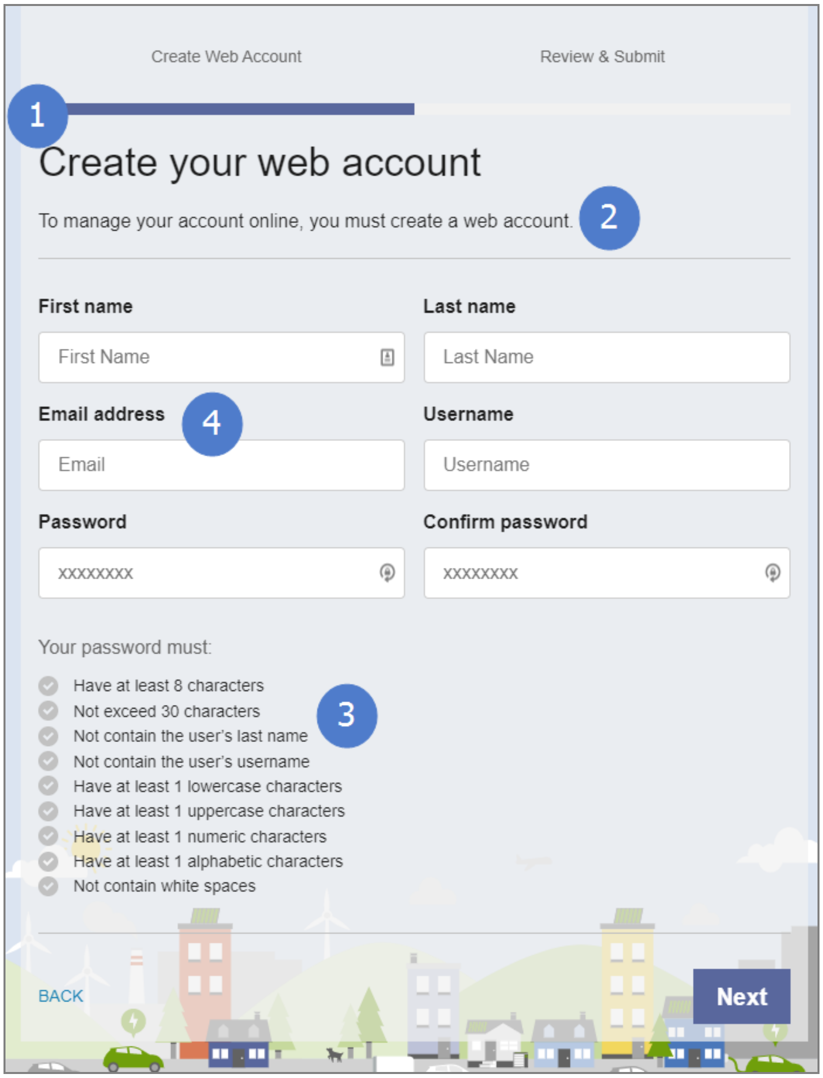
Digital Self Service - Transactions' built-in integration with Oracle Cloud Infrastructure Identity and Access Management includes features that allow customers to create an account, reset their password, and login with valid account credentials through the Digital Self Service - Transactions interface, as opposed to an external identity provider's interface. Use the following information to review Oracle Cloud Infrastructure Identity and Access Management 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 Cloud Infrastructure Identity and Access Management, including:

- First name
- Last name
- Email address
- A password that meets the configured password requirements



Create your web account

To manage your account online, you must create a web account.

First name: First Name

Last name: Last Name

Email address: Email

Username: Username

Password: xxxxxxxx

Confirm password: xxxxxxxx

Your password must:

- Have at least 8 characters
- Not exceed 30 characters
- Not contain the user's last name
- Not contain the user's username
- Have at least 1 lowercase characters
- Have at least 1 uppercase characters
- Have at least 1 numeric characters
- Have at least 1 alphabetic characters
- Not contain white spaces

