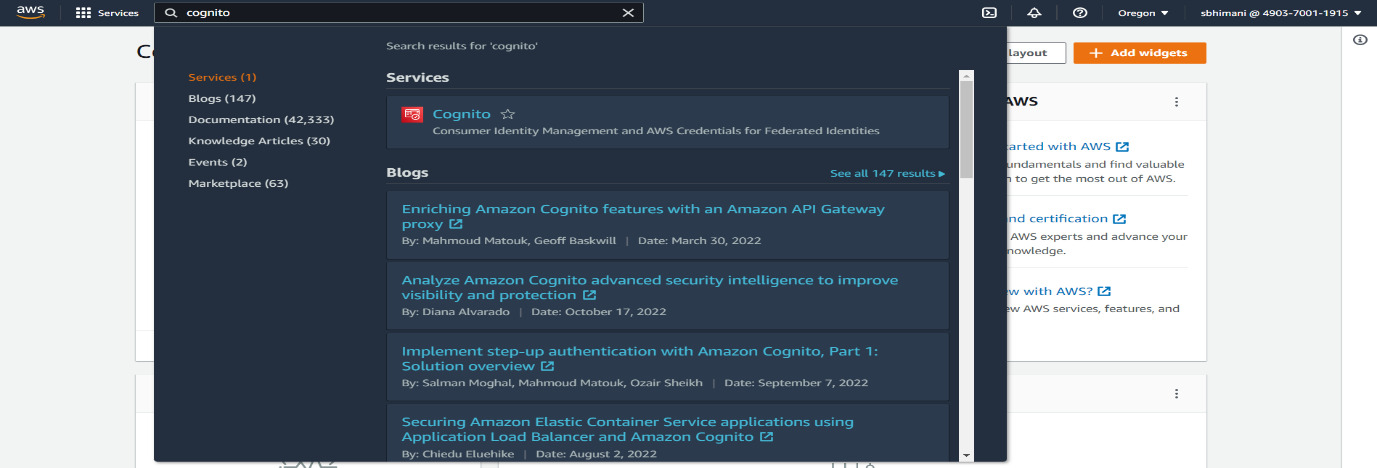
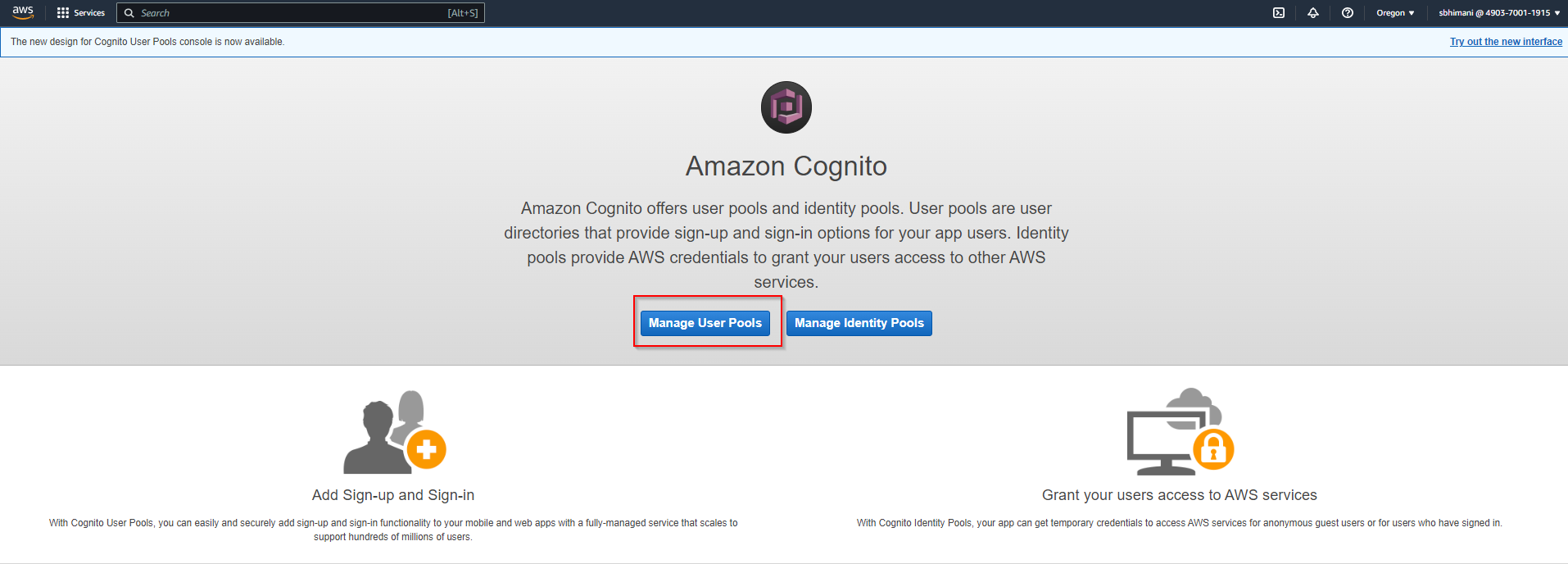
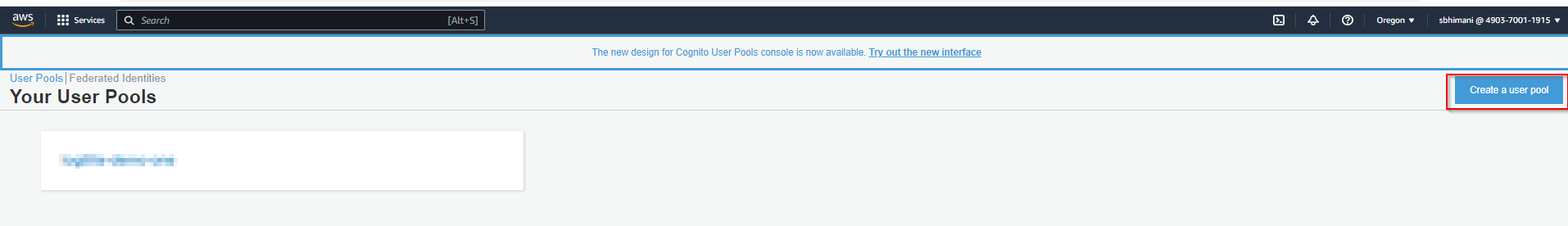
