



## **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 also 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.

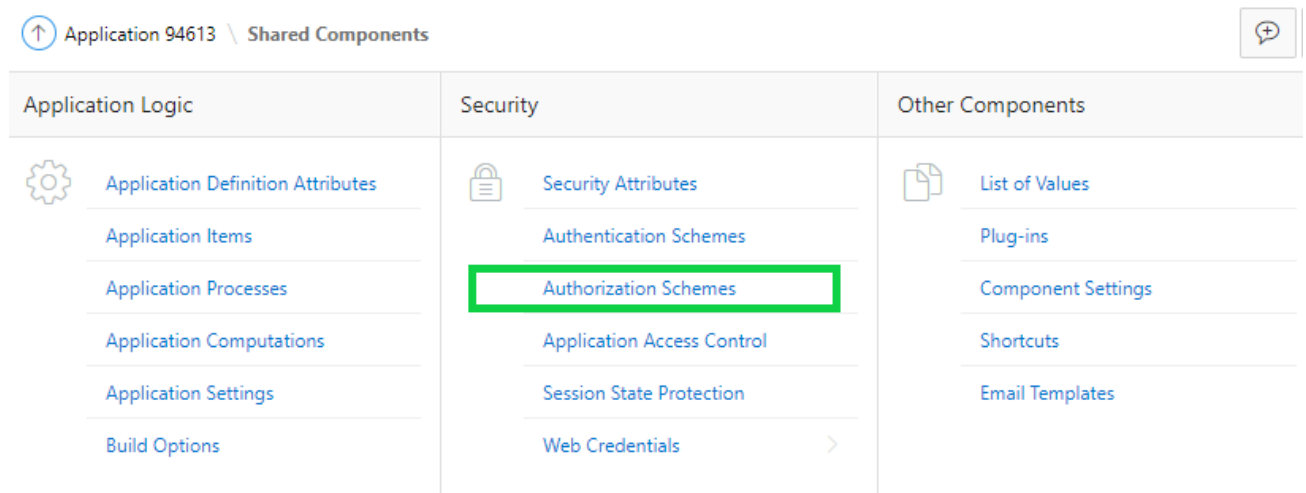
**HOL 13-3 Controlling User Access by Using the Access Control Administration:** In this hands-on lab, you create three different users as Administrator, Developer and End User. You create an Access Control Administration page, set the application mode to restrict access and add these users to the Access 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

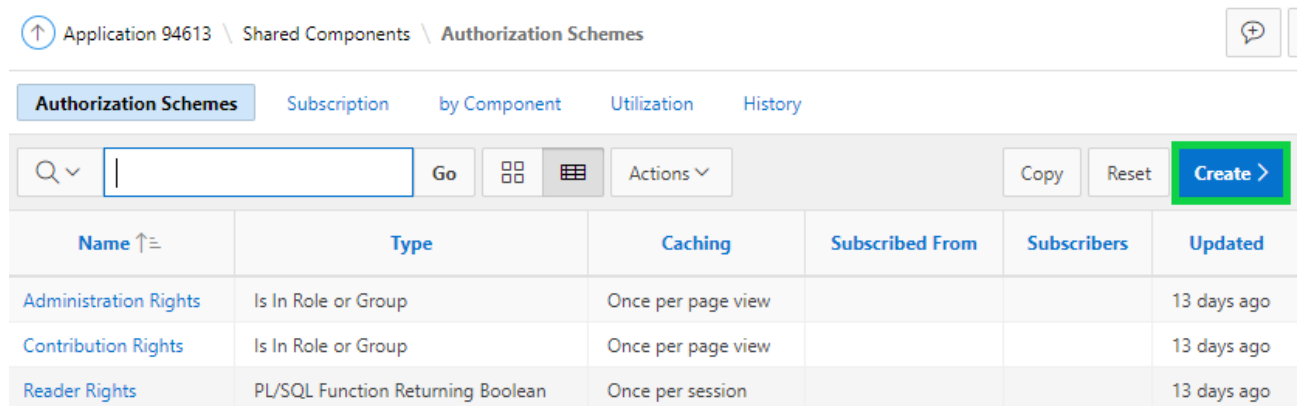
In this hands-on lab, you create an authorization scheme to ensure only people entered as Team Members can log into the Demo Projects application. You apply the authorization scheme to the application properties.