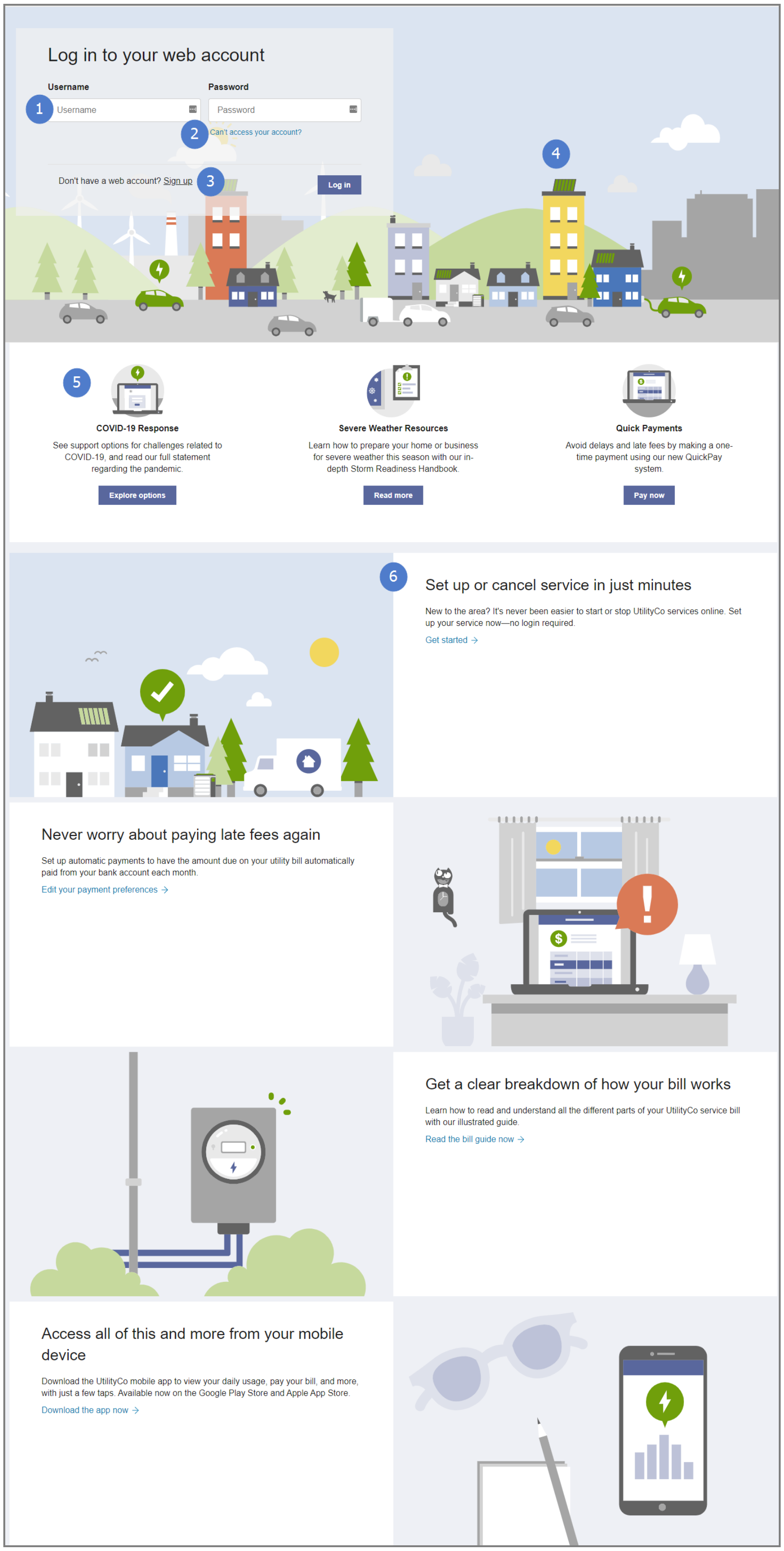
Image Number	Configuration Option
1	**Registration Widget Name** The title for the registration widget. **Default:** Create your web account
2	**Sub header** The supporting text for the registration widget.

Image Number	Configuration Option
	Default: To manage your account online, you must create a web account.
3	**Password Policy** A simple, standard, or custom password policy must be configured in Oracle Cloud Infrastructure Identity and Access Management. **Default:** Standard
4	**Unique Email as Web Username** Web account registration, login, and password reset is based on the customer's email address by default. Utilities can also enable users to register, login, and reset their password with a unique username instead of a unique email. If you enable a unique username instead of the default configuration that uses an email address, ensure that when defining invite guest user tasks, roles, and alerts, the **Allow Duplicate Web User Email** option is selected for linking self-service users. **Default:** Email
Not Pictured	**Resend Verification Email** The supporting text for the resend email link. **Default:** Didn't receive the email? Resend
Not Pictured	**Resend Verification Email Success** The supporting text for the resend email success message. **Default:** Email verification has been resent. Please check your inbox.

Image Number	Configuration Option
Not Pictured	**Terms and Conditions** A terms and conditions link can be displayed, which sends users to the utility's public terms and conditions page on their website. Customers are required to select the terms and conditions checkbox to confirm that they agree to the terms and conditions as part of their account registration. **Default**: False

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.



Log in to your web account

Username

Username

Password

Password

Can't access your account?

Don't have a web account? Sign up

Log in

COVID-19 Response

See support options for challenges related to COVID-19, and read our full statement regarding the pandemic.

Explore options

Severe Weather Resources

Learn how to prepare your home or business for severe weather this season with our in-depth Storm Readiness Handbook.

Read more

Quick Payments

Avoid delays and late fees by making a one-time payment using our new QuickPay system.

Pay now

Set up or cancel service in just minutes

New to the area? It's never been easier to start or stop UtilityCo services online. Set up your service now—no login required.

Get started →

Never worry about paying late fees again

Set up automatic payments to have the amount due on your utility bill automatically paid from your bank account each month.

Edit your payment preferences →

Get a clear breakdown of how your bill works

Learn how to read and understand all the different parts of your UtilityCo service bill with our illustrated guide.

Read the bill guide now →

Access all of this and more from your mobile device

Download the UtilityCo mobile app to view your daily usage, pay your bill, and more, with just a few taps. Available now on the Google Play Store and Apple App Store.

Download the app now →

Image Number	Configuration Option
1	**Login ID** Customers can log in using a unique email address or username. **Default:** Email
2	**Account Recovery Link** A link to allow the customer to reset their own password. **Default:** The "Can't access your account?" link directs users to the account recovery widget.
3	**Sign Up Link** 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
4	**Background Image** An image can be displayed as the background of the login area. The background is also displayed on the Password Reset and Registration widgets if enabled. Utilities may use the default background image and work with Oracle Utilities to customize its colors to meet their brand guidelines per the utility branding guidelines in the *Oracle Utilities Opower Platform Configuration Guide*. **Default**: A graphic city-scape image, as shown in the example above.
5	**Quick Links** The quick links section includes three configurable links that support an image, title, description, and call to action button that links to additional resources. Be aware that links must redirect users to content that does not require authentication, as these links are provided on the login page and thus customers are not