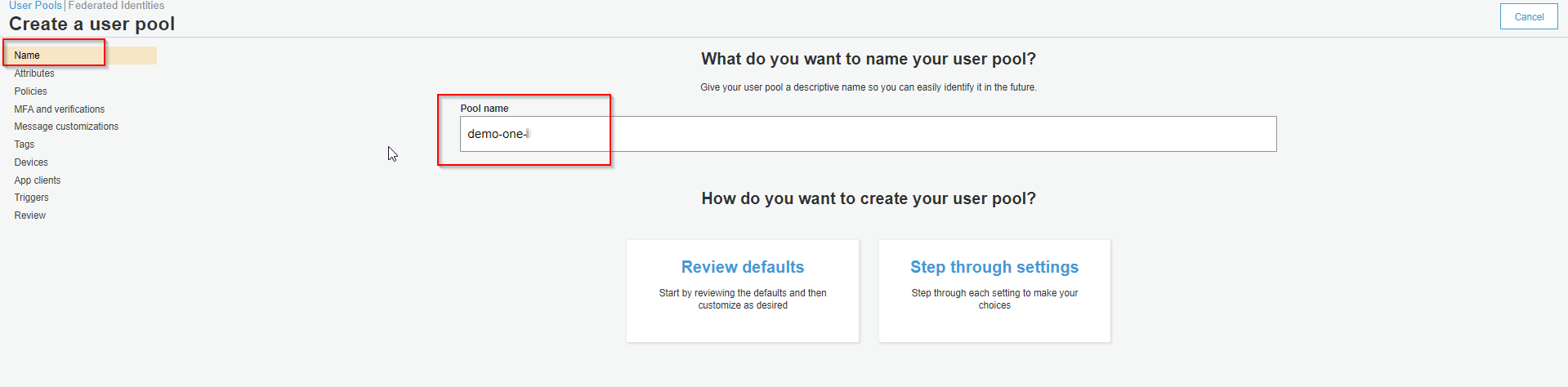
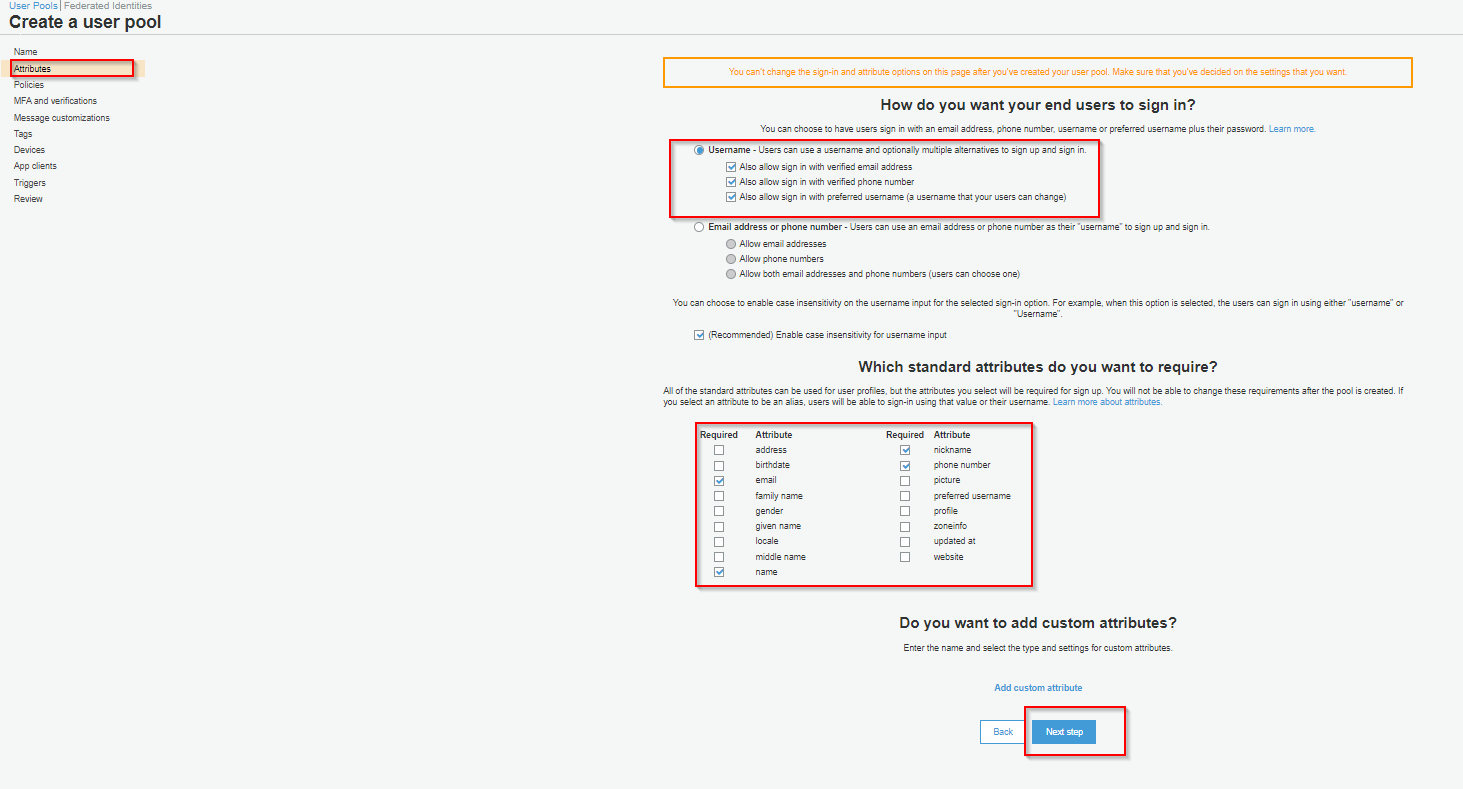
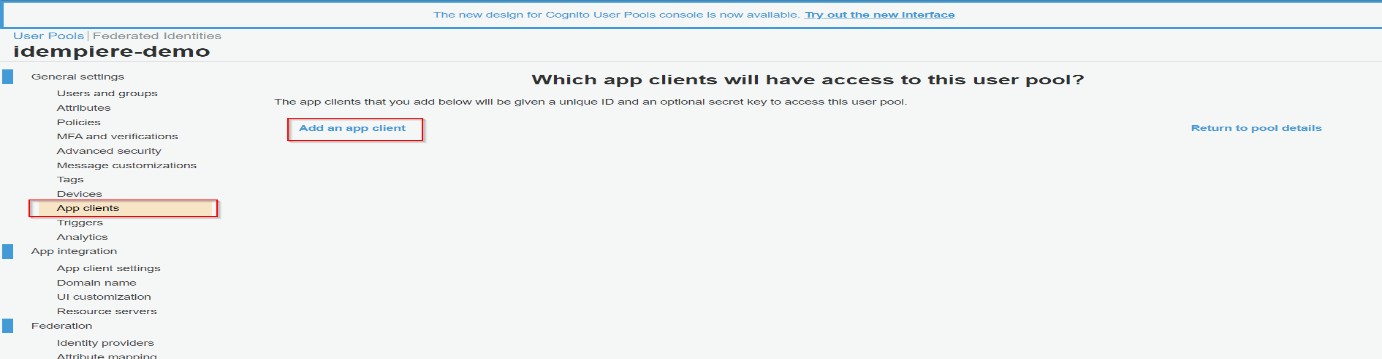
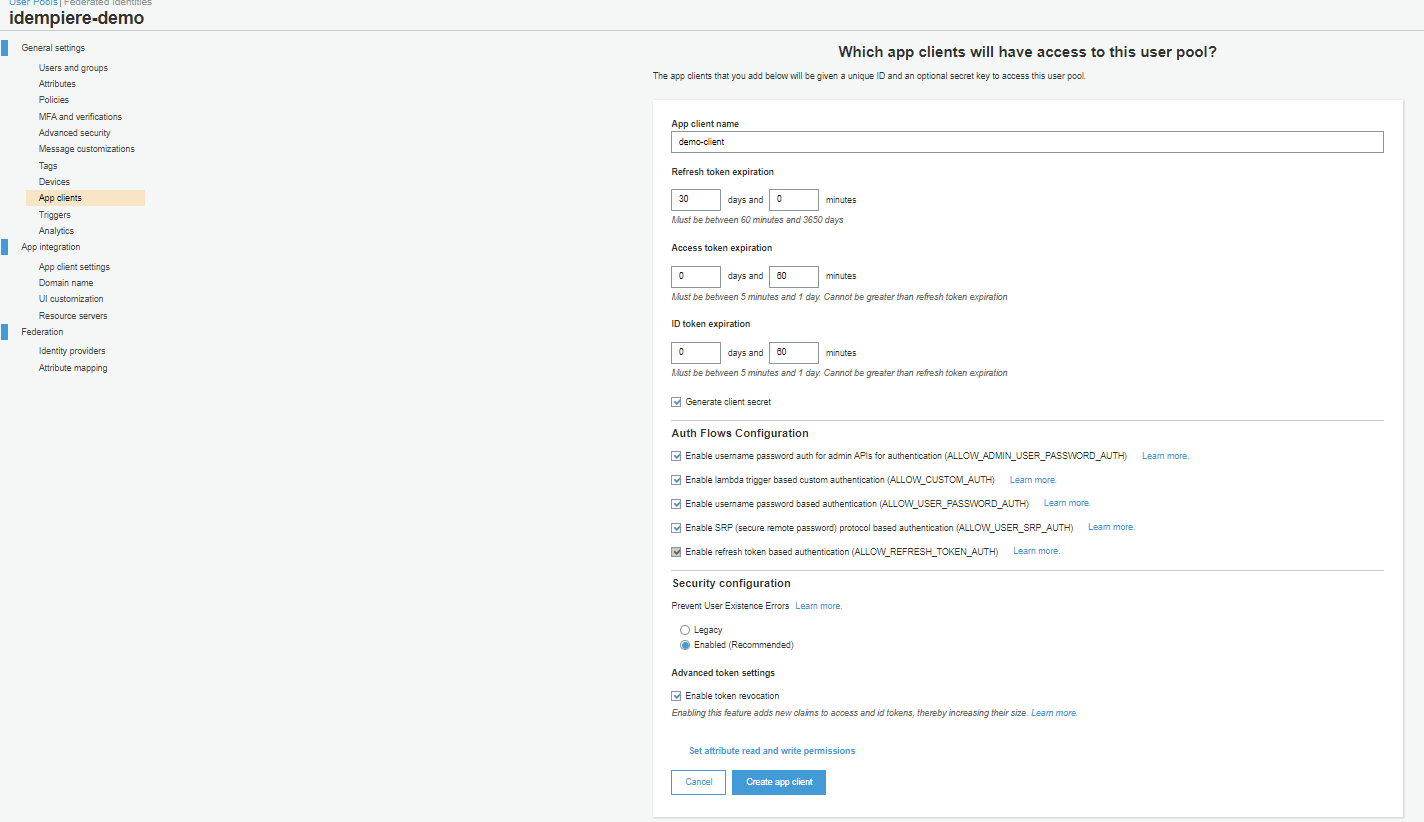
