ORACLE

APPLICATION EXPRESS



Oracle Application Express: Developing Database Web Applications

Hands-On-Labs Guide

Unit 13: Implementing Security in your Application

Application security is very important in the majority of applications, except for "Public" applications. You must ensure users enter valid credentials, generally username and password (Authentication), and that once logged in that each user has appropriate rights within the application (Authorization).

This exercise includes three hands-on-labs.

HOL 13-1 uses the Demo Projects application.
HOL 13-2 and 13-3 use the Budget App application.

HOL 13-1 Creating and Using an Authorization Scheme: In this lab, you create an authorization scheme to ensure only people entered as Team Members can log into the Demo Projects application. You create a user and verify if the user can access the application.

HOL 13-2 Creating and Using an Authentication Scheme: In this hands-on lab, you create an Open Door Credentials authentication scheme and make it current. You test the authentication scheme and then switch back to the default Application Express Authentication scheme.

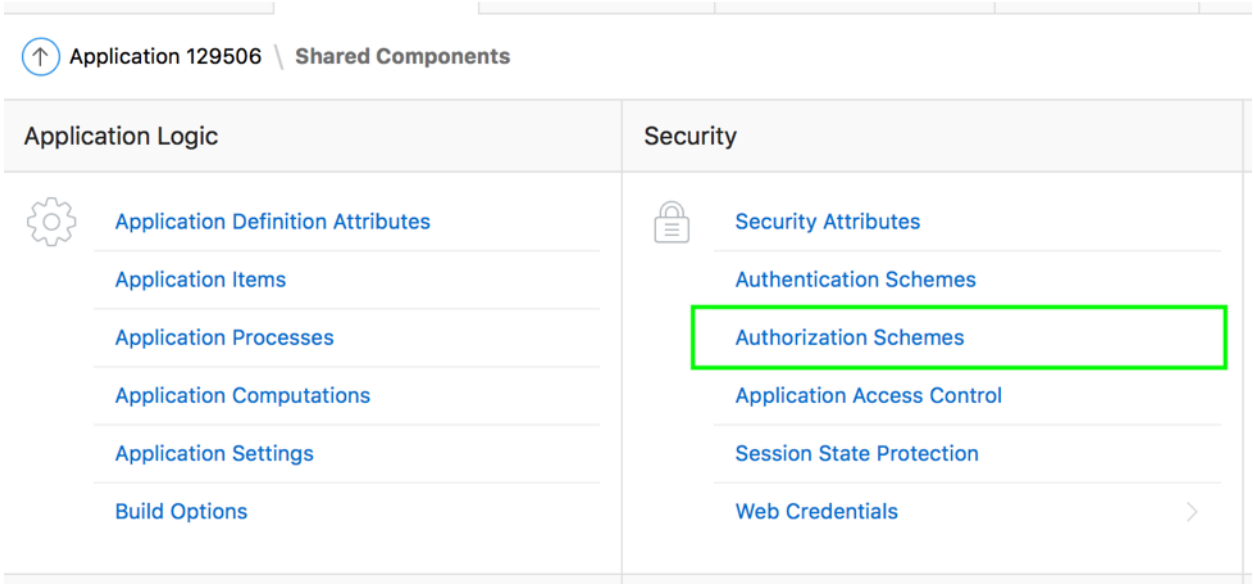
HOL 13-3 Controlling User Access by Using the Access Control Administration: In this hands-on lab you create three different users as Administrator, Developer and End User. You create an Access Control Administration page, set the application mode to restrict access and add these users to the Access Control list. Finally, you apply the authorization scheme to pages and verify if users are allowed or denied access.

HOL 13-1: Creating and Using an Authorization Scheme

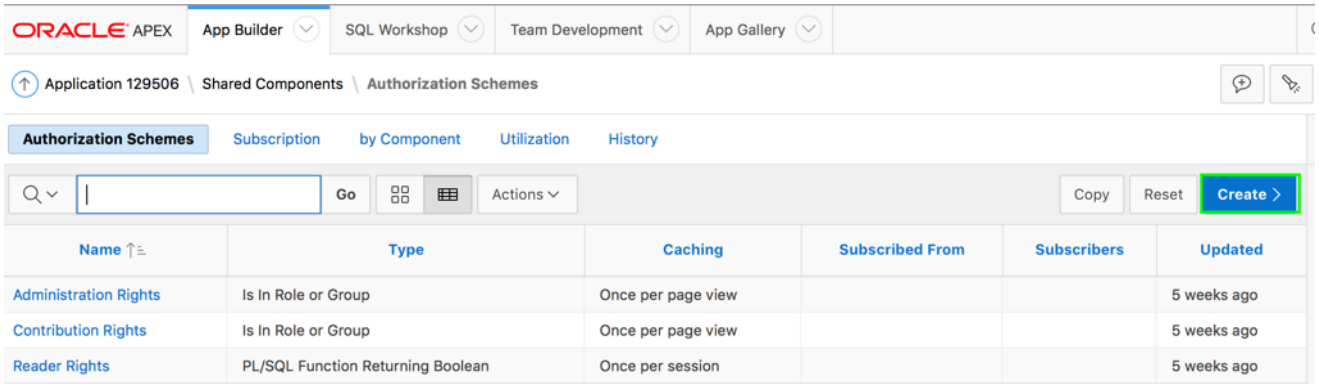
In this hands-on lab, you create an authorization scheme to ensure only people entered as Team Members can log into the Demo Projects application. You apply the authorization scheme to the application properties.

1. Navigate to **App Builder** and run the **Demo Projects** application.
   In the Developer Toolbar, click **Application <*n*>**.

2. In the application home page, click **Shared Components**.
   Under Shared Components > Security, click **Authorization Schemes**.



3. Click **Create**.



4. For Create Authorization Scheme, select **From Scratch and** click **Next**.

5. For Details, input the following:
   - Name - enter **Team Members**
   - Scheme Type - select **Exists SQL Query**

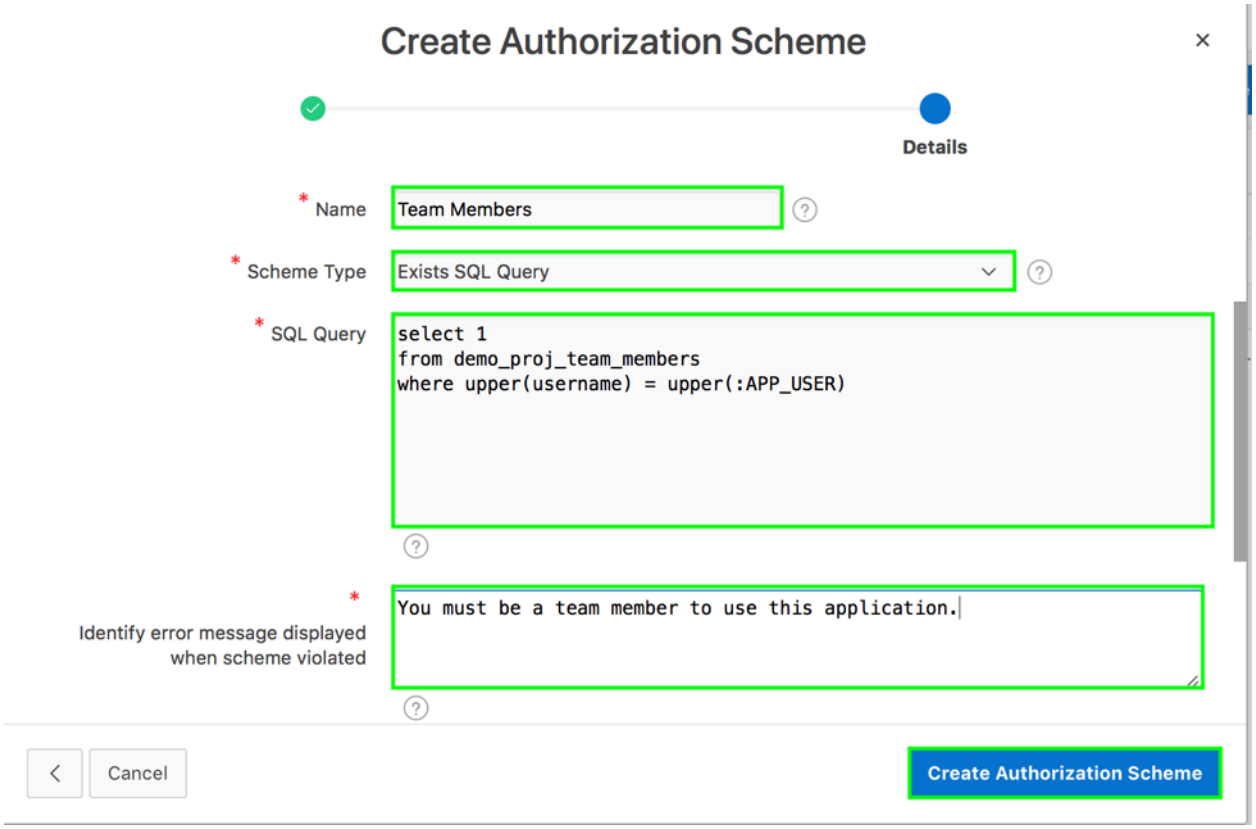
- SQL Query - copy and paste the following:

```
select 1
from demo_proj_team_members
where upper(username) = upper(:APP_USER)
```

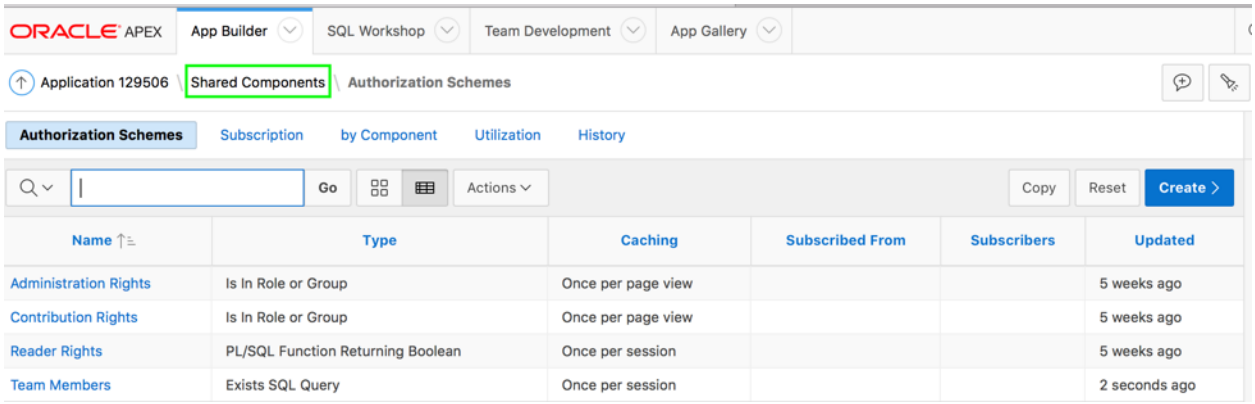
- Identify error message displayed when scheme violated - enter **You must be a team member to use this application**.

Click **Create Authorization Scheme**.

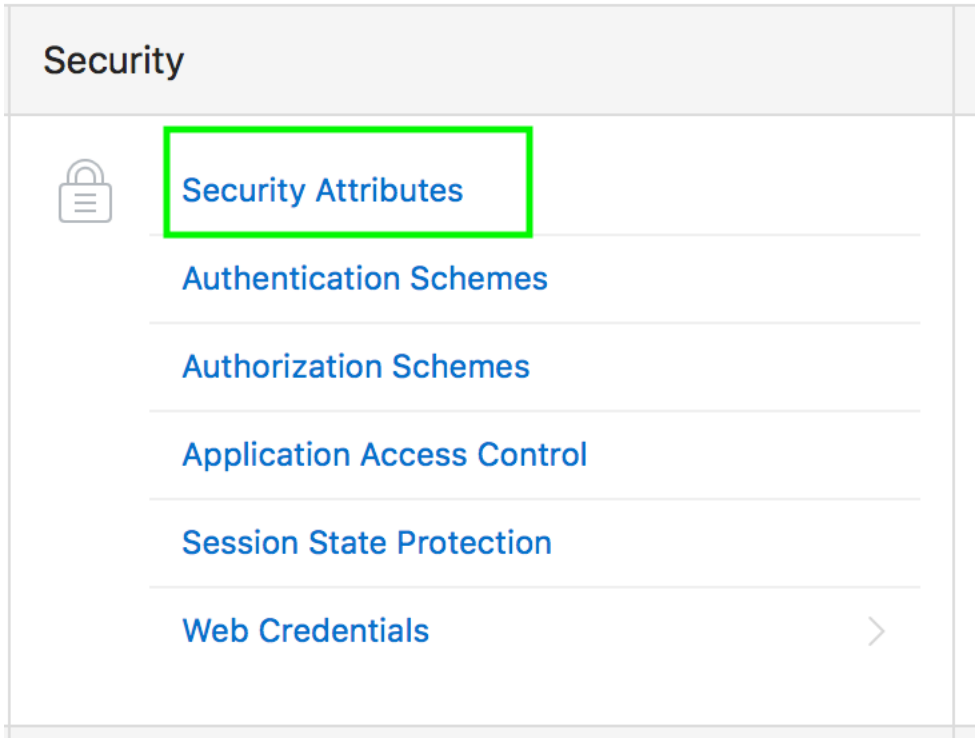
Note: **`:APP_USER`** is a built-in application item that returns the username of the currently logged in user.