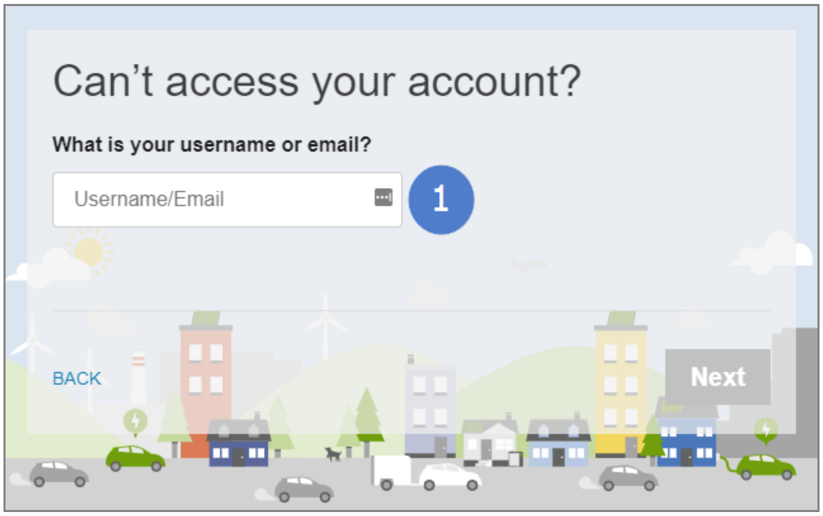
Image Number	Configuration Option
	yet signed in to their accounts. The quick links are enabled by default and use the following default content. If enabled, applicable content must be provided for the three quick link slots, including an applicable redirect link. If disabled, the entire quick links section is hidden. Utilities may use the default quick link images and work with Oracle Utilities to customize their colors to meet their brand guidelines per the utility branding guidelines in the *Oracle Utilities Opower Platform Configuration Guide*. **Defaults**: ■ **Slot 1**: COVID-19 Response See support options for challenges related to COVID-19, and read our full statement regarding the pandemic. Explore options ■ **Slot 2**: Severe Weather Resources Learn how to prepare your home or business for severe weather this season with our in-depth Storm Readiness Handbook. Read more ■ **Slot 3**: Quick Payments Avoid delays and late fees by making a one-time payment using our new QuickPay system. Pay now
6	**Content Blocks**

Image Number	Configuration Option
	Content blocks are full-width spaces to promote utility programs and content. At least one content block is required with a maximum of four. Content blocks support a title, description, call to action link, and image. Be aware that links must redirect users to content that does not require authentication, as these links are provided on the login page and thus customers are not yet signed in to their accounts. Utilities may use the default content block images and work with Oracle Utilities to customize their colors to meet their brand guidelines per the utility branding guidelines in the *Oracle Utilities Opower Platform Configuration Guide*. **Defaults**: ■ **Block 1**: Set up or cancel service in just minutes New to the area? It's never been easier to start or stop UtilityCo services online. Set up your service now—no login required. Get Started ■ **Block 2**: Never worry about paying late fees again Set up automatic payments to have the amount due on your utility bill automatically paid from your bank account each month. Edit your payment preferences ■ **Block 3**: Get a clear breakdown of how your bill works Learn how to read and understand all the different parts of your UtilityCo service bill with our illustrated guide. Read the bill guide now

Image Number	Configuration Option
	■ **Block 4**: Access all of this and more from your mobile device Download the UtilityCo mobile app to view your daily usage, pay your bill, and more, with just a few taps. Available now on the Google Play Store and Apple App Store. Download the app now
Not Pictured	**iFrame Slot** A full-width content block can be enabled to embed and display iFrame content beneath the content blocks. **Default**: Disabled
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.



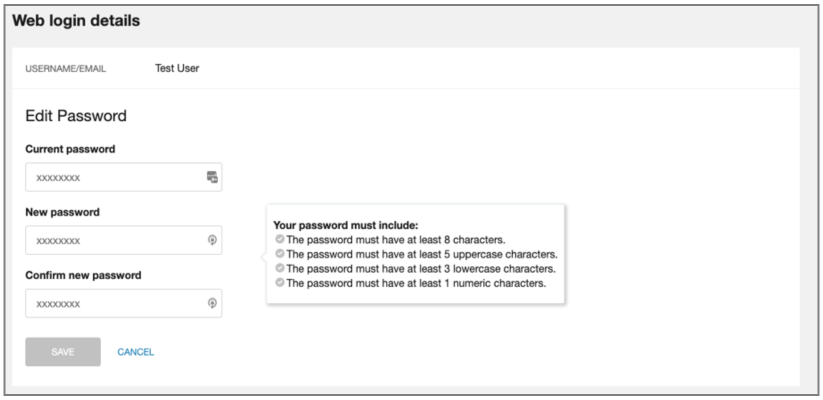
Can't access your account?

What is your username or email?

Image Number	Configuration Option
1	**Login ID** Customers can trigger a password reset notification based on their email address or username. **Default:** Email
Not Pictured	**Destination URL** The destination after login. **Default:** /dss/overview

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

USERNAME/EMAIL Test User

Edit Password

Current password

xxxxxxxx

New password

xxxxxxxx

Confirm new password

xxxxxxxx

Your password must include:
- The password must have at least 8 characters.
- The password must have at least 5 uppercase characters.
- The password must have at least 3 lowercase characters.
- The password must have at least 1 numeric characters.

Reset Password

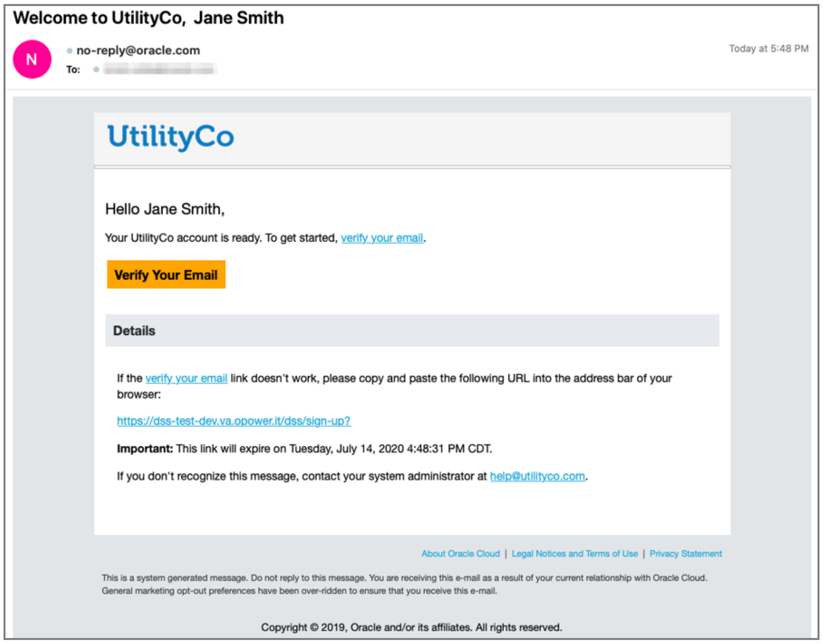
Users can be required to reset their passwords in the following scenarios:

- **Expired Password**: Oracle Cloud Infrastructure Identity and Access Management administrators can configure passwords to expire after a defined number of days. If a customer's password has expired and they try to log in with their previous password, they are redirected to the password reset page. The customer is required to provide their current password and set a new password in accordance with the current password policy to regain access to their account.
- **Password Reset Forced by an Administrator**: Oracle Cloud Infrastructure Identity and Access Management administrators can force all users to set a new password on their next login. This action can be taken when the password policy is modified, and this reset ensures that customer passwords meet the new criteria

  When an administrator forces a password reset, customers receive an automated email with a link to reset their password. If the customer attempts to log in with their previous password after an administrator forces a password reset, an error message is displayed until their password has been reset.

Notifications

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



Welcome to UtilityCo, Jane Smith

N

no-reply@oracle.com

To: [redacted]

Today at 5:48 PM

UtilityCo

Hello Jane Smith,

Your UtilityCo account is ready. To get started, verify your email.

Verify Your Email

Details

If the verify your email link doesn't work, please copy and paste the following URL into the address bar of your browser:

https://dss-test-dev.va.opower.it/dss/sign-up?

Important: This link will expire on Tuesday, July 14, 2020 4:48:31 PM CDT.

If you don't recognize this message, contact your system administrator at help@utilityco.com.

About Oracle Cloud | Legal Notices and Terms of Use | Privacy Statement

This is a system generated message. Do not reply to this message. You are receiving this e-mail as a result of your current relationship with Oracle Cloud. General marketing opt-out preferences have been over-ridden to ensure that you receive this e-mail.

Copyright © 2019, Oracle and/or its affiliates. All rights reserved.

When Oracle Cloud Infrastructure Identity and Access Management is used for authentication to Digital Self Service - Transactions, customers can receive email notifications in their preferred language. For example, if a customer defines their preferred language as Spanish within Digital Self Service - Transactions, the notifications they receive directly from Oracle Cloud Infrastructure Identity and Access Management display content in Spanish.

The language must be supported by all integrated products for customers to receive a notification in the respective language. Languages that are supported by Oracle Cloud Infrastructure Identity and Access Management, Customer Care and Billing, and Digital Self Service - Transactions include:

- English
- Spanish

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 Cloud Infrastructure Identity and Access Management is locked.

User Account Unlocked: An end user is notified that their account in Oracle Cloud Infrastructure Identity and Access Management 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.

In addition to the standard notifications listed above, the following notifications are supported when a utility requires customers to register with a separate username and email address.

Recovery Email Verification: After a user changes their password recovery email address, this notification is sent to the user to verify the address.

Primary Email Verification: After a user changes their primary email address, this notification is sent to the user to verify the email address.

Secondary Email Verification: After a user changes their secondary email address, this notification is sent to the user to verify the email address.

Recovery Email Update: After a user changes their password recovery email address, this notification is sent to the user confirming the change.

Primary Email Update: After a user changes their primary email address, this notification is sent to the user confirming the change.

Secondary Email Update: After a user changes their secondary email address, this notification is sent to the user confirming the change.

Third-Party Applications

A utility's online portal can require that authenticated web applications are available to their customers alongside Digital Self Service - Transactions to maintain a single, integrated experience for their customers. For example, a utility can link to a customer rewards program and website directly from Digital Self Service - Transactions, redirecting the customer without requiring them to log in again.

Oracle Cloud Infrastructure Identity and Access Management Product Configuration Steps

After reviewing all of the feature configuration options provided in the "Oracle Cloud Infrastructure Identity and Access Management User Experience" on page 3 section, you then complete the following configuration tasks using Oracle Cloud Infrastructure Identity and Access Management.

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

Configuration tasks include:

Be aware that you are required to create and integrate an additional identity domain to support your customers in your live production environment. Production readiness configuration tasks include:

Application Configuration

Within the context of the integration with Digital Self Service - Transactions, Oracle Cloud Infrastructure Identity and Access Management acts as the Identity Provider (IDP). This means that Oracle Cloud Infrastructure Identity and Access Management 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 Cloud Infrastructure Identity and Access Management:

1. Navigate to your domain in the Oracle Cloud Infrastructure Identity and Access Management Admin Console and select the **Applications** menu.
2. Select **Add application** and then select **Confidential Application** from the list of applications. Select **Launch Workflow** to begin creating the new application.
3. Enter the following information in the new application wizard, and then click **Next**:
   - **Name:** For example, enter DSS-Production, which is used later in authentication configuration steps. You will need to provide this name to your Oracle Utilities 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.opower.com`.
   - **Enforce Grants as authorization**: Ensure this option is cleared, which disables this option.
4. Within the **Client configuration** area, select the **Configure this application as a client now** option and complete the following fields:
   - **Authorization:** Within the Allowed Grant Types area, select **Client Credentials** and **JWT Assertion**.
   - **Redirection URL**: Provide the URL to the main landing page of your Web Portal.
   - **Token Issuance Policy:** Select the **Add app roles** option, and then click **Add** to add each of the following roles:
     - Me
     - Signin
     - Verify Email
     - Forgot Password
     - Self Registration
     - Reset Password
     - User Administrator

    - Identity Domain Administrator - This role is required if you plan to send notifications to pre-authenticated customers that reflect their preferred language

5. Click **Next**, and in the **Web tier policy** area, verify that **Skip for later** is selected.
6. Click **Finish**, and make note of the Client ID and Client Secret that are generated. You must provide these to your Oracle Utilities Delivery Team to complete the integration.
7. After the application has been created in Oracle Cloud Infrastructure Identity and Access Management, you activate the application. From the Admin Console, select **Applications**, select the check box for the application you created, and then from the Actions drop-down list select **Activate**.