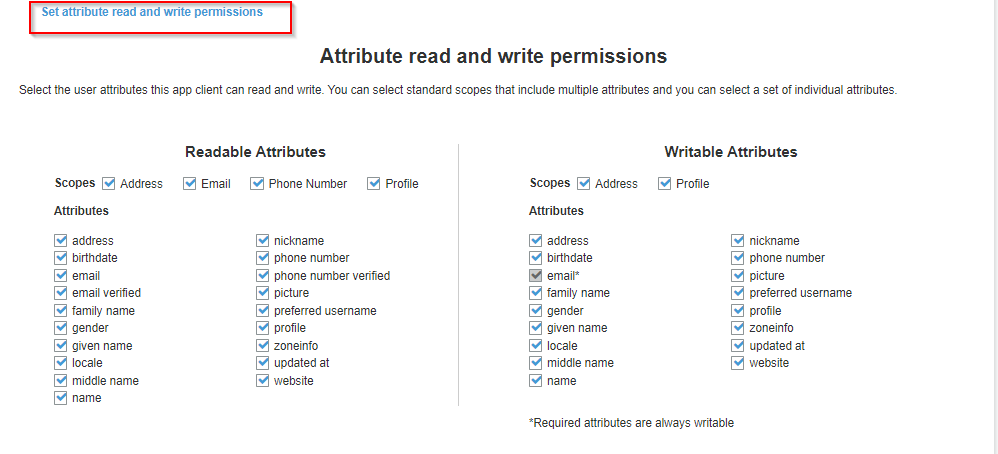
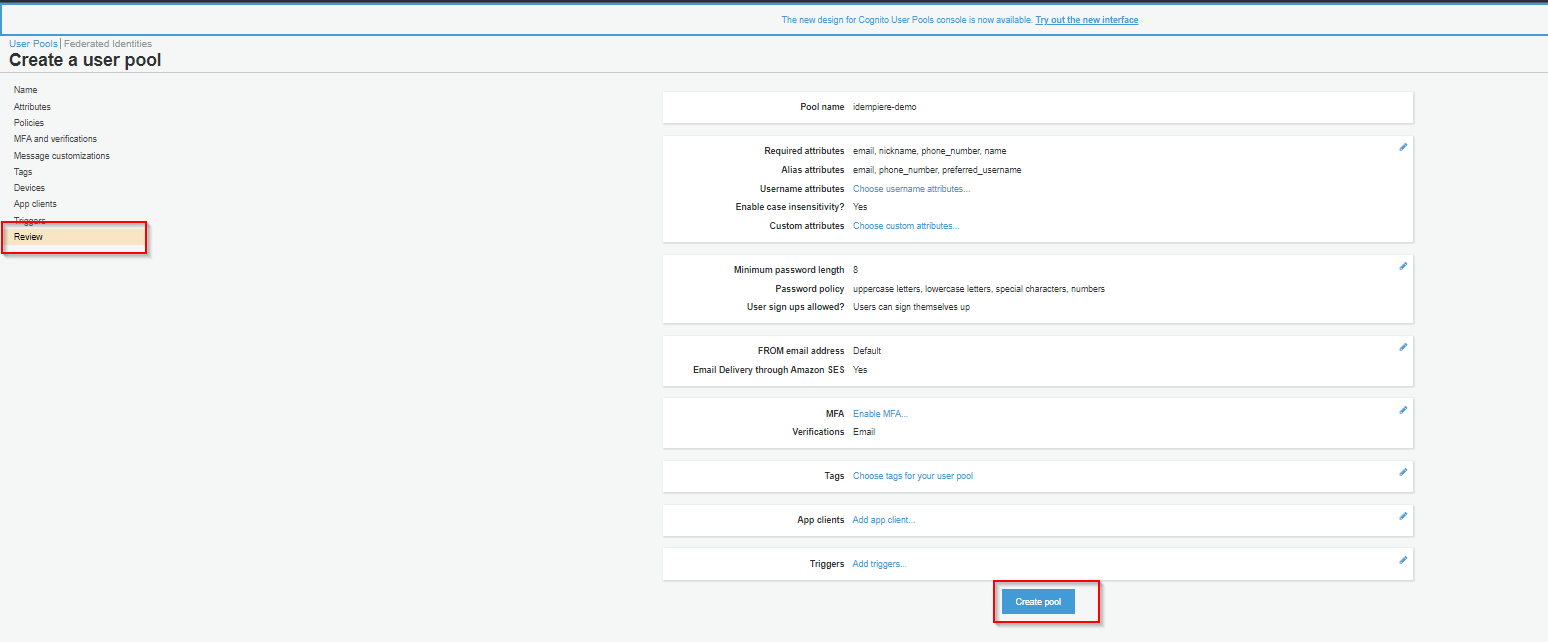
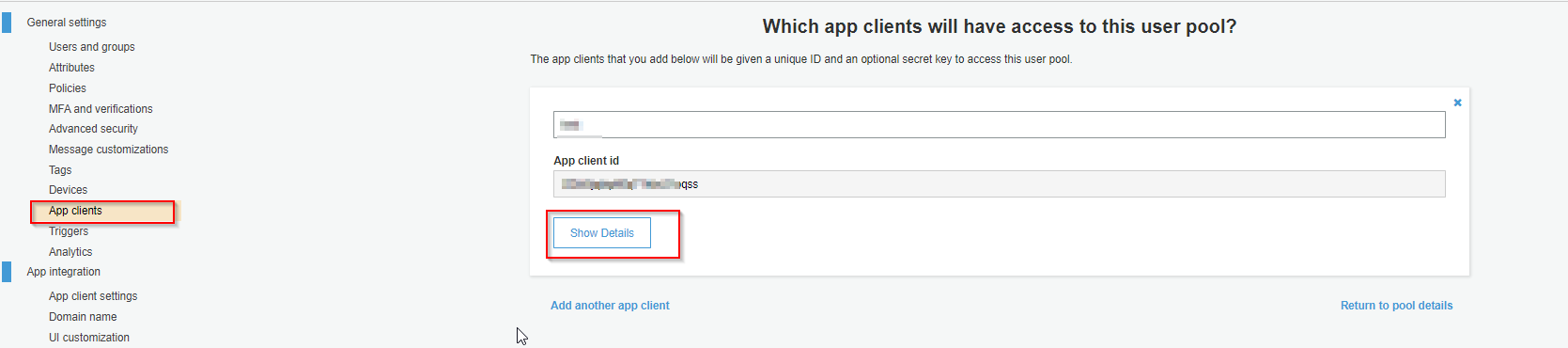