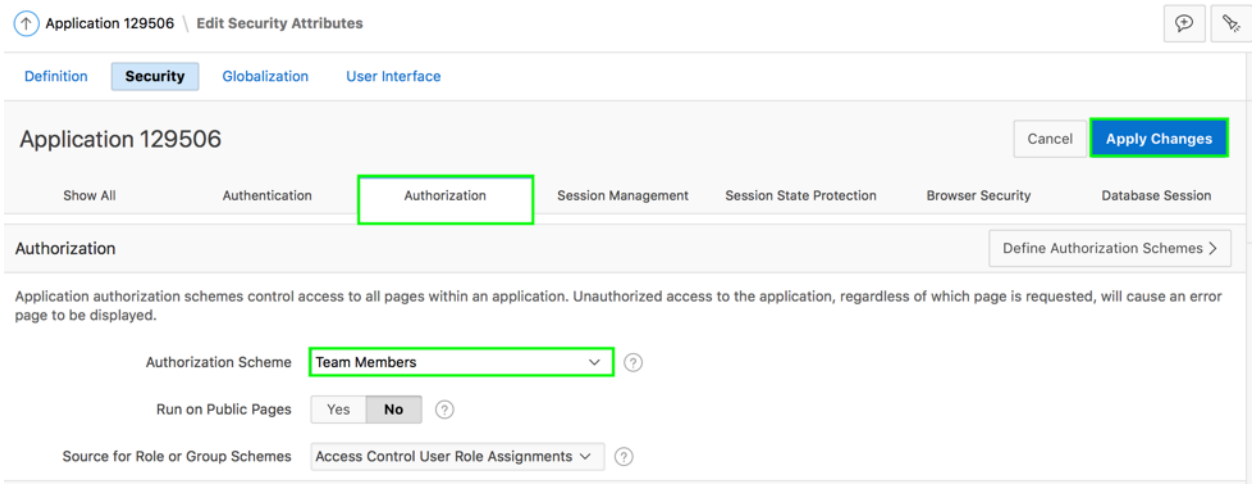
6. The Team Members authorization scheme is created now.
   Rather than applying the authorization scheme to every page, apply the scheme to the application properties.
   Click the **Shared Components** breadcrumb entry.
   Alternatively, on the toolbar, click the Shared Components button, which is located in the top-right and contains a triangle, circle, and square in its icon.



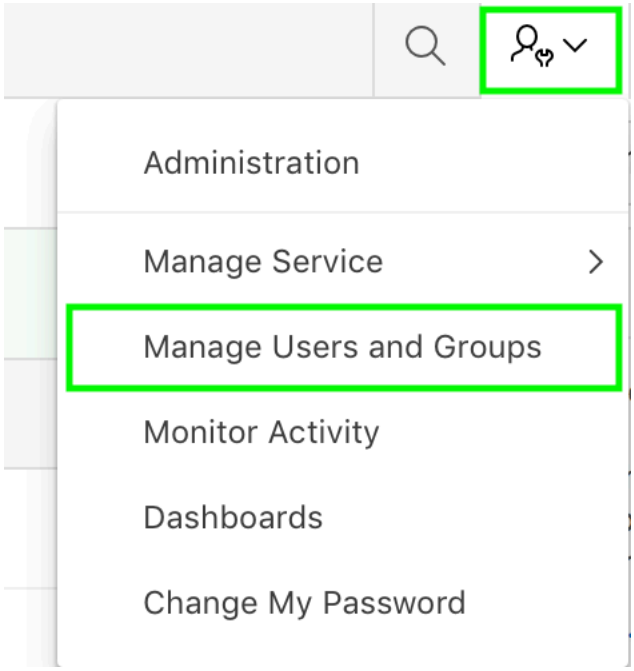
7. Under Security, click **Security Attributes**.



8. Click the **Authorization** tab.
   For Authorization Scheme, select **Team Members** from the list.
   Click **Apply Changes**.

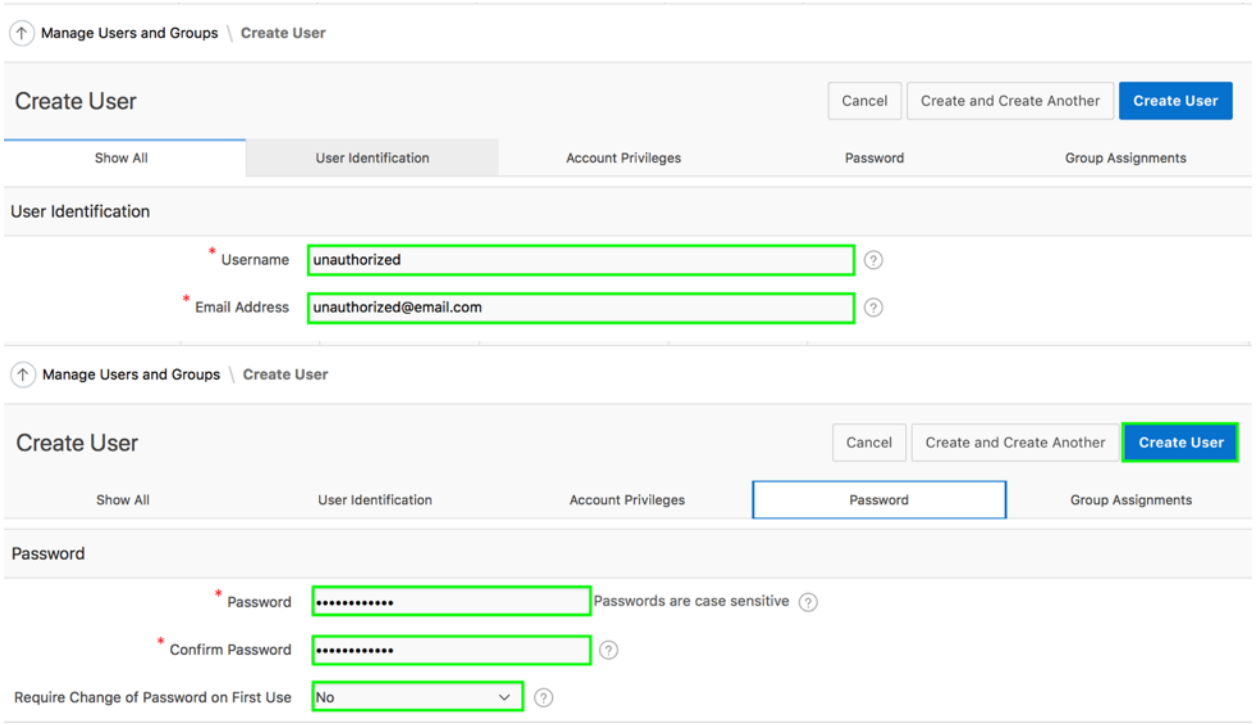


9. In order to test the authorization scheme it is necessary to create a new user account. In the Application Express toolbar, click **Administration**, identified by a user icon with a spanner, then select **Manage Users and Groups**.



10. Click **Create User**.
    To create a user, input the following:
    - Username - enter unauthorized
    - Email Address - enter unauthorized@email.com
    - Password - enter unauthorized
    - Confirm Password - enter unauthorized
    - Require Change of Password on First Use - No

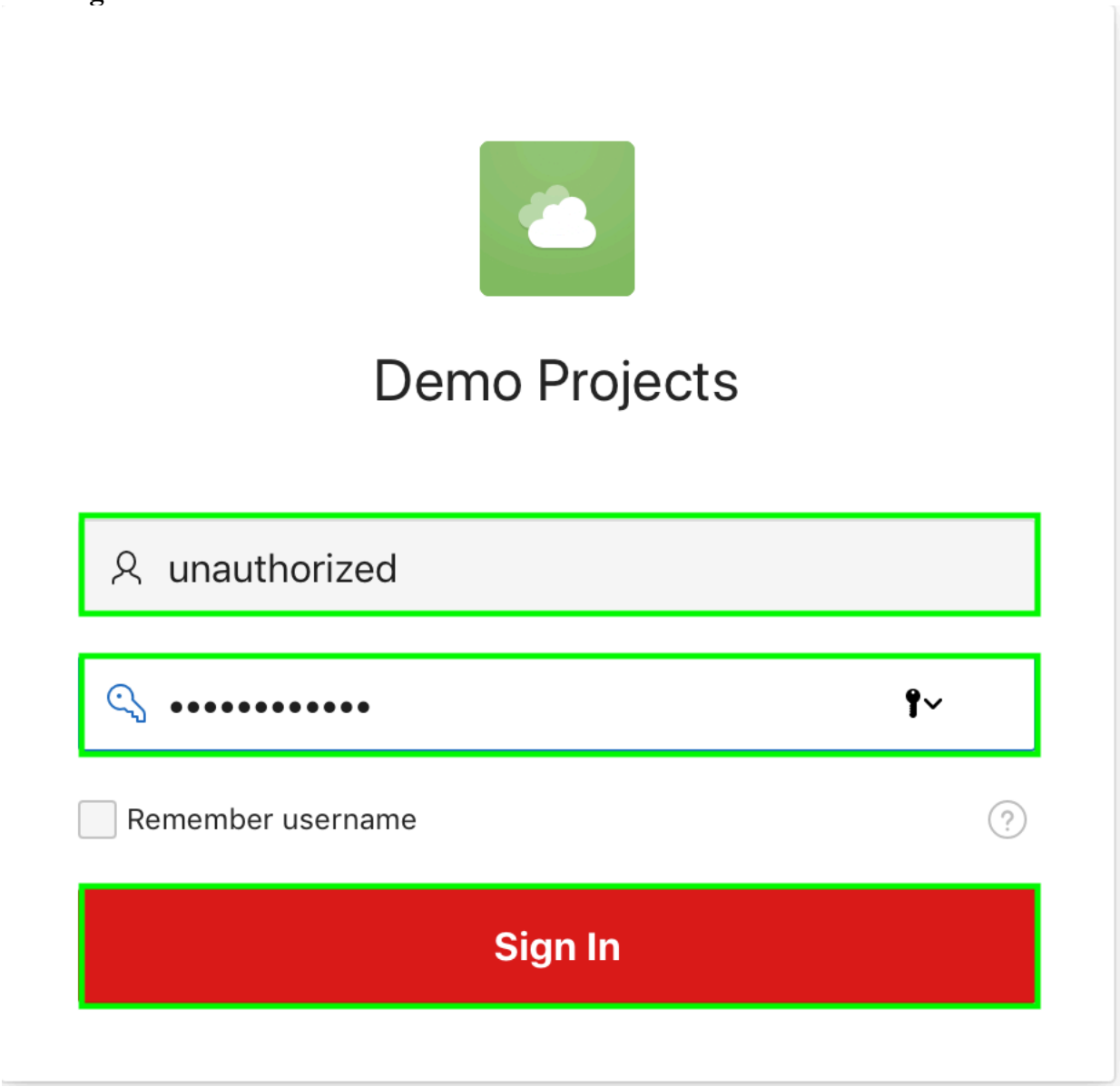
Click **Create User**.



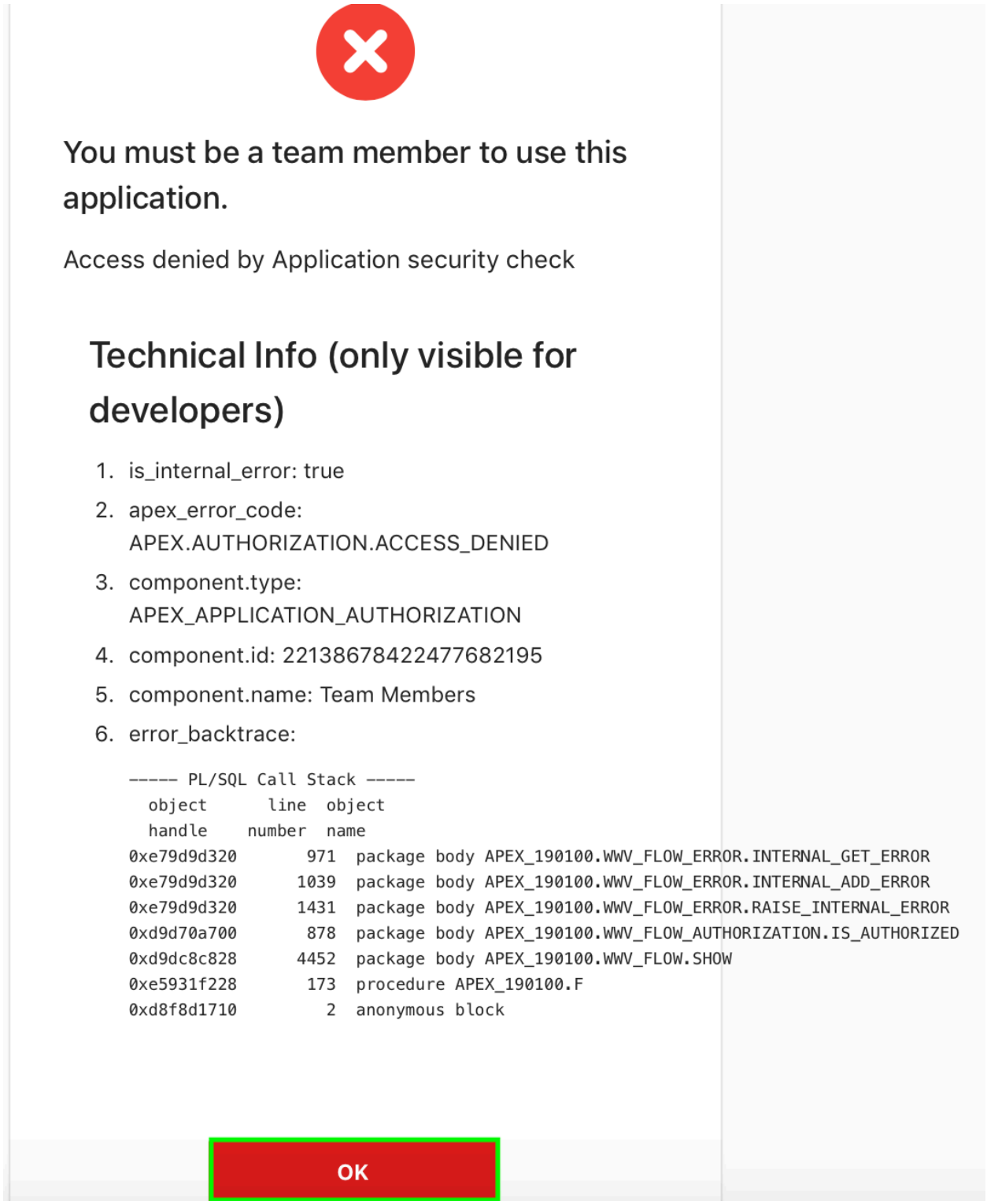
11. Navigate to the runtime environment (tab or window). Click **Sign Out** in the navigation bar (top left).