Create Groups

A group can be used to grant access to organize users within your identity system and, in some cases, control their access to applications. Groups are an optional way to control access to Digital Self Service - Transactions. To create a group in Oracle Cloud Infrastructure Identity and Access Management that can control access to Digital Self Service - Transactions:

1. Navigate to your domain in the Oracle Cloud Infrastructure Identity and Access Management Admin Console, and then select **Groups**.
2. Select **Create group** and enter group information using the following information:
    - **Name**: DSSUserGroup
    - **Description**: Use this group for utility customers who have access to standard Digital Self Service - Transactions customer pages.
    - **User can request access**: Ensure this option is selected.
3. Save your changes to create the group.

Assign the Application to Groups

If you use groups in your implementation, you must assign the DSS Production application to the group 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 select the DSSUserGroup group you created.
2. While viewing the group, select **Applications**, and select **Assign applications** to assign the **DSS Production** application to the group.

Create Users

You must create users to control access to Digital Self Service - Transactions. Admin and CSR users are manually created through the Oracle Cloud Infrastructure Identity and Access Management Admin Console. If you use groups as part of your implementation, you may assign users to their respective group. External users can self-register for Digital Self Service - Transactions accounts or can be bulk imported. See Create a Self-Registration Profile for additional information required to configure user self-registration.

Creating Individual Admin and CSR Users

When adding individual users including administrators and CSRs, consider the rights of access you want to grant them within Oracle Cloud Infrastructure Identity and Access Management.

It is recommended that only a few users have Identity domain administrator access and that supporting staff including CSRs have a lower-level role such as Help desk administrator to prevent unintentional changes.

See Understanding Administrator Roles for additional information about administrator roles and how to add or remove a user account from an administrator role.

CSRs will need access to Oracle Cloud Infrastructure Identity and Access Management only if they are expected to be able to unlock web user accounts on behalf of a customer. Otherwise, CSRs can assist customers with password resets using existing tools including the Customer Billing System and the Digital Self Service - Transactions web portal.

To create new users individually:

1. Log in to the Oracle Cloud Infrastructure Identity and Access Management Admin Console, navigate to **Users** and select **Create user**.
2. Enter the user’s personal information.
3. Click **Create**.

Bulk Importing External Users

You may also import multiple users using the bulk import process in Oracle Cloud Infrastructure Identity and Access Management. To import users in bulk, from the **Users** area, in the **More actions** drop-down list, select **Import users**. In the dialog box that opens, you can select **Download sample file** to download the import template. You can update the sample csv file with applicable user information. When finished, you then import the file using the same **Import users** action.

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 Cloud Infrastructure Identity and Access Management passes to Digital Self Service - Transactions:

Name	Format	Type	Value	Condition
groups This attribute is not required if groups are not used in your implementation.	Basic	User Attribute	DSSUserGroup	All Groups
firstName	Basic	User Attribute	First Name	
lastName	Basic	User Attribute	Last Name	
email	Basic	User Attribute	Primary Email	
username	Basic	User Attribute	Username	
userID	Basic	User Attribute	Assigned User ID	

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 profile for users to enter their information.

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. If you use groups as part of your user access implementation, this profile automatically assigns the user to the DSSUserGroup.

To create a self-registration page for external users:

1. Navigate to your domain in the Oracle Cloud Infrastructure Identity and Access Management Admin Console.
2. Select **Settings**, then select **Self Registration**, and then select **Add profile**.
3. Specify the following information, which are the only configurations supported by Digital Self Service - Transactions:
   - **Profile Name:** DSS_Production_Self_Registration_Profile
   - **User Consent required:** Ensure this checkbox is cleared.
   - **Assign to Group:** DSSUserGroup
     This setting is only required if you use groups as part of your user access implementation.
   - **Allow Email Domains:** all
4. Under **Self-Registration Content**, provide a name in **Registration Page Name** such as `Production_Self_Registration`. This name is internal only and is not shown to customers.
5. Click **Add profile**.
6. Select the self-registration profile you just created, and from the menu on the right-hand side select the **Activate** option.
7. Re-open the profile and 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.

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

Supporting Notifications for Pre-authenticated Customers in Preferred Language

If you plan to send notifications to pre-authenticated customers that reflect their preferred language, additional configuration for the self-registration portal is required.

To support notifications for pre-authenticated customers in their preferred language

1. To update the self-registration profile, a REST API must be used. Refer to IAM Identity Domains API for information on how to use the applicable REST APIs, which includes tasks such as retrieving a required access token for the REST API calls.
2. Use the Update a Self-Registration Profile endpoint to update the profile to support a customer's preferred language. The following request must be made, replacing `Host` with the applicable host value for your system. You must also provide the required access token, which can be obtained using the Generate access token endpoint, and other applicable authorization requirements in the header of the request:

```
PATCH {{Host}}/admin/v1/SelfRegistrationProfiles/
{SelfRegistrationProfileID}

{

        "schemas": [

        "urn:ietf:params:scim:api:messages:2.0:PatchOp"

        ],

        "Operations": [{

                "op": "add",

                "path": "userAttributes",

                "value": [

                        {

                                "value": "locale",
                                "deletable": false,
                                "fullyQualifiedAttributeName":
"urn:ietf:params:scim:schemas:core:2.0:User:locale",
                                "seqNumber": 8
                        },
                        {
                                "value": "preferredLanguage",
                                "deletable": false,
                                "fullyQualifiedAttributeName":
"urn:ietf:params:scim:schemas:core:2.0:User:preferredLangua
ge",
                                "seqNumber": 9
                        }
                ]
        }
]
}
```

In addition to updating the self-registration profile, email template updates are required as described in "Customize Email Templates" on page 25.