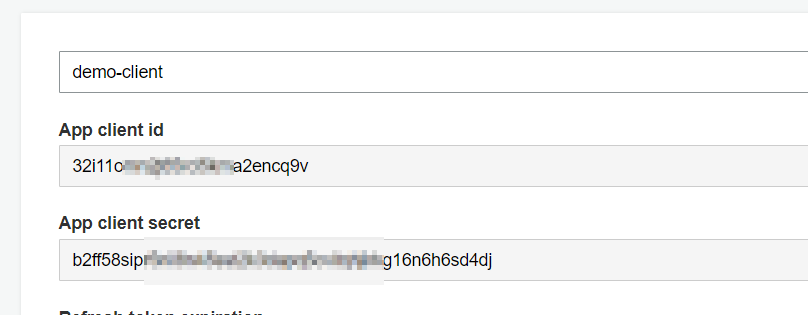
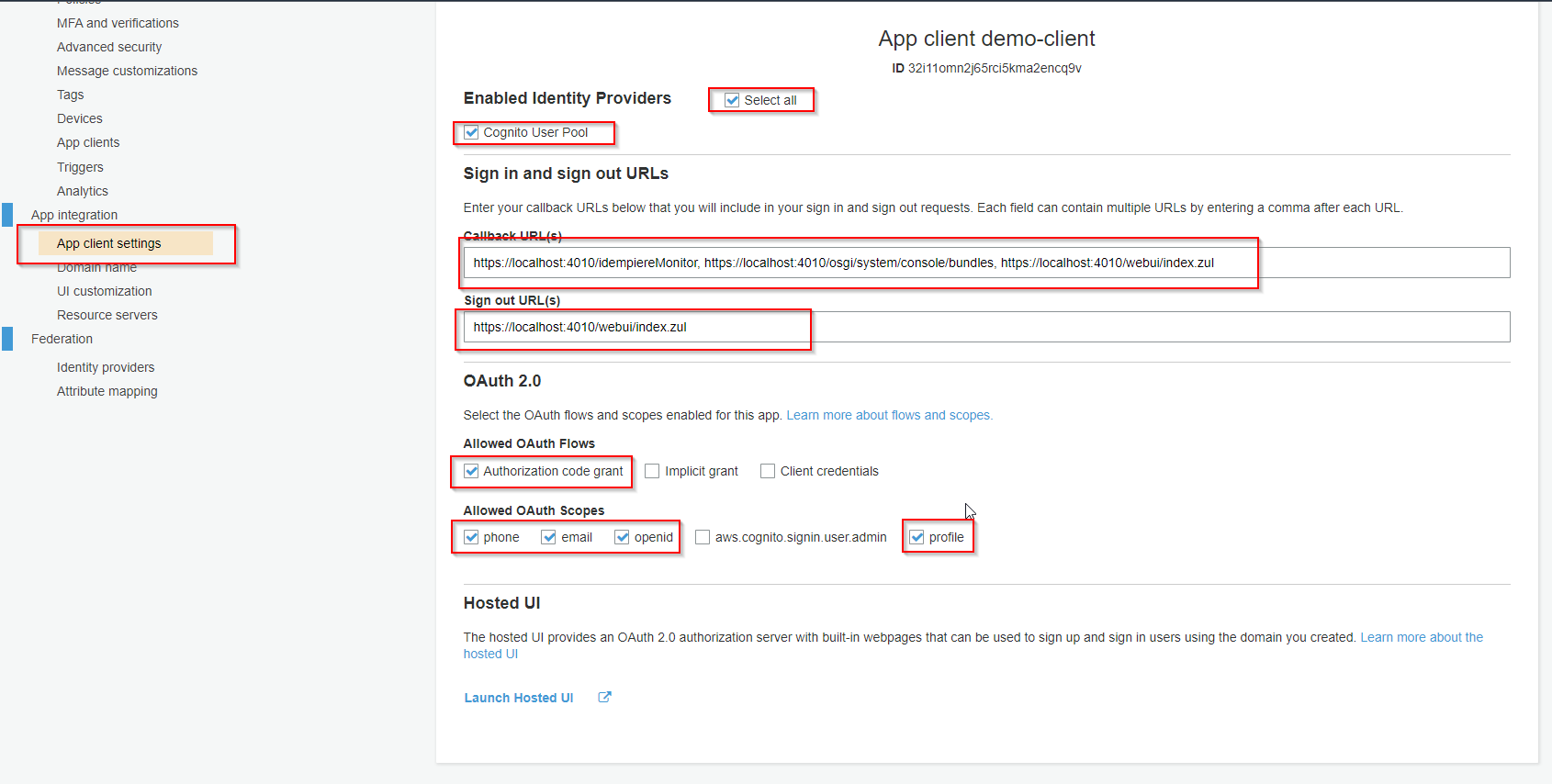
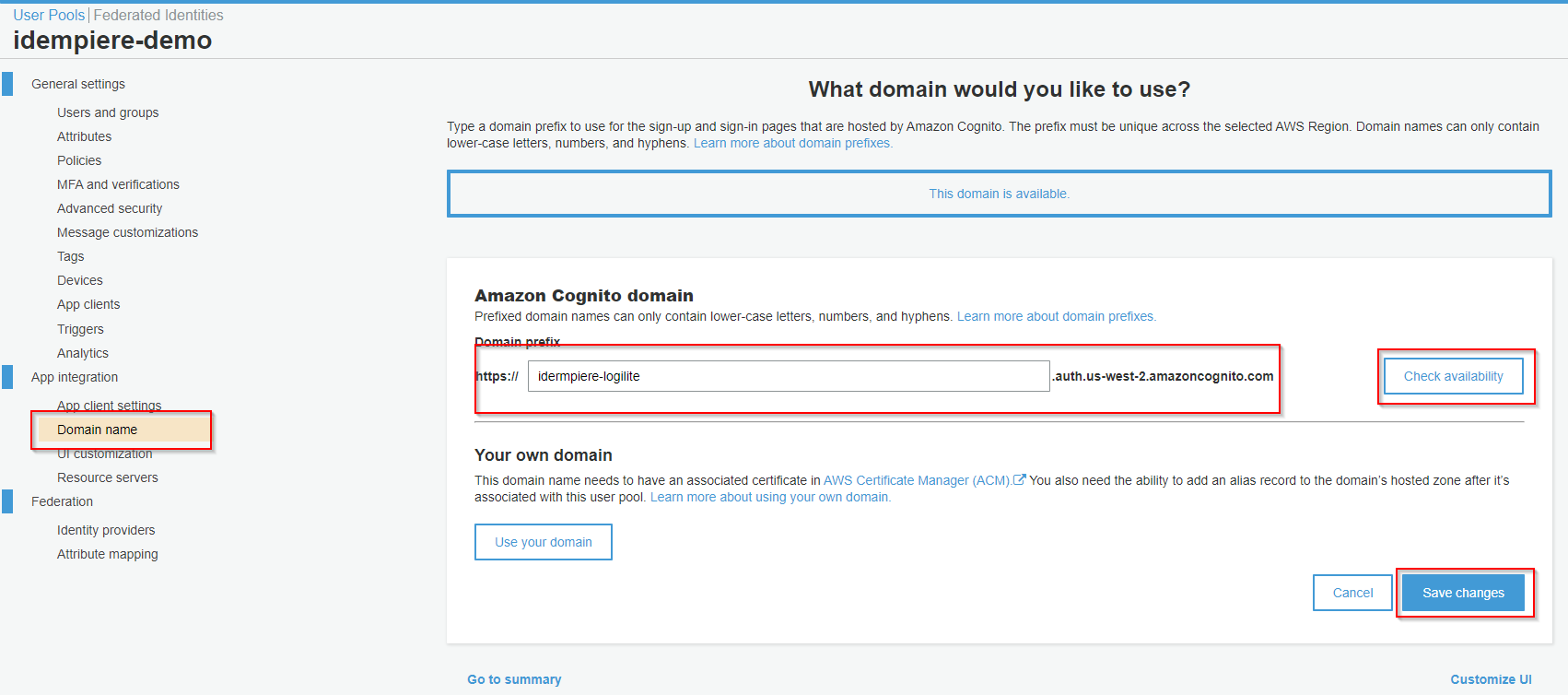
## SSO Amazon Cognito Configuration.