12. On the Log In page, for Username enter **unauthorized**, and for Password enter **unauthorized**.

Click **Sign In**.



13. Verify the access denied message is displayed.
Click **OK**.



You must be a team member to use this application.

Access denied by Application security check

Technical Info (only visible for developers)

1. is_internal_error: true
2. apex_error_code: APEX.AUTHORIZATION.ACCESS_DENIED
3. component.type: APEX_APPLICATION_AUTHORIZATION
4. component.id: 22138678422477682195
5. component.name: Team Members
6. error_backtrace:

```
----- PL/SQL Call Stack -----
  object      line  object
  handle    number  name
0xe79d9d320       971  package body APEX_190100.WWV_FLOW_ERROR.INTERNAL_GET_ERROR
0xe79d9d320      1039  package body APEX_190100.WWV_FLOW_ERROR.INTERNAL_ADD_ERROR
0xe79d9d320      1431  package body APEX_190100.WWV_FLOW_ERROR.RAISE_INTERNAL_ERROR
0xd9d70a700       878  package body APEX_190100.WWV_FLOW_AUTHORIZATION.IS_AUTHORIZED
0xd9dc8c828      4452  package body APEX_190100.WWV_FLOW.SHOW
0xe5931f228       173  procedure APEX_190100.F
0xd8f8d1710         2  anonymous block
```

OK

14. On the Log In page, enter your username and password credentials that you use to log into the App Builder.
    Click **Log In**.

HOL 13-2: Creating and Using an Authentication Scheme

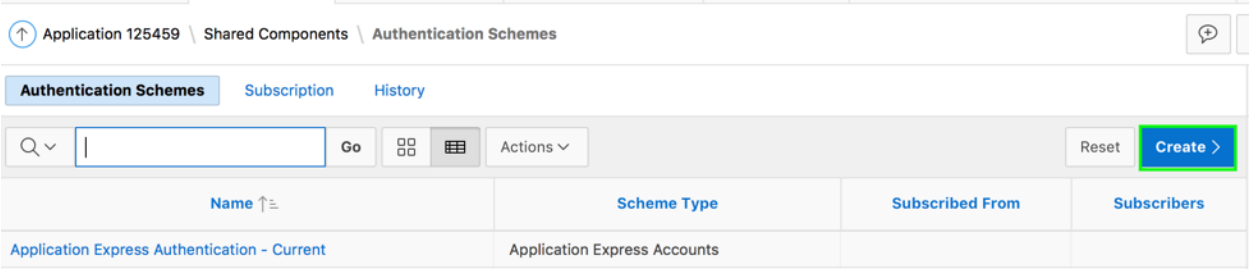
In this hands-on lab, you create an authentication scheme named Open Door Credentials in the Budget App application. Upon creation, this scheme becomes Current Scheme by default. You test this scheme by logging in to the application. Finally, you switch back to Application Express Authentication scheme.

1. In the App Builder, click **Budget App** application.

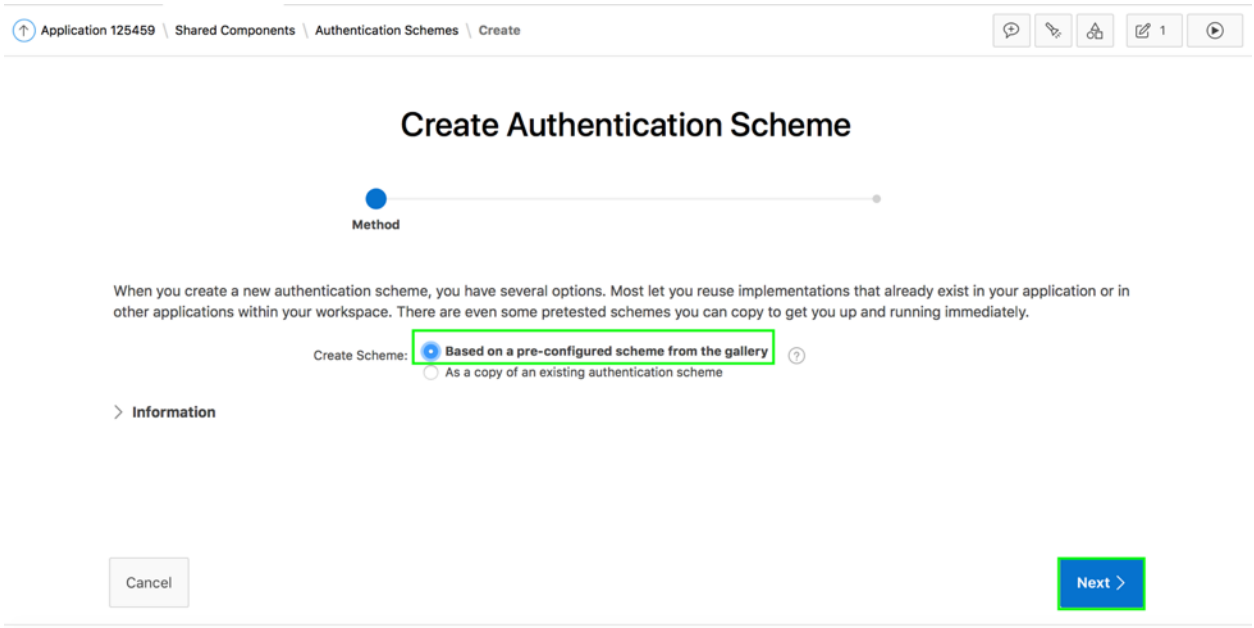
2. Navigate to **Shared Components**.
   Under Security, click **Authentication Schemes**.



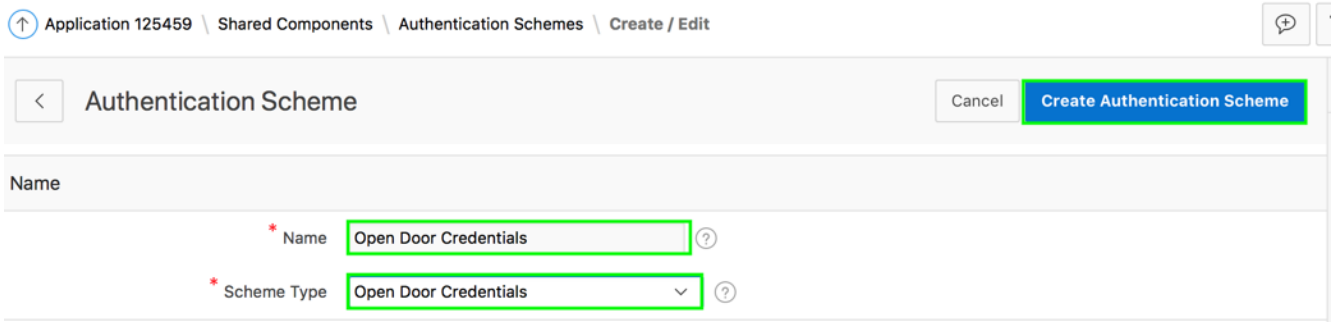
3. You want to create an authentication scheme. Click **Create**.



4. For Create Scheme, select **Based on a pre-configured scheme from the gallery**, and click **Next**.

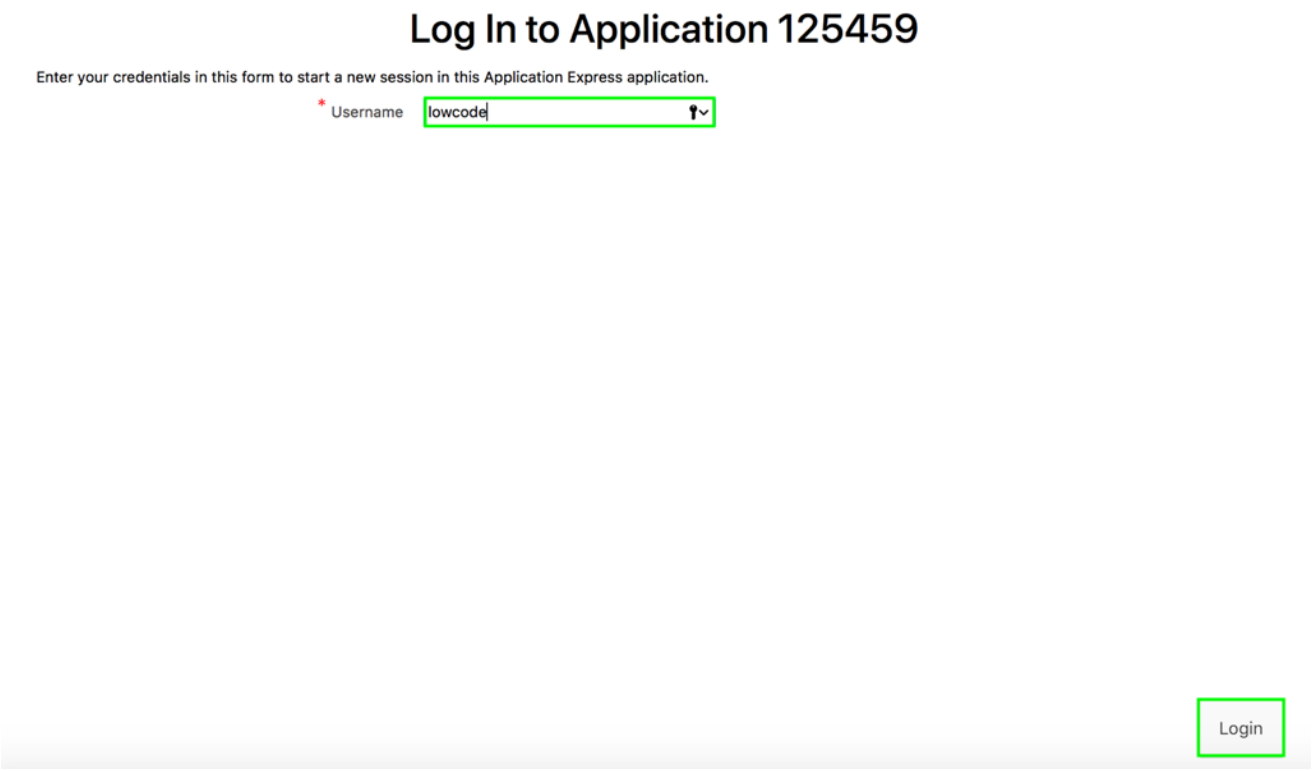


5. For Name, enter **Open Door Credentials**.
   For Scheme Type, select **Open Door Credentials** from the list.
   Click **Create Authentication Scheme**.

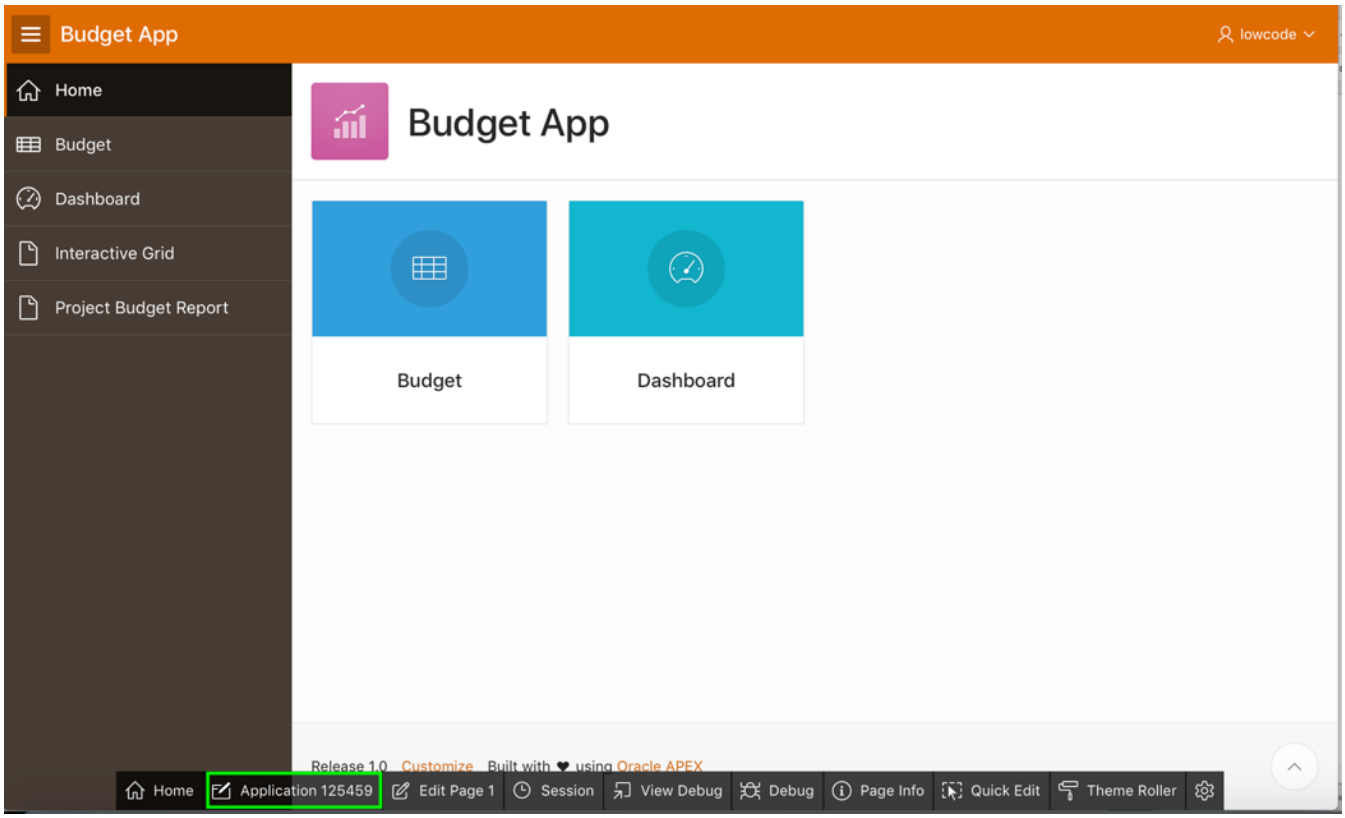


6. In the toolbar, click the **Run Page** icon.
   If you are already logged in, then click Sign Out to perform the next step.