Update Account Recovery Settings

Customers must verify their email address before they can log in to the Digital Self Service - Transactions Web Portal with their web account credentials for the first time. This requirement ensures that customers have access to the email address that they provided when signing up.

To ensure a customer is required to verify their address prior to logging in:

1. Navigate to your domain in the Oracle Cloud Infrastructure Identity and Access Management Admin Console.
2. Select **Security**, then select **Account Recovery**, and then select the **Email** checkbox. You can also select **Configure** to further configure the email recovery options.
3. Click **Save changes**.

Update the Password Policy

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

- Simple
- Standard
- Custom

To create a custom policy in Oracle Cloud Infrastructure Identity and Access Management:

1. Navigate to your domain in the Oracle Cloud Infrastructure Identity and Access Management Admin Console. From **Settings**, select **Password Policy** page.
2. Select an available password policy to modify, or select **Add** to create a new password policy.
3. Select the password policy strength as **Custom**, and then 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 Cloud Infrastructure Identity and Access Management branding customizations include the application logo, company name, contact email addresses, and notification email address.

To update Oracle Cloud Infrastructure Identity and Access Management branding:

1. Log in to the Oracle Cloud Infrastructure Identity and Access Management Admin console. Navigate to your domain and select **Settings**, and then select **Domain Settings**.
2. Update the **Contact** area with applicable email addresses. For example, enter: customerservice@UtilityCo.com. Select **Save changes** as required.
3. From the same **Settings**, select **Notifications**, and then update the **Sender's Email Address**. For example, enter no-reply@UtilCo.com. Select **Save changes** as required.
4. From the same **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. Select **Save changes** as required.

Customize Email Templates

Integration with Oracle Cloud Infrastructure Identity and Access Management 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 Cloud Infrastructure Identity and Access Management.

Self-Registration Email Verification: After successfully creating an account, this notification is sent to the user to verify the email address. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal and the token for confirmation. For example, `https://dss-example.opower.com/dss/user/email/confirm?confirm=${userToken}.`

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. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal and the token for confirmation. For example, `https://dss-example.opower.com/dss/password-reset?token=${userToken}`. 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 Cloud Infrastructure Identity and Access Management is locked. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/password-reset`.

User Account Unlocked: An end user is notified that their account in Oracle Cloud Infrastructure Identity and Access Management 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. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal and the token for confirmation. For example, `https://dss-example.opower.com/dss/user/email/confirm?confirm=${userToken}`.

In addition to the standard notifications listed above, the following notifications are supported when a utility requires customers to register with a separate username and email address.

Recovery Email Verification: After a user changes their password recovery email address, this notification is sent to the user to verify the address. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/login`.

Primary Email Verification: After a user changes their primary email address, this notification is sent to the user to verify the email address. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/user/email/confirm?confirm=${userToken}`.

Secondary Email Verification: After a user changes their secondary email address, this notification is sent to the user to verify the email address. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/login`.

Recovery Email Update: After a user changes their password recovery email address, this notification is sent to the user confirming the change. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/login`.

Primary Email Update: After a user changes their primary email address, this notification is sent to the user confirming the change. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/login`.

Secondary Email Update: After a user changes their secondary email address, this notification is sent to the user confirming the change. By default, the link provided in this notification references Oracle Cloud Infrastructure Identity and Access Management. Modify this link to use the host name for Digital Self Service - Transactions Web Portal. For example, `https://dss-example.opower.com/dss/login`.

To customize email templates:

> **Note**: If supporting multiple languages, complete the steps below for templates of all of your supported languages.

1. Log in to the Oracle Cloud Infrastructure Identity and Access Management 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 Cloud Infrastructure Identity and Access Management Admin Console.
2. Navigate to your domain and select **Settings**, then select **Notifications**, and then choose one of the following options:
   - **Verify Sender's Domain**: Validation emails are sent to the postmaster account of the email's domain.
   - **Verify Sender's Email**: Validation emails are sent to the email that you provide.

Create Additional Oracle Cloud Infrastructure Identity and Access Management Domains

A minimum of two dedicated Oracle Cloud Infrastructure Identity and Access Management domains are required for your Digital Self Service - Transactions integration. This separates users and configurations for production and non-production environments and ensures you utilize universal credits effectively.

The first domain that was provisioned as part of your cloud tenancy is used by your implementation and UAT Digital Self Service - Transactions environments, and is limited in functionality and number of supported users as a free service. You must provision a second domain for your customer production environment through a premium service of Oracle Cloud Infrastructure Identity and Access Management.

Note: If you intend to use a third-party identity provider for authentication in production, refer to "Single Sign-On (SSO) Configuration" on page 35.

To create your production domain, complete these steps in your Oracle Cloud Account:

1. Open the navigation menu and select **Identity & Security**. Within **Identity**, select **Domains**.
2. Select **Create domain**. The Create domain page opens.
3. Provide the following information:
   - **Display name**: A descriptive name such as customerprod. Use only letters, numerals, hyphens, periods, or underscores. The name can contain up to 100 characters. Choose your display name carefully. Changing the display can cause additional updates such as updates to bookmarked URLs to use the new display name.
   - Description: Provide a detailed description of the domain.
   - **Domain type**: From the available **Domain Types**, select **External User**. For additional information about domain types, see IAM Identity Domain Types.
   - **Domain administrator**: If you want to use your administrative user account for this identity domain, then clear the **Create an administrative user for this account** option. Otherwise, enter the details of the user you want to administer this identity domain.
   - **Compartment**: You have the option to choose a different compartment if required.
   - **Show Advanced Options**: To add tagging, select **Show Advanced Options** and enter the tagging details.
4. Select **Create Domain**. You are now ready to configure the production instance like you did for implementation following the "Oracle Cloud Infrastructure Identity and Access Management Product Configuration Steps" on page 16.