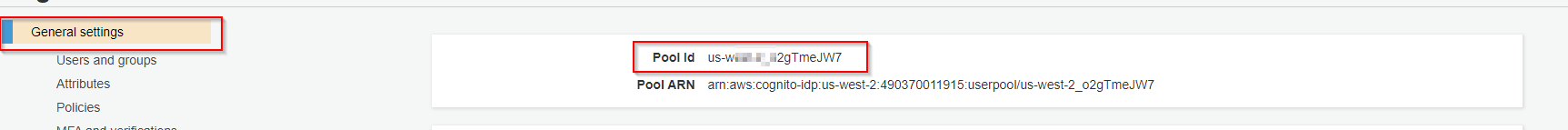
* 1. Log in to the [AWS portal](https://portal.aws.amazon.com/billing/signup) as an admin user.
  2. Search & Select “Cognito” service.
  3. Click on “**Manage User Pool**”
  4. Click Create User Pool
  5. Create a User pool (For More info check [here](https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-as-user-directory.html))
     + Pool Name: <Any\_Name>
     + Select “**Attribute**”
       - Select the Username flag and check all checkboxes below.
       - Select attributes like (email, name, phone number, etc.).
     + Select “**App Clients**”
       - Click “**Add an app client**” & fill the detail as below
         * App client name: <any\_name>
         * In Auth Flows Configuration select all flags
         * (Optional) Click on “**Set attribute read and write permissions**”