7. Enter your Username and click **Login**.



8. The Home page is displayed.
   In the Developer Toolbar, click **Application<*n*>**.

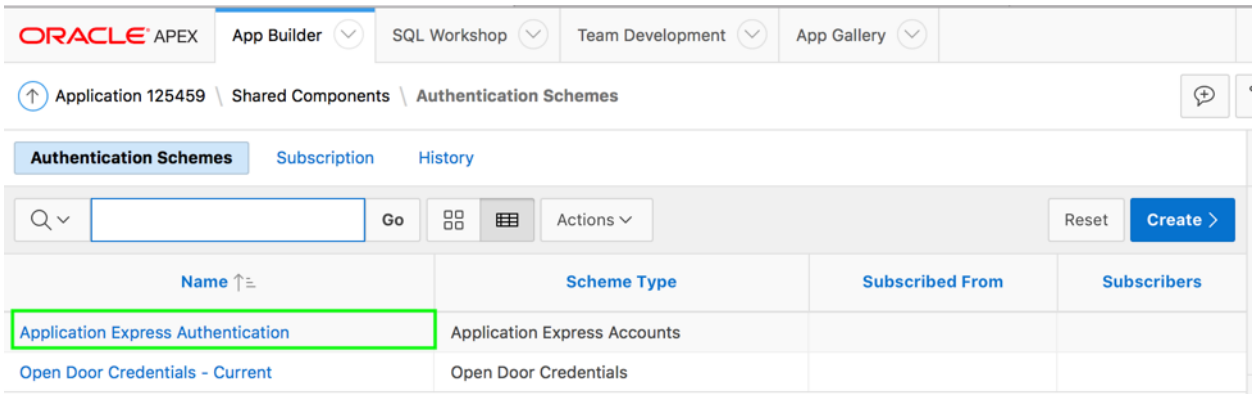


Your application might display the Vita (Copy) Theme Style. Click the **Customize** link at the bottom of the page, select **Vita** for Theme Style and click **Apply Changes**.

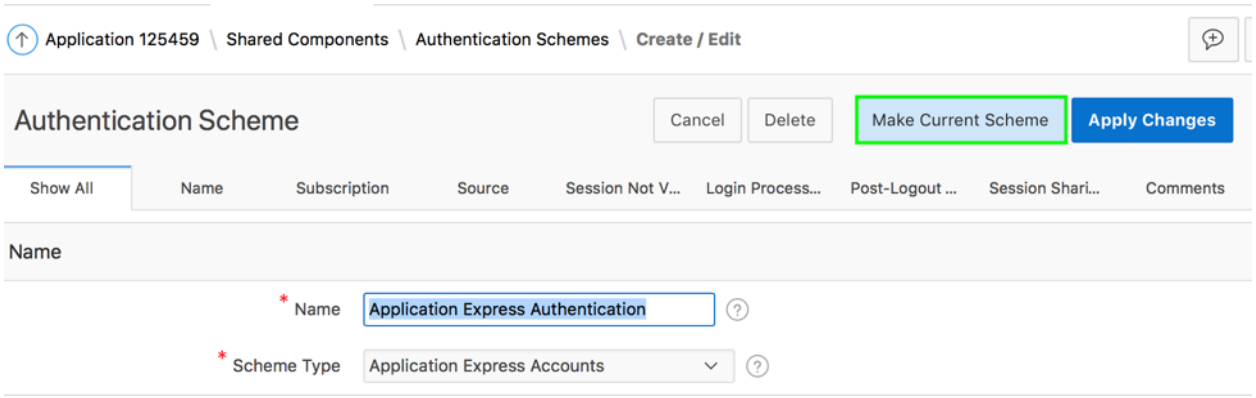
9. You want to switch back to the Application Express Authentication scheme. In the application home page, click **Shared Components**.

10. Under Security, click **Authentication Schemes**.

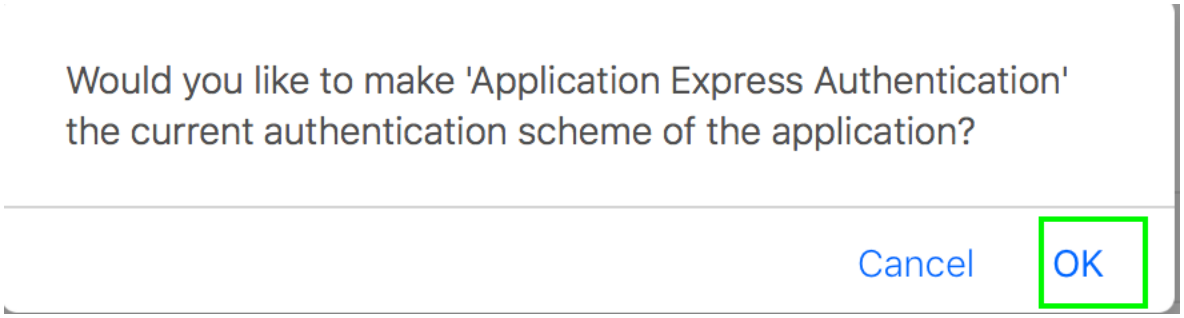
11. Click **Application Express Authentication** in the report.



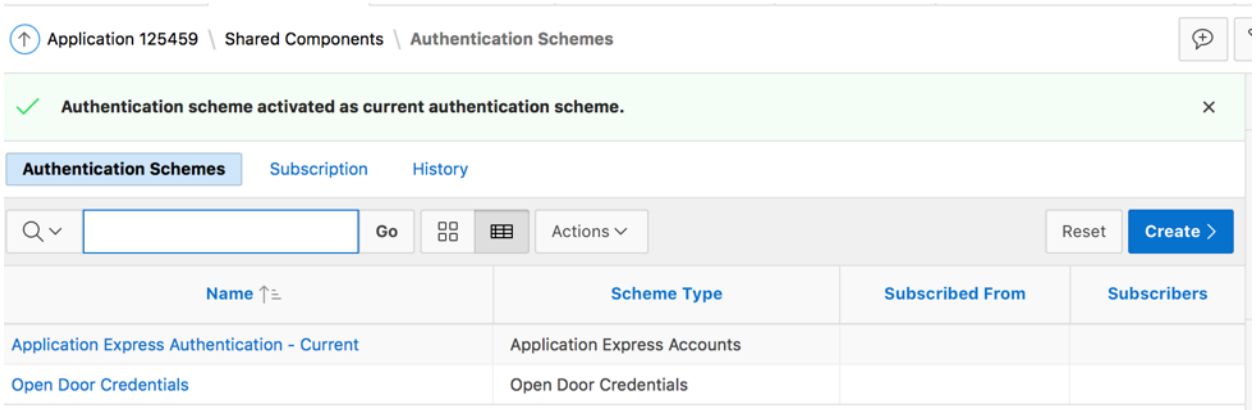
12. Click **Make Current Scheme**.



13. Click **OK**.



14. The Application Express Authentication scheme is now activated as current authentication scheme.



15. In the toolbar, click the **Run Page** icon. Then, click **Sign Out**.

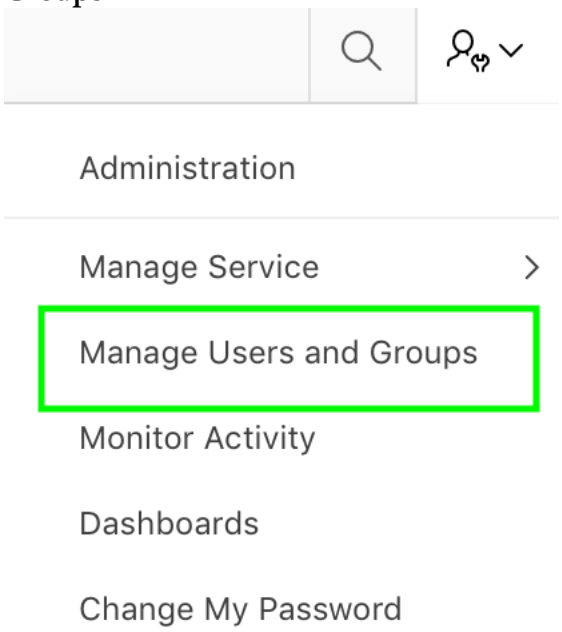
16. Notice that the authentication scheme has changed. Enter your username and password and click **Sign In**.

HOL 13-3: Controlling User Access by Using the Access Control Administration

In this hands-on lab, you first create an access control page and set the application mode to restrict access. Then, you create the access control list and assign the Budget App application components to an authorization scheme.

1. If you are in the application runtime environment, switch to the window or tab for App Builder environment.

2. In the Application Express toolbar, click **Administration** and select **Manage Users and Groups**.

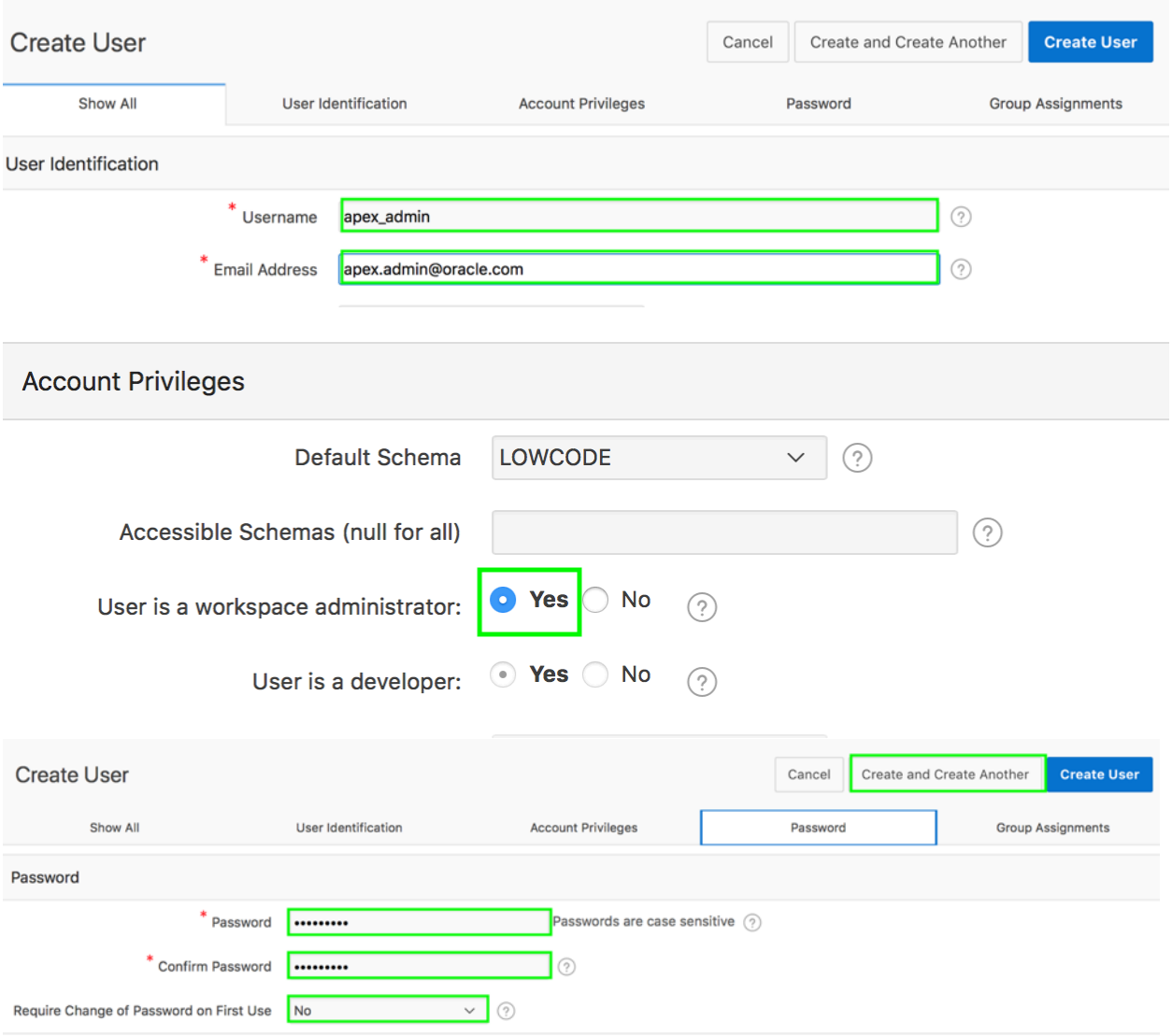


3. Create the following users to add to the Access Control List.
   - apex_admin: Workspace Administrator
   - apex_dev: Developer
   - apex_user: End User

   Click **Create User**.