Integrate Third-Party Applications

A utility's online portal can require that authenticated web applications are available to their customers alongside Digital Self Service - Transactions to maintain a single, integrated experience for their customers. For example, a utility can link to a customer rewards program and website directly from Digital Self Service - Transactions, redirecting the customer without requiring them to log in again.

Refer to the information below to integrate your third-party application with Digital Self Service - Transactions.

Resource Requirements

The third-party application or partner resource must expose an endpoint that consumes a JWT assertion form parameter using a POST method. The resource uses the JWT assertion to request an access token from Oracle Cloud Infrastructure Identity and Access Management. Upon successful validation of the JWT assertion, an access token including the web user ID is sent to the resource. The resource uses the access token along with the JWT assertion to create a user session. At this point, a 302 redirect to the resource can be sent to the browser to provide the user with access to the resource.

A utility must ensure any third-party resources meet integration requirements. The third-party application or partner resource must expose an endpoint that consumes a JWT assertion form parameter using a POST method. The resource uses the JWT assertion to request an access token from Oracle Cloud Infrastructure Identity and Access Management. Upon successful validation of the JWT assertion, an access token including the web user ID is sent to the resource. The resource uses the access token along with the JWT assertion to create a user session. A 302 redirect to the resource can then be sent to the browser to provide the user with access to the resource.

> **Note**: A GET method is a supported option as well. In this case, a `jwt_assertion` query parameter contains the JWT assertion. This option is considered less secure and prone to issues with very large JWT assertions. For these reasons Oracle Utilities recommends a POST method strategy instead.

Rules of redirection to specific partner resources are up to the implementation. For example, the partner can expose an endpoint that contains `targetResource` as one of query parameters, which specifies a page where the user is redirected after successful JWT assertion validation. In this scenario, it is up to the partner resource to verify the validity of the resource specified in the `targetResource` parameter.

Endpoint Specification

A Digital Self Service - Transactions resource sends the JWT assertion in the body of a POST method. The endpoint specification requirements are provided below for the recommended POST method.

- Method: POST
- Content-Type: application/x-www-form-urlencoded

- Endpoint Path: The path can be any valid path, and this path information must be shared with Oracle Utilities.
- Endpoint Form Parameters:
  - jwt_assertion: String containing the JWT assertion.
- Endpoint Responses: The response must perform the required redirection, and aside from the redirection the responses are up to the utility to meet their requirements. Example responses include:
  - 302: Successful response with a location header pointing to partner resource site page.
  - 302: Error response with location header pointing to an error page on partner resource site page.

Contact the Oracle Utilities Delivery Team for methods in which to securely share this information.

Oracle Cloud Infrastructure Identity and Access Management Configuration

Oracle Cloud Infrastructure Identity and Access Management configuration for a third-party application or partner resource requires the creation of an application which supports JWT Assertion authorization.

1. Navigate to the Oracle Cloud Infrastructure Identity and Access Management 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 Partner-Resource. You will need to provide this to your delivery team to complete the integration.
   - **Application URL:** Provide the URL for the third-party application or partner resource.
   - **Enforce Grants as authorization**: Ensure this option is cleared.
4. On the next page, select the **Configure this application as a client now** option and complete the following fields:
   - **Authorization:** Within the Allowed Grant Types area, select **JWT Assertion**.
   - **Redirection URL**: Provide the URL to the main landing page of your third-party application or partner resource.

- **Token Issuance Policy:** Select the **Add app roles** option, and then click **Add** to add each of the following roles:
    - Me
    - Signin
    - Verify Email
    - Forgot Password
    - Self Registration
    - Reset Password
    - User Administrator

5. Click **Next**, and in the **Web tier policy** area, verify that **Skip for later** is selected.
6. Click **Finish**, and make note of the Client ID and Client Secret that are generated. You will provide these to your Oracle Utilities Delivery Team to complete the integration.
7. After the application has been created in Oracle Cloud Infrastructure Identity and Access Management, you activate the application. From the Admin Console, select **Applications**, select the check box for the application you created, and then from the Actions drop-down list select **Activate**.
8. Navigate to **Menu**, then **Settings**, and then select **Trusted Partner Certificates**.
9. Select the option to **Import Certificate**, and then select the Digital Self Service - Transactions certificate provided by Oracle Utilities.

Oracle Cloud Infrastructure Identity and Access Management Testing Procedure

Oracle Utilities follows thorough testing procedures for Oracle Cloud Infrastructure Identity and Access Management 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.

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 identity assertion only authenticates a web user ID, group, and identifying information.

To support single 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.

Determine Your SSO Implementation

Determine if your identity system supports OpenID Connect (OIDC) and the ability to maintain separate configuration for Stage and Production environments.

- If your identity system, including Oracle Identity and Access Management, supports OpenID Connect refer to "OpenID Connect Single Sign-On Configuration" on page 36.
- If your identity system does not support OpenID Connect, an identity bridge is required. Refer to "Supported SAML Single Sign-On Profiles" on page 38.

Single Sign-On User Experience

The user experience can be customized when implementing 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 40) 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.

OpenID Connect Single Sign-On Configuration

When implementing SSO using OpenID Connect, you must complete the following configurations.

Define the Redirect for Single Logout

When configuring SSO along with single logout (SLO), a redirect URL must be configured. This URL determines where customers are redirected to after the logout process is completed. If configured incorrectly, the logout process can produce an error or redirect the customers to an unintended location.