Currently we have selected all (Default)

* + - * + Click “**Create app clients**”
    - Select **Review** check all details & Click “**Create Pool”**
  1. After User Pool is create Click on “**App Clients**” (For more info check [here](https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-configuring-app-integration.html))
     + Click “**Show Details**”
     + Copy ‘**App client id**’
     + Copy ‘**App client secret**’
  2. App client settings
     + Please select below check box as shown in image
       - Select all
       - Cognito User Pool
       - Authorization code grant
       - Phone
       - Email
       - OpenID
       - Profile
     + Add iDempiere Monitor, Felix Web Console & , IDempiere Webui URLS comma separated in Callback URL(s)
       - Note:- It is recommended to provide HTTPS URL
       - Our iDempiere is running in localhost 4010



* 1. Domain name
     + Copy ‘**Amazon Cognito domain**’
       - E.g. “https://idermpiere-logilite.auth.us-west-2.amazoncognito.com”
  2. General setting
     + Copy ‘**Pool id**’



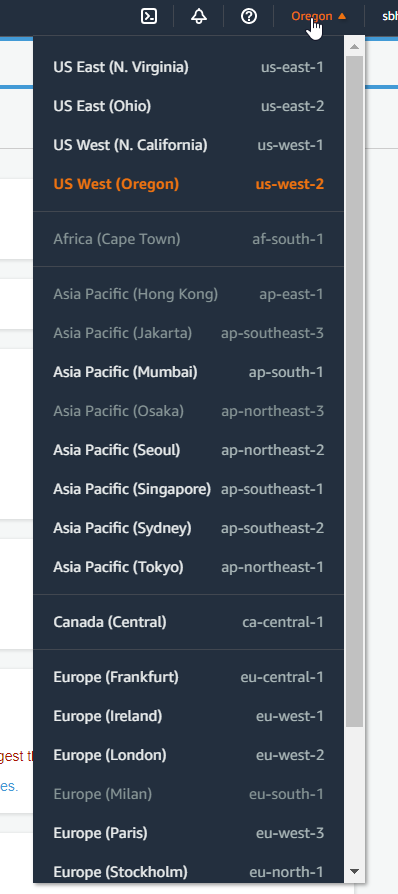
## Configuring Single Sign-On (SSO) in iDempiere.