4. Enter the following information and click **Create and Create Another**.
   - Username: **apex_admin**
   - Email Address: **apex.admin@oracle.com**
   - Select **Yes** for User is a workspace administrator
   - Password: **apexadmin123$**
   - Confirm Password: **apexadmin123$**

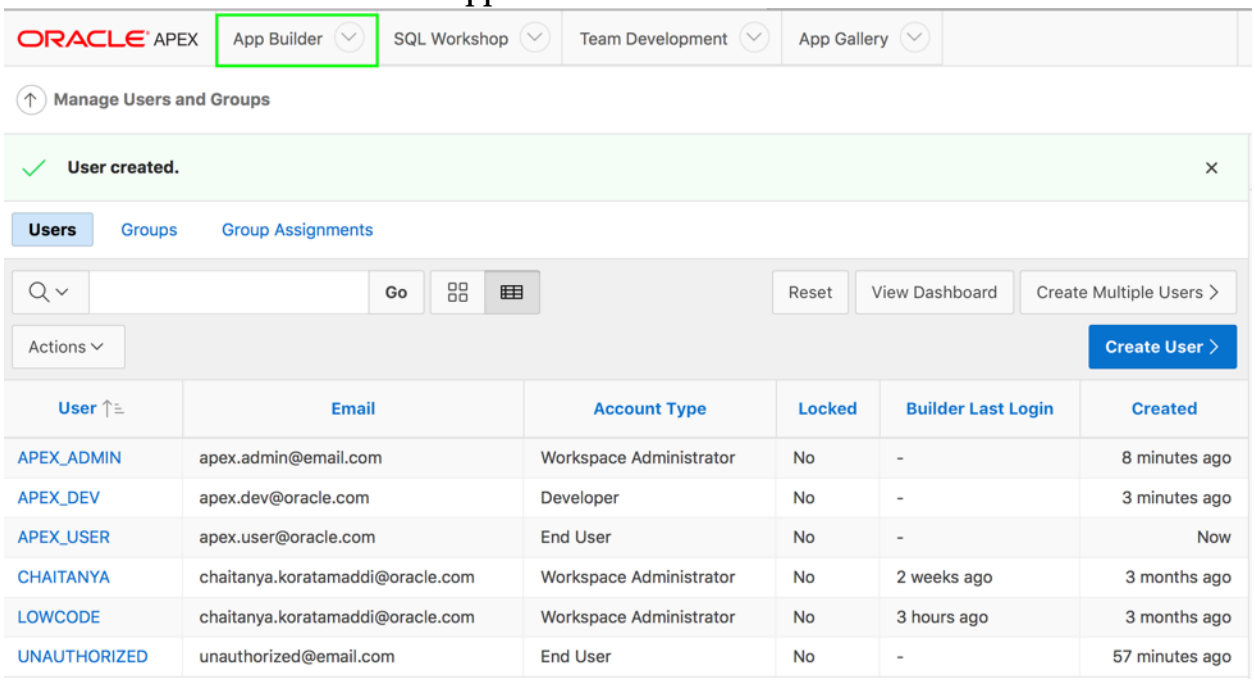
- Select **No** for Require Change of Password on First Use.



5. Enter the following information and click **Create and Create Another**.
   - Username: **apex_dev**
   - Email Address: **apex.dev@oracle.com**
   - Select **No** for User is a workspace administrator
   - Select **Yes** for User is a developer
   - Password: **apexdev123$**
   - Confirm Password: **apexdev123$**
   - Select **No** for Require Change of Password on First Use.

6. Enter the following information and click **Create User**.
   - Username: **apex_user**
   - Email Address: **apex.user@oracle.com**
   - Select **No** for User is a workspace administrator
   - Select **No** for User is a developer
   - Password: **lowcode123$**
   - Confirm Password: **lowcode123$**
   - Select **No** for Require Change of Password on First Use.

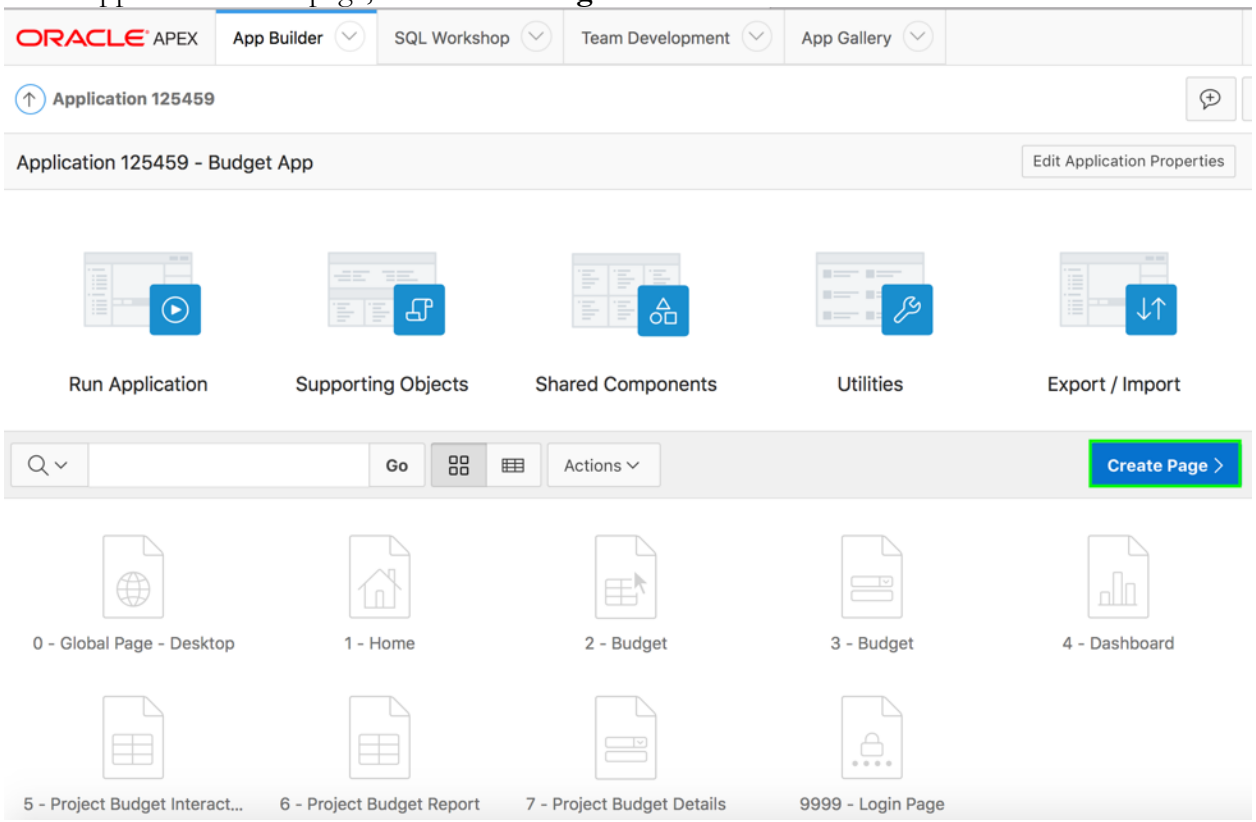
7. You see users in the list now. Click **App Builder**.



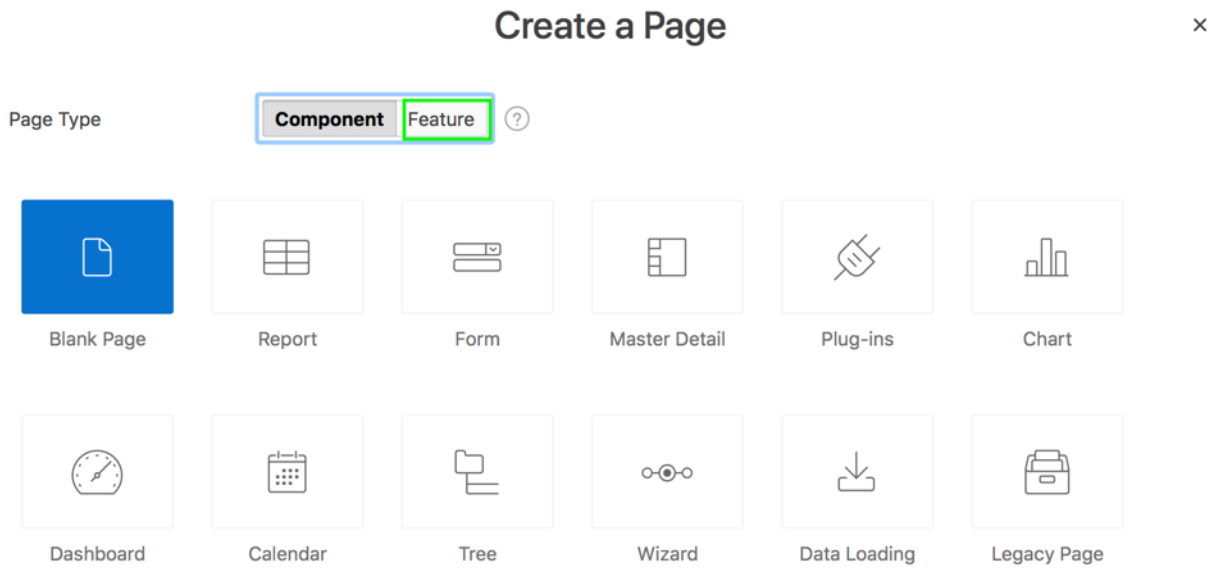
User	Email	Account Type	Locked	Builder Last Login	Created
APEX_ADMIN	apex.admin@email.com	Workspace Administrator	No	-	8 minutes ago
APEX_DEV	apex.dev@oracle.com	Developer	No	-	3 minutes ago
APEX_USER	apex.user@oracle.com	End User	No	-	Now
CHAITANYA	chaitanya.koratamaddi@oracle.com	Workspace Administrator	No	2 weeks ago	3 months ago
LOWCODE	chaitanya.koratamaddi@oracle.com	Workspace Administrator	No	3 hours ago	3 months ago
UNAUTHORIZED	unauthorized@email.com	End User	No	-	57 minutes ago

8. In the report, click the **Budget App** application.

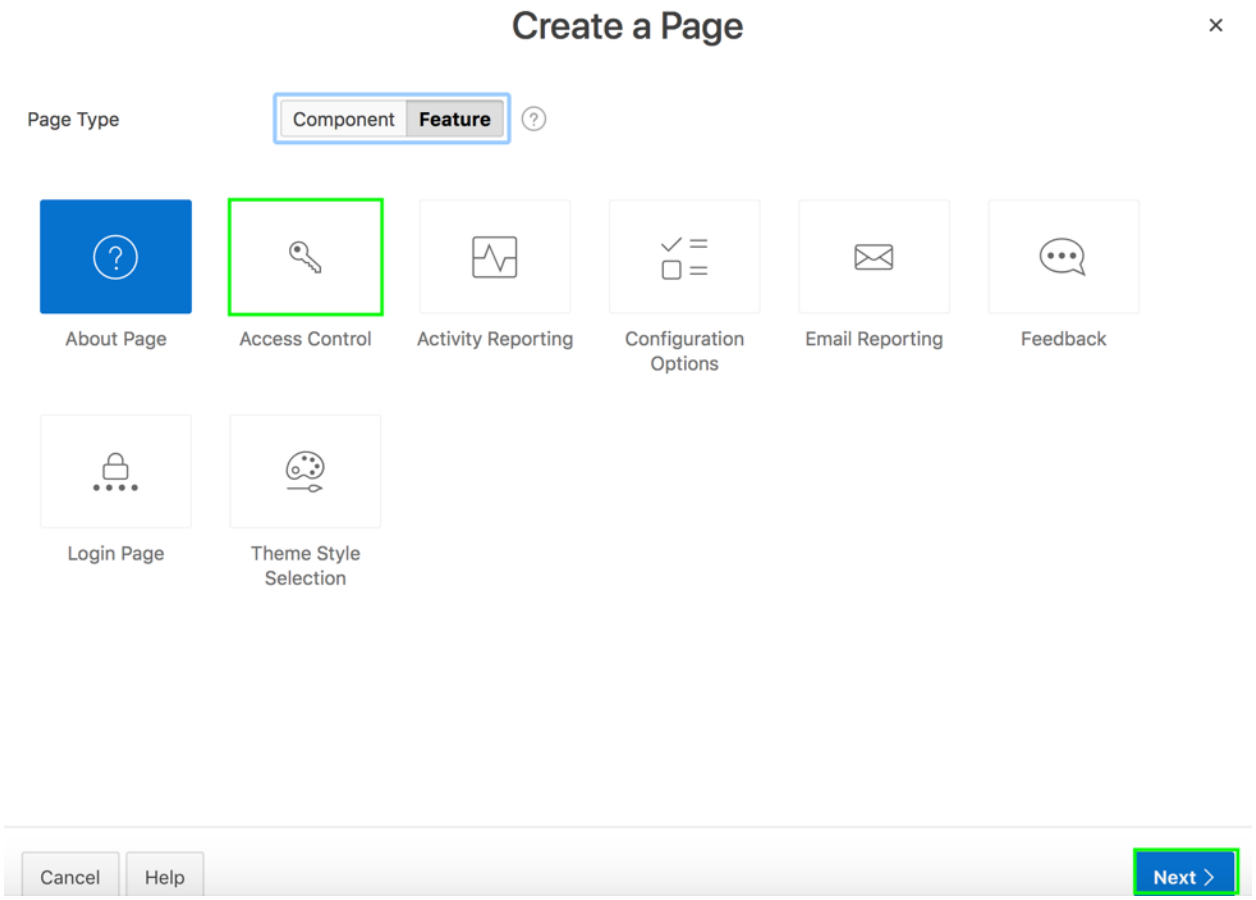
9. In the application home page, click **Create Page**.