The redirect URL can be configured using the Post Logout Redirect URL parameter within the Oracle Identity and Access Management application created for Digital Self Service - Transactions, as well the `logoutPath` value which can be defined by Oracle Utilities. Oracle Utilities recommends defining both values to redirect to the same location, which provides the most consistent behavior for customers. Oracle Utilities also recommends to redirect customers to the main Overview page of the Digital Self Service - Transactions web portal. Refer to "Configuring the Identity System" on page 36 below, which includes steps to define the Post Logout Redirect URL and provide an applicable `logoutPath` value to Oracle Utilities that results in customers being redirected to the Overview page.

Configuring the Identity System

Configuration steps may differ depending on your identity system. The following steps cover configuration with Oracle Identity and Access Management:

1. Create a "Confidential Application" with the following definitions:
    - **Application Name**: Provide a descriptive name for the application.
    - **Authorization**: Within the **Allowed Grant Types** area, select both **Client Credentials** and **Authorization Code**.
    - **Redirect URL**: This URL must direct users to the appropriate location that hosts Digital Self Service - Transactions content. Redirect URL format is as follows `https://[fqdn]/webcenter/edge/apis/identity-management-v1/cws/v1/auth/`

    `[utilityCode]/sso/login/callback` where:
    - `fqdn` is the Fully qualified domain name of your Digital Self Service - Transactions web portal.
    - `utilityCode` is a three- or four-character code that identifies the utility.
  - **Logout URL**: Is required if SLO is enabled. The URL must direct users to the appropriate location that hosts Digital Self Service - Transactions. Logout URL format is as follows `https://[fqdn]/webcenter/edge/apis/identity-management-v1/cws/v1/auth/[utilityCode]/sso/logout/external` where:
    - `fqdn` is the Fully qualified domain name of your Digital Self Service - Transactions web portal.
    - `utilityCode` is a three- or four-character code that identifies the utility.
  - **Post Logout Redirect URL**: Is required if SLO is enabled. The URL must direct users to the appropriate location after they log out of Digital Self Service - Transactions. Post Logout Redirect URL format is as follows `https://[fqdn]/[location]` where:
    - `fqdn` is the Fully qualified domain name of your Digital Self Service - Transactions web portal or other redirect resource.
    - `location` is the relative path to the location in the Digital Self Service - Transactions web portal, or other redirect resource, to redirect customers to. For example, a value of `dss/overview` redirects customers to the main Overview page of Digital Self Service - Transactions web portal. For additional information on this resource, refer to " Define the Redirect for Single Logout" on page 36.

2. Configure user groups if required:
   a. Create a separate user group.
   b. Assign the application created from the previous step to the new user group.
   c. When creating new users assign them to this user group. This also includes the users in the Confidential Application.

3. After configuration of the application is complete, provide Oracle Utilities with the following information from your configuration through a service request (to create a service request, see "Contacting Your Delivery Team" on page 45):
   - The Client ID is a public identifier for the Digital Self Service - Transactions application.

- The Client Secret is the secret that matches the application's Client ID.
- The Identity and Access Management host, for example, `https://[hostID].identity.preprod.oraclecloud.com/`.
- The `logoutPath` value, if single logout is configured and supported. To redirect to the recommended Overview page, the configuration can be requested as `/oauth2/v1/userlogout?post_logout_redirect_url=https://FQDN/dss/overview` where:
  - `fqdn` is the Fully qualified domain name of your Digital Self Service - Transactions web portal.
- **Post Logout Redirect URL**: Is required if SLO is enabled. The URL must direct users to the appropriate location after they log out of Digital Self Service - Transactions. Post Logout Redirect URL format is as follows `https://[fqdn]/[location]` where:
  - `fqdn` is the Fully qualified domain name of your Digital Self Service - Transactions web portal or other redirect resource.
  - `location` is the relative path to the location in the Digital Self Service - Transactions web portal, or other redirect resource, to redirect customers to.
- The web user accounts to be used for end-to-end testing.

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. Oracle Utilities requires 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 optional attribute controls the user landing page for groups of users. For example a `DSSUserGroup` group can support all users of Digital Self Service - Transactions, including utility customers and customer service representatives who can masquerade as utility customers.
- `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.

```
<saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" Name="userDataXML">

    <saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><![CDATA[<?xml
version="1.0" encoding="UTF-8" ?>

    <sso_user_properties>

          <property>

                <name>language_preference</name>

                <value>zh_HK</value>

          </property>

    </sso_user_properties>

    ]]></saml:AttributeValue>

  </saml:Attribute>

</saml:AttributeStatement>
```

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.

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

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

Information Required by Oracle Utilities from the 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:

- **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 IdP 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.

Define the Redirect for Single Logout

When configuring SSO along with single logout (SLO), a redirect URL must be configured within your identity provider as well as by Oracle Utilities. This URL determines where customers are redirected to after the logout process is completed.

If configured incorrectly, the logout process can produce an error or redirect the customers to an unintended location.

Oracle Utilities recommends defining both values to redirect to the same location, which provides the most consistent behavior for customers. Oracle Utilities also recommends redirecting customers to the main Overview page of the Digital Self Service - Transactions web portal.

SSO Testing Procedures

Oracle Utilities follows thorough testing procedures for SSO implementations. Oracle Utilities has separate instances of Digital Self Service - Transactions specifically for integration testing. This is known as our staging environment.

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

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 SSO 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 assisting your deployment of Digital Self Service - Transactions. Contact your Delivery Team if you have any questions about your program products and implementation. Open a service request in My Oracle Support to coordinate configuration of Digital Self Service - Transactions features.

To request changes to default product and message configurations:

1. Review the tables provided in this documentation for each feature that has applicable configuration options.
2. Provide any changes to the default product and message configurations listed for each feature by submitting your request through My Oracle Support.
    a. Go to My Oracle Support. Click **Cloud Support** and log in.
    b. Click the **Create Service Request** button and follow the prompts to complete the Service Request.