1. **Log in as System User**

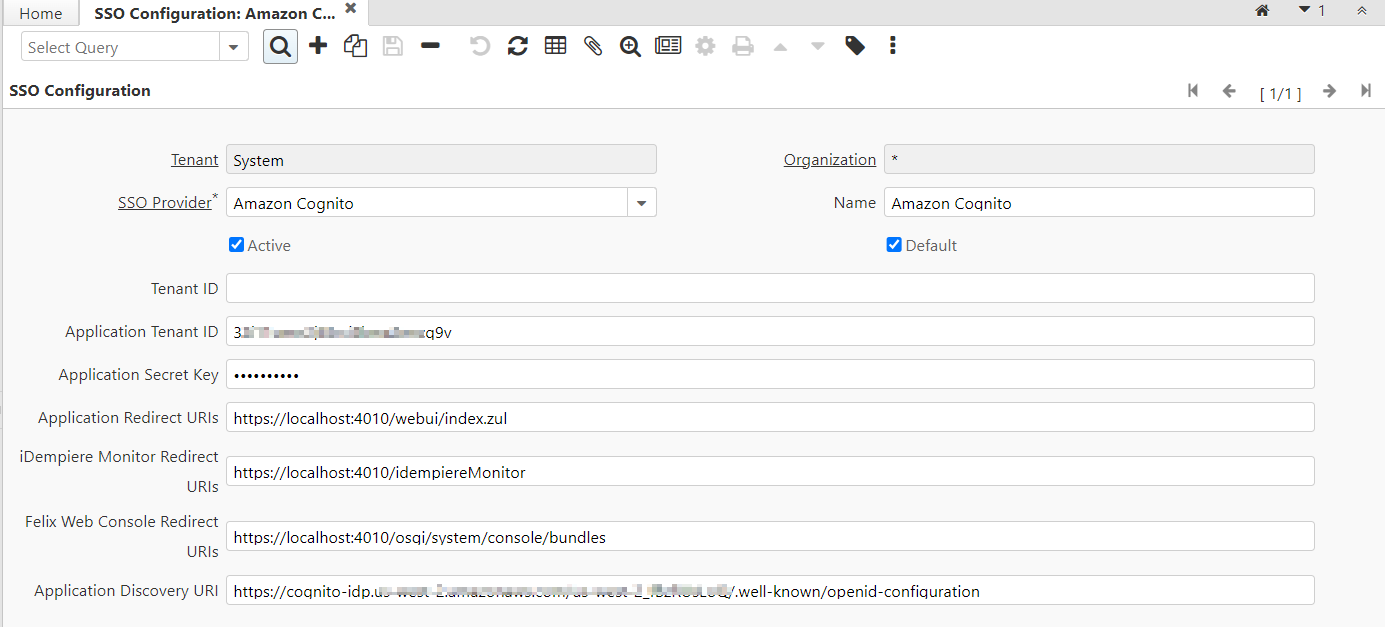
* Begin by logging into iDempiere with System User privileges.