10. Select **Feature**.

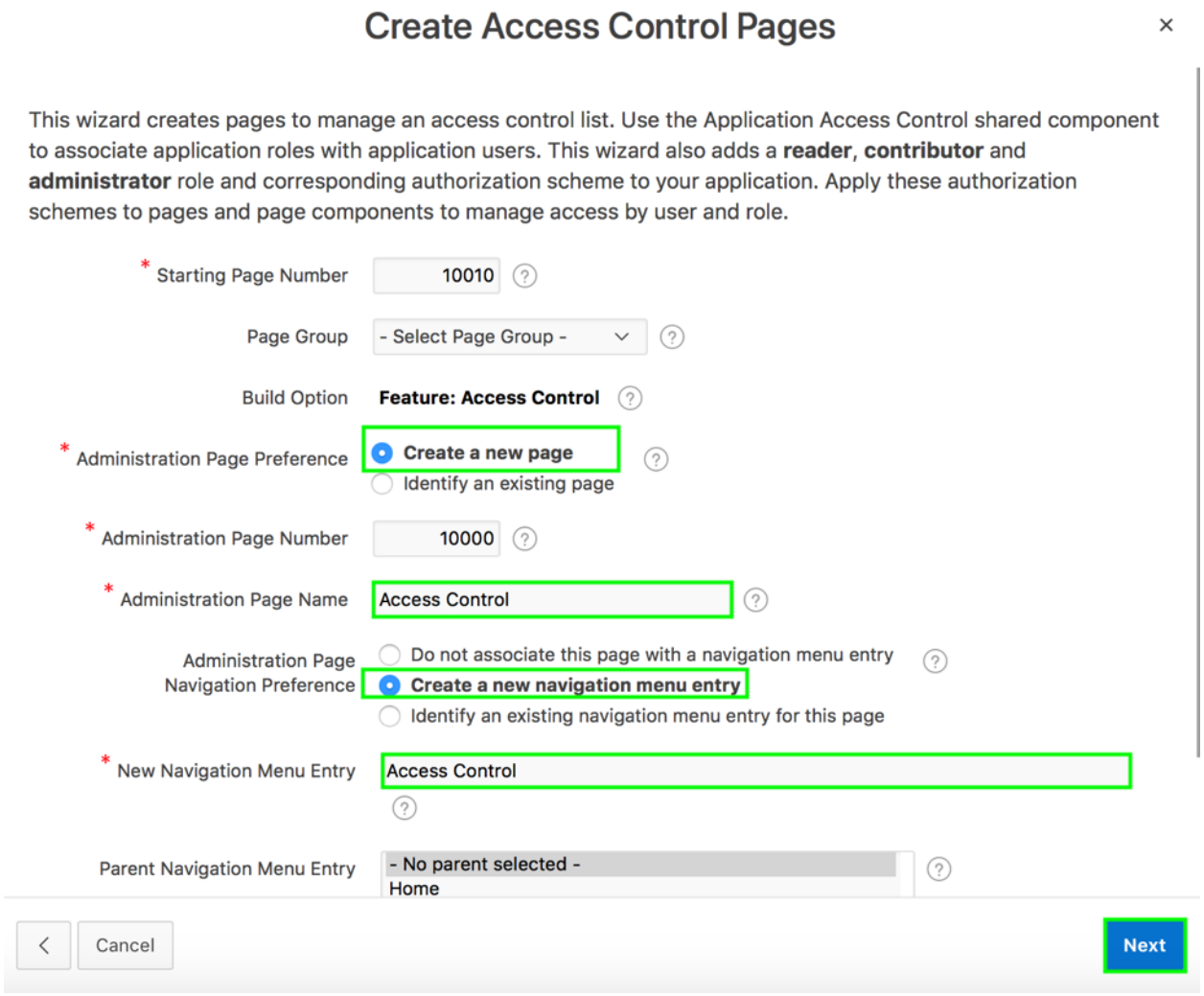


11. Select **Access Control** for Page Type, and click **Next**.

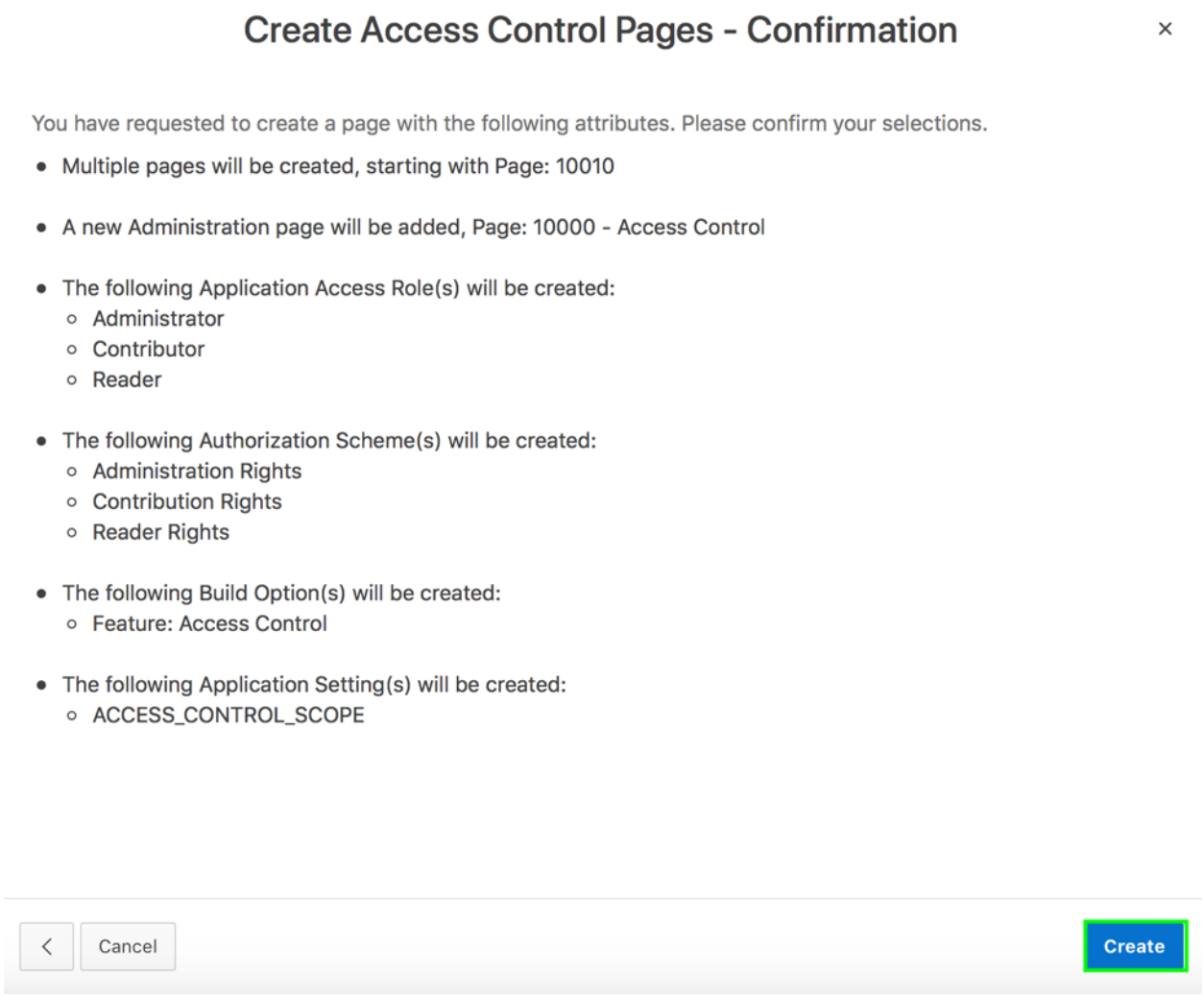


12. In the Create Access Control Pages dialog, enter / select the following:
    - Administration Page Preference: **Create a new page**
    - Administration Page Name: **Access Control**
    - Administration Page Navigation Preference: **Create a new navigation menu entry**
    - New Navigation Menu Entry: **Access Control**.

    Then, click **Next**.

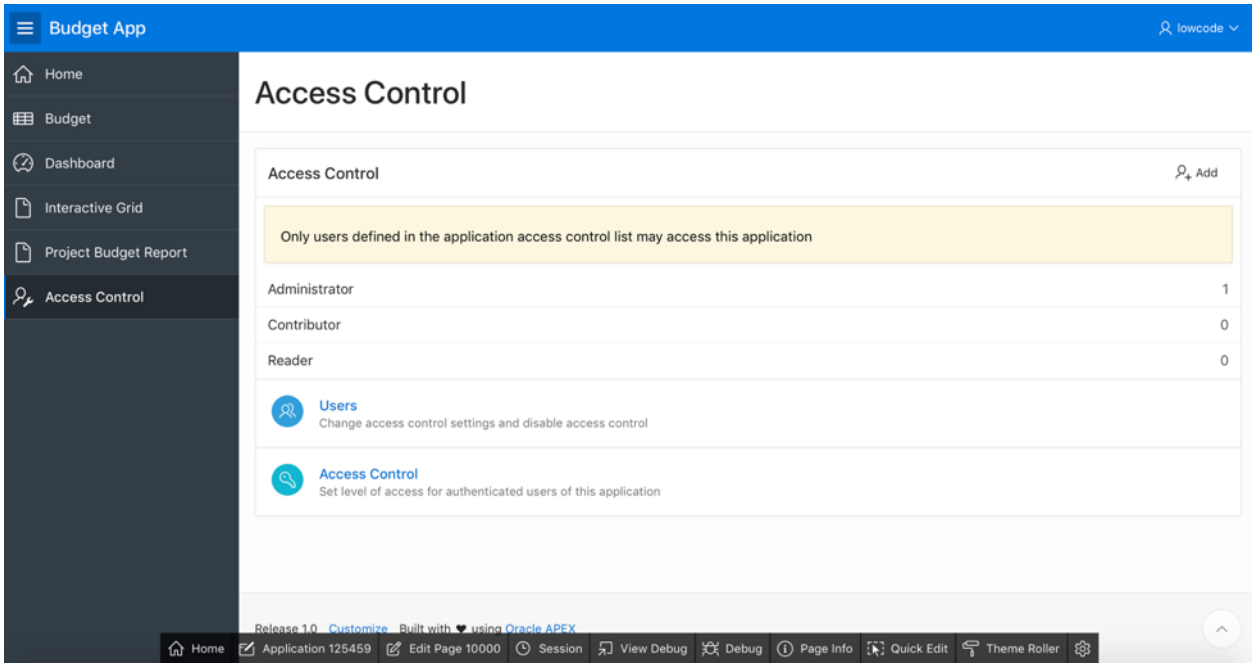


13. On the Confirmation page, click **Create**.



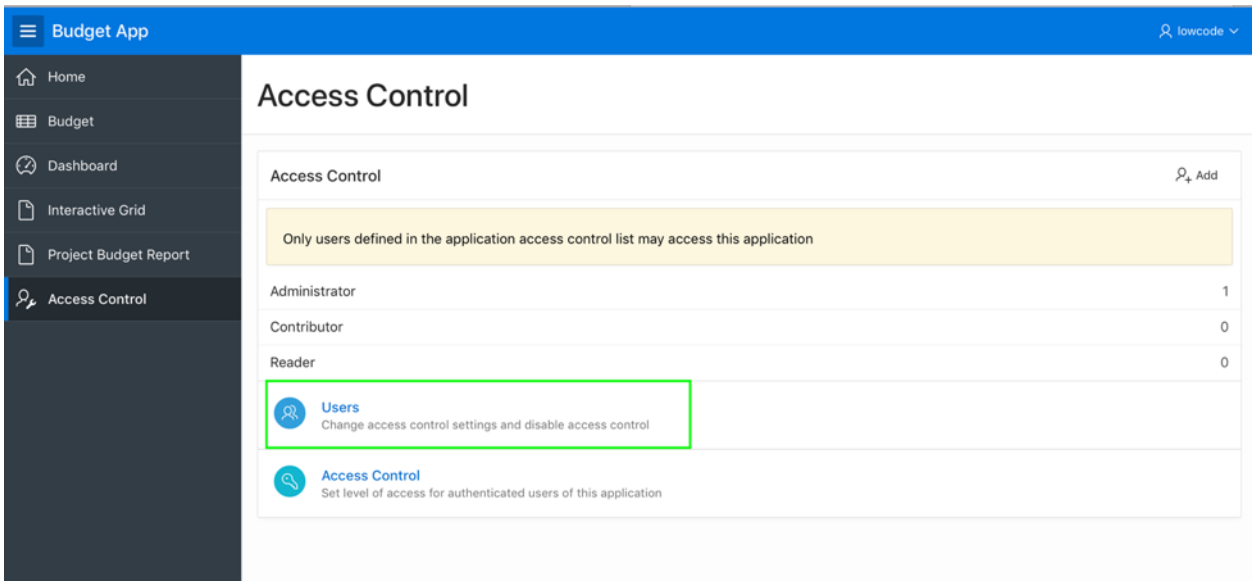
14. In the Page Designer, click **Save and Run Page**.

15. The Access Control page is displayed. Only users defined in the access control list may access this application.

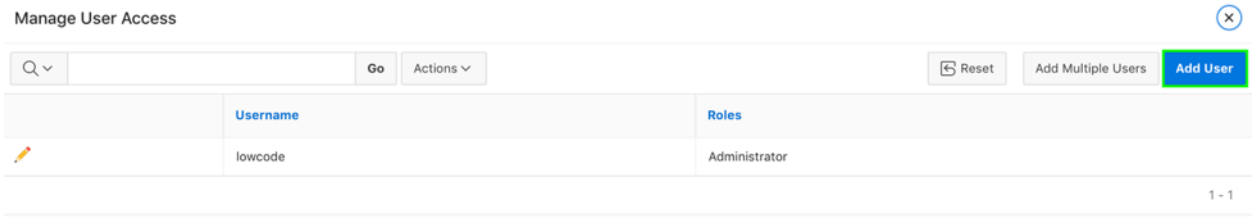


16. Now, add users to the access control list. You add the three users you created in a previous step and also your workspace administrator username.
    - apex_admin is the administrator and so can modify anything including the user privileges
    - apex_dev is the developer and is allowed to edit application data. However, this user cannot change the application administration settings
    - apex_user is the end user and can only view the application but cannot make any changes to the data
    - <your username> is the administrator.

    Click **Users**.



17. Click **Add User**.

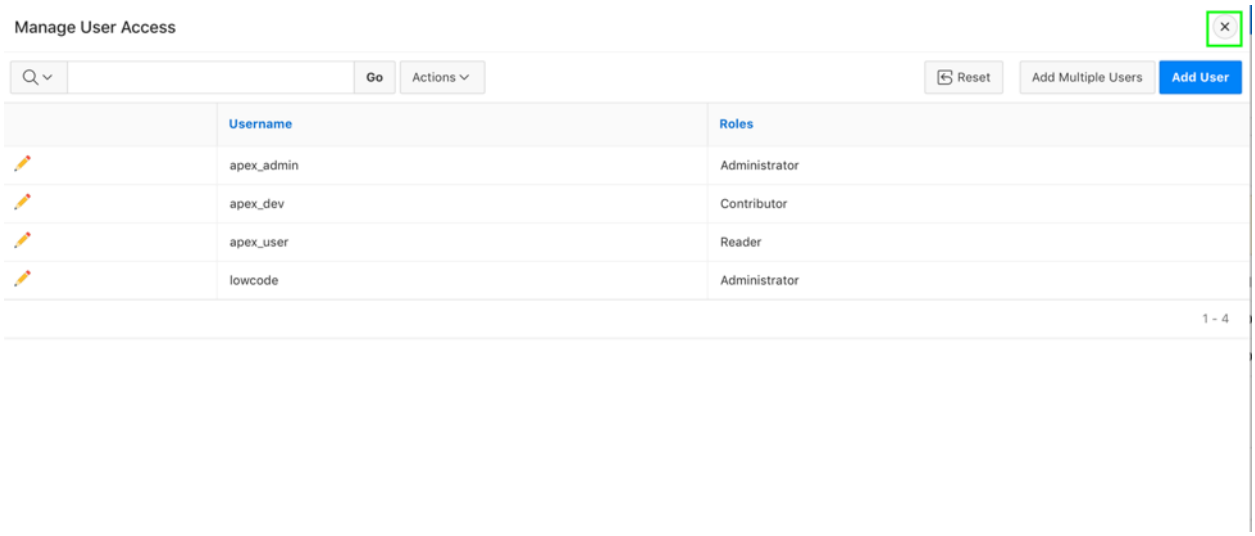


18. Enter **apex_admin** for Username, select **Administrator** for Role and click **Add User**.

19. Click **Add User** again.
    Enter **apex_dev** for Username, select **Contributor** for Role and click **Add User**.

20. Click Add User again.
    Enter **apex_user** for Username, select **Reader** for Role and click **Add User**.

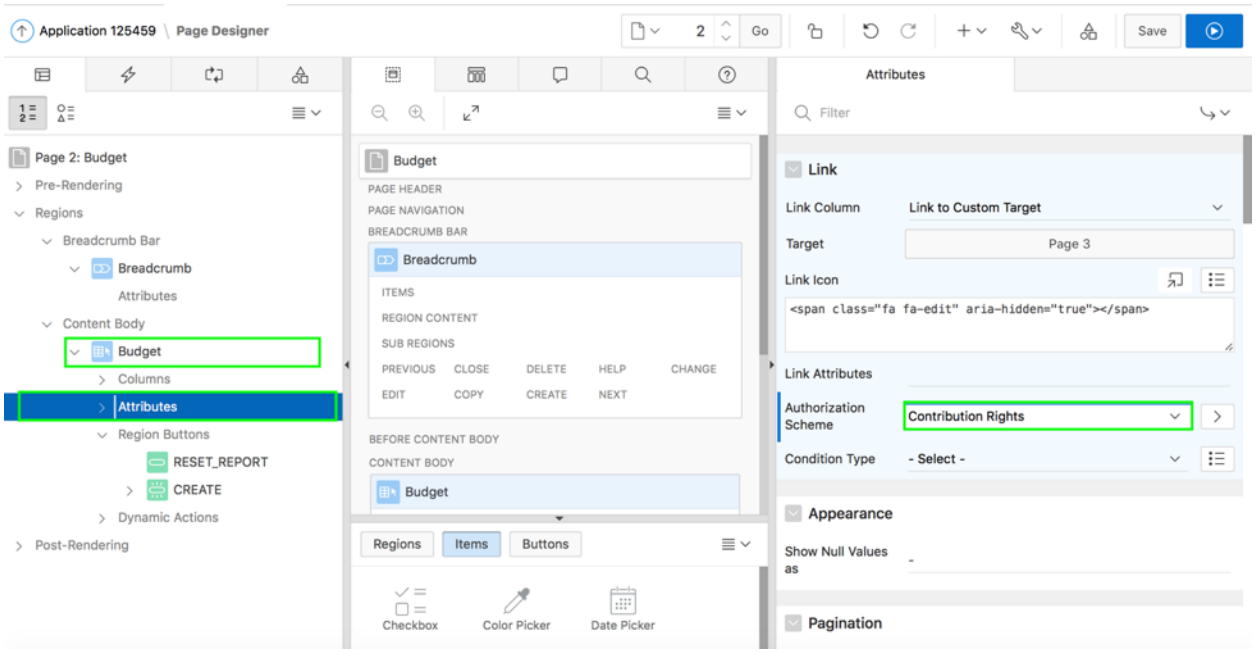
21. Notice that **<*your username*>** is already listed as Administrator. You can now close the dialog.



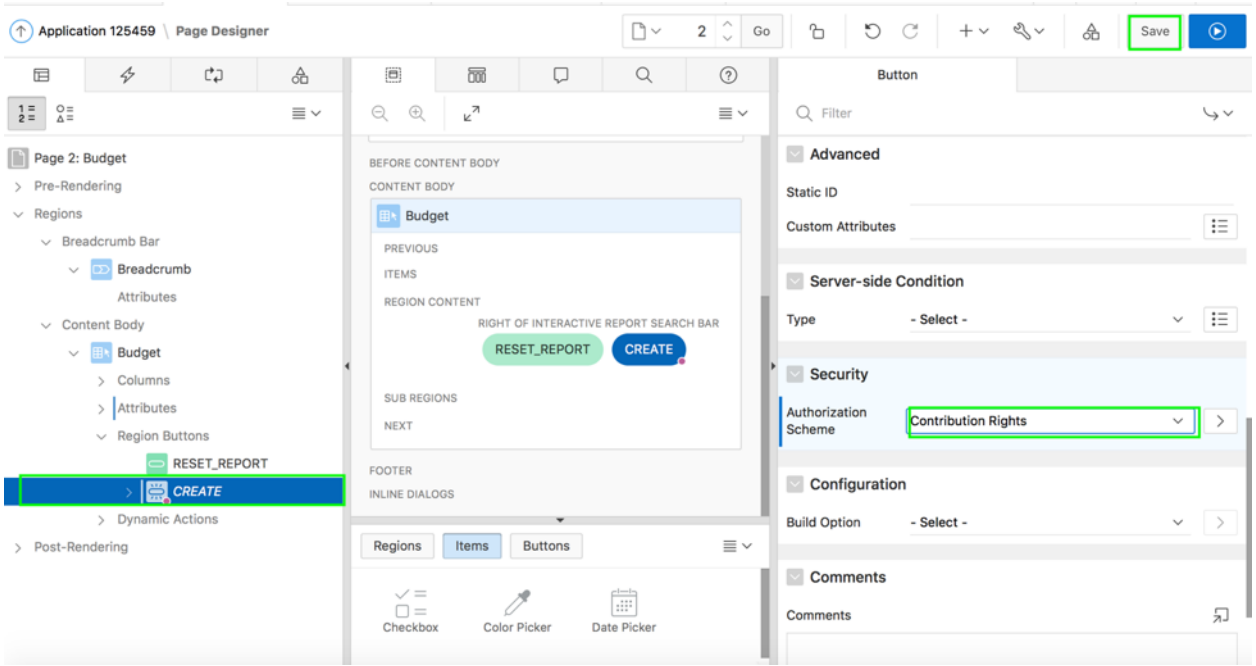
22. Now, you are ready to define and apply the authorization schemes to each application component.
    - Users with the Administrator privilege can make any changes, including administering the Budget App application
    - Users with the Contributor privilege can modify the data in the report but cannot make changes to the application mode and the access control list.
    - Users with the Reader privilege can review the interactive report, but cannot modify the data.

    In the application runtime environment, click **Budget** in the navigation menu.
    In the Developer Toolbar, click **Edit Page 2**.

23. Under Rendering, expand **Regions**. Under the Budget region, select **Attributes**.
In the property editor, locate Authorization Scheme and select **Contribution Rights** from the list.



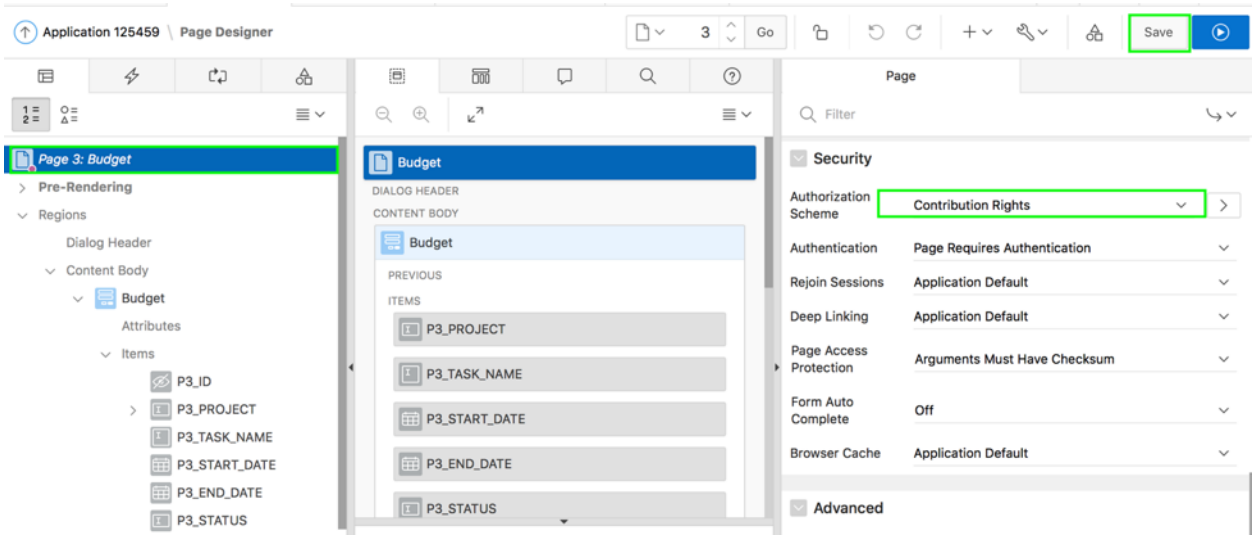
24. You want the Create Button to appear only if the user has either the Contributor or Administrator role. Under Rendering, locate **Region Buttons** and select **CREATE**.
In the property editor, navigate to Security and select **Contribution Rights** for Authorization Scheme.
Click **Save**.



25. You also want to protect against direct access to the Budget form dialog page. Though you restrict end users from editing the interactive report on the Home page, they can still access the Budget form page by entering the correct URL in the browser. To avoid this, you must restrict the Form page access to only users with the Contributor and Administrator roles.

    In the page designer, click **Navigate to Next Page** arrow in the toolbar.
    You are now viewing the Budget form page in page designer.

26. Under Rendering, select **Page 3: Budget**.
    In the Property Editor, navigate to **Security** and select **Contribution Rights** for Authorization Scheme.
    Click **Save**.

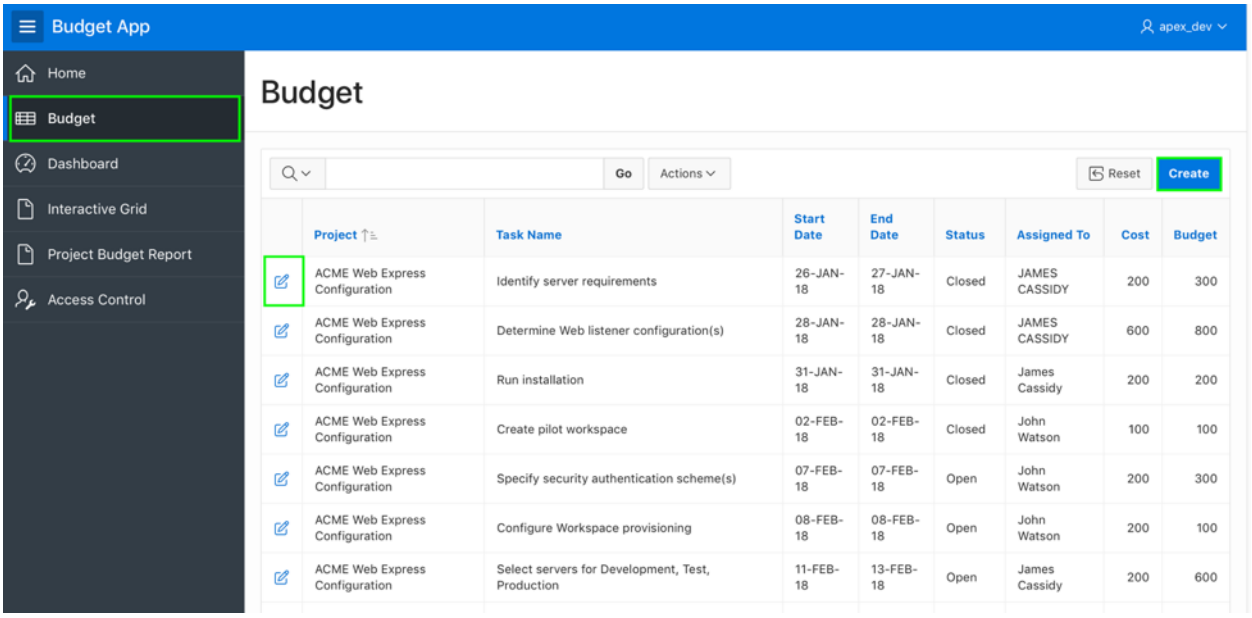


27. In the page designer, enter **2** in the Page Finder and click **Go**.

28. In the page designer, click **Save and Run Page**.
    If you are logged in, click **Sign Out** before performing the next step.