1. **SSO Configuration**

* Open the "SSO Configuration" window.
* Provide the following details for Amazon Cognito as the SSO Provider:
* Fill in the following details:
* **SSO Provider:** Amazon Cognito as SSO Authenticator
* **Name:** "Logilite-demo" (You can choose any name, this is used as the AD App)
* **Application Client ID:** [Found in your app at User Pools > General Settings > App Clients > "App Client ID"]
* **Application Secret Key:** [Found in your app at User Pools > General Settings > App Clients > "App Client Secret"]
* **Application Redirect URIs:** [URL found in your app at User Pools > App Integration > App Clients Settings > "Callback URL(s)" > <https://your-idempiere-instance.com/webui/index.zul>]
* **iDempiere Monitor Redirect URIs:** [URL found in your app at User Pools > App Integration > App Clients Settings > "Callback URL(s)" > <https://your-idempiere-instance.com/idempiereMonitor>]
  + - * **Felix Web Console Redirect URIs:** [URL found in your app at User Pools > App Integration > App Clients Settings > "Callback URL(s)" > <https://your-idempiere-instance.com/osgi/system/console/bundles>]
        + **Note**: It is recommended to provide HTTPS URLs
      * **Application Discovery URI**: [https://cognito-idp.Region.amazonaws.com/User Pool ID/.well-known/openid-configuration]
        + Region: [Click "Oregon" to find your Region]
        + Pool ID: [Found in your app at User Pools > General Settings > "User Pool ID"]

****

* + - * **Default:** True (Indicates that the current config is used for SSO login)
    - Note: Only one SSO configuration can be set as default at a time.



1. **Enabling SSO**

* Open the "System Configurator" window.
* Search for **ENABLE\_SSO**.
* Set **Configured Value** to Y/N (default is N).
* If **ENABLE\_SSO = Y**, the SSO login page will be displayed.
* If **ENABLE\_SSO = N**, the iDempiere default login page will be shown.

1. **Enabling SSO for iDempiere Monitor**

* Search for **ENABLE\_SSO\_IDEMPIERE\_MONITOR** in the "System Configurator" window.
* Set **Configured Value** to Y/N (default is N).
* If **ENABLE\_SSO = Y**, the SSO login page will be shown for iDempiere Monitor.
* If **ENABLE\_SSO = N**, the iDempiere default login page will be displayed.

1. **Enabling SSO for Felix Web Console**

* Search for **ENABLE\_SSO\_OSGI\_CONSOLE** in the "System Configurator" window.
* Set **Configured Value** to Y/N (default is N).
* If **ENABLE\_SSO = Y**, the SSO login page will be shown for Felix Web Console.
* If **ENABLE\_SSO = N**, the iDempiere default login page will be displayed.

1. **Using Email for Login Validation** (Optional)

* Search for **USE\_EMAIL\_FOR\_LOGIN** in the "System Configurator" window.
* Set **Configured Value** to Y/N (default is N).
* If **USE\_EMAIL\_FOR\_LOGIN = Y**, use email for login validation.
* If **USE\_EMAIL\_FOR\_LOGIN = N**, use display name for login validation.

1. **Role Selection when Logging in with SSO** (Optional)

* Search for **SSO\_SELECT\_ROLE** in the "System Configurator" window.
* Set **Configured Value** to Y/N (default is N).
* If **SSO\_SELECT\_ROLE = Y**, the Role Panel will be shown when logging in with SSO for single Client & role.
* If **SSO\_SELECT\_ROLE = N**, the Role Panel will not be shown when logging in with SSO for single Client & role.

## **Using /admin for Web Login with SSO Enabled**

When Single Sign-On (SSO) is enabled in iDempiere, you have the option to access the default login page using the /webui/admin route. This allows for web-based authentication even when SSO is in effect.

**Prerequisites**

* Ensure that SSO is configured and enabled in your iDempiere instance.
* The **ENABLE\_SSO** configuration parameter must be set to **Y**.

**Accessing the Login Page**

* Open your web browser and enter the URL of your iDempiere instance.
* For example: **https://your-idempiere-instance.com/webui/admin**
* You will be directed to the default login page of iDempiere.

**Important Note**

* This feature is designed to provide a fallback option for web-based login in case SSO is enabled.
* The **/webui/admin** route will only function when the **ENABLE\_SSO** configuration parameter is set to **Y**.