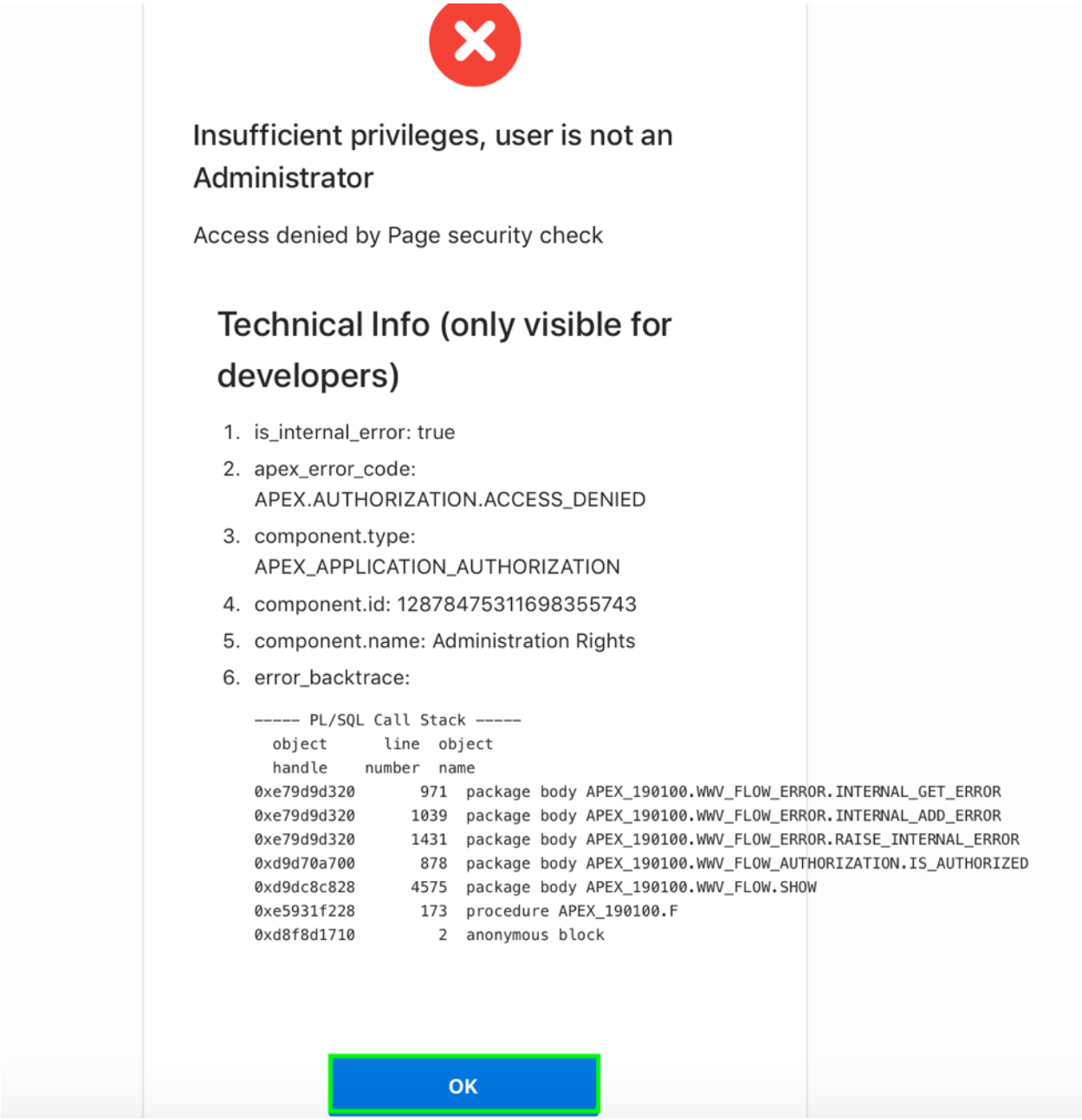
29. Enter **apex_dev** for Username and **apexdev123$** for Password and click **Sign In**.

30. In the navigation menu, click **Budget**.
    Notice that apex_dev can edit the interactive report, and also create a new project.



31. In the navigation menu, click **Access Control**.

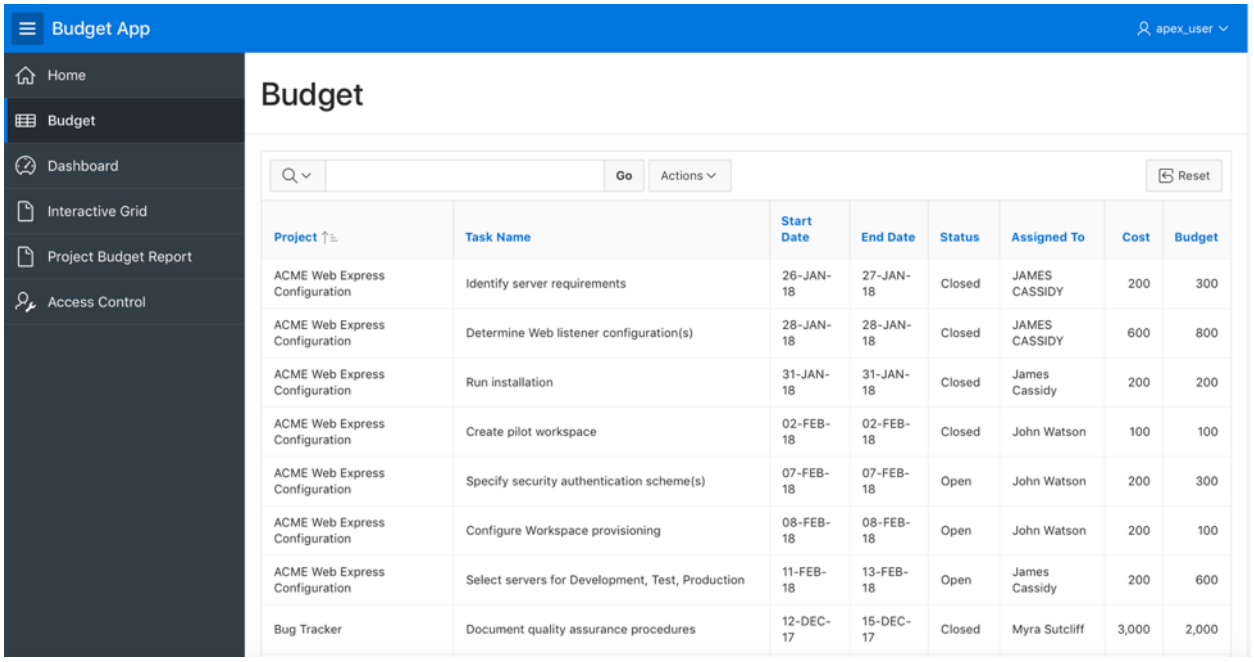
32. Notice that you receive an error as you need the Administrator privilege to use the Access Control Administration page.
    Click **OK**.



33. Click **Sign Out.**

34. Now sign in by entering **apex_user** for Username and **lowcode123$** for password.

35. In the navigation menu, click **Budget**. Notice that you cannot edit the interactive report and also cannot create a new project now.

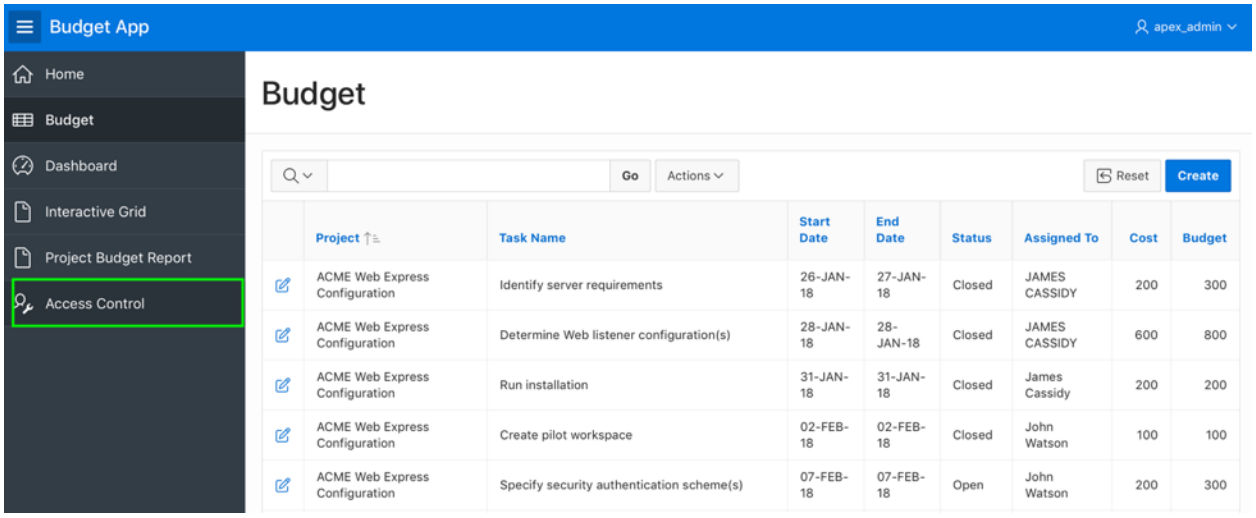


36. Click **Sign Out**.

37. Now sign in by entering **apex_admin** for Username and **apexadmin** for password.

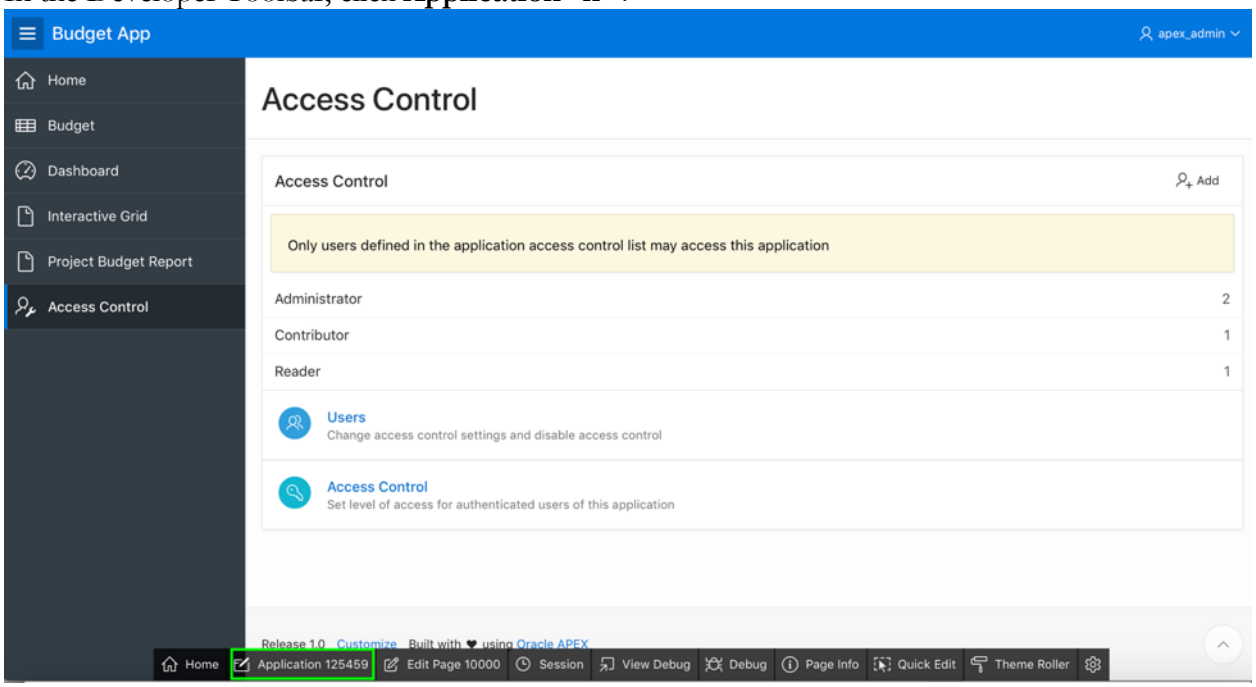
38. In the navigation menu, click **Budget**.

39. Notice that you can now edit the interactive report, and also create a project.
In the navigation menu, click **Access Control**.



40. As you have the Administrator privilege, you can access the Access Control Administration page.

In the Developer Toolbar, click **Application<*n*>**.







Oracle is committed to developing practices and products that help protect the environment

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. Licensed under the Creative Commons Attribution 4.0 International License as shown at https://creativecommons.org/licenses/by/4.0/legalcode.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Hardware and Software, Engineered to Work Together