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**.



1 - 3

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.

### Create Authorization Scheme ×

✓
●

Details

Use this page to define an authorization scheme. By creating an authorization schemes, you can protect applications, pages, and application components and extend the security provided by your application authentication scheme. You can use authorization schemes to identify additional security beyond simple user authentication. For example a user with administration rights may need access to more navigation bar icons, pages, and tabs than other users.

Application: **94613 Demo Projects** ?

\* Name  ?

\* Scheme Type Exists SQL Query ?

\* SQL Query 

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

?

\* Identify error message displayed when  ?



<
Cancel
Create Authorization Scheme


- 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.

Application 94613 **Shared Components** Authorization Schemes

Authorization Schemes Subscription by Component Utilization History




Q  Go   Actions

Name 	Type	Caching	Subscribed From	Subscribers	Updated
<a href="#">Administration Rights</a>	Is In Role or Group	Once per page view			13 days ago
<a href="#">Contribution Rights</a>	Is In Role or Group	Once per page view			13 days ago
<a href="#">Reader Rights</a>	PL/SQL Function Returning Boolean	Once per session			13 days ago
<a href="#">Team Members</a>	Exists SQL Query	Once per session			1 seconds ago

1 - 4

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

Application 94613 \ Shared Components

Application Logic	Security	Other Components
 <a href="#">Application Definition Attributes</a> <a href="#">Application Items</a> <a href="#">Application Processes</a> <a href="#">Application Computations</a> <a href="#">Application Settings</a> <a href="#">Build Options</a>	 <b><a href="#">Security Attributes</a></b> <a href="#">Authentication Schemes</a> <a href="#">Authorization Schemes</a> <a href="#">Application Access Control</a> <a href="#">Session State Protection</a> <a href="#">Web Credentials</a> >	 <a href="#">List of Values</a> <a href="#">Plug-ins</a> <a href="#">Component Settings</a> <a href="#">Shortcuts</a> <a href="#">Email Templates</a>

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

Application 94613 \ Edit Security Attributes

Definition **Security** Globalization User Interface

Application 94613

Show All Authentication **Authorization** Session Managem... Session State Prote... Browser Security Database Session

Authorization Define Authorization Schemes >

Application authorization schemes control access to all pages within an application. Unauthorized access to the application, regardless of which page is requested, will cause an error page to be displayed.

Authorization Scheme **Team Members** ?

Run on Public Pages ☐ ?

Source for Role or Group Schemes Access Control User Role Assignments ?

- 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**.

ORACLE APEX App Builder SQL Workshop Team Development App Gallery

Application 94613 \ Shared Components

Application processed.

Application Logic	Security	Other Components
<ul style="list-style-type: none"> <li>Application Definition Attributes</li> <li>Application Items</li> <li>Application Processes</li> </ul>	<ul style="list-style-type: none"> <li>Security Attributes</li> <li>Authentication Schemes</li> <li>Authorization Schemes</li> </ul>	<ul style="list-style-type: none"> <li>List of Values</li> <li>Plug-ins</li> <li>Component Settings</li> </ul>

Administration  
Manage Service  
**Manage Users and Groups**  
Monitor Activity  
Change My Password

- 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 - select **No**

Click **Create User**.

The screenshot displays the 'Create User' wizard in Oracle APEX. The 'User Identification' tab is selected, showing fields for Username (unauthorized), Email Address (unauthorized@email.com), First Name, and Last Name. The 'Password' tab is also visible, showing fields for Password, Confirm Password, and a dropdown for 'Require Change of Password on First Use' set to 'No'. The 'Create User' button is highlighted in blue.

**User Identification**

\* Username  ?

\* Email Address  ?

First Name  ?

Last Name  ?

**Create User**

Cancel Create and Create Another **Create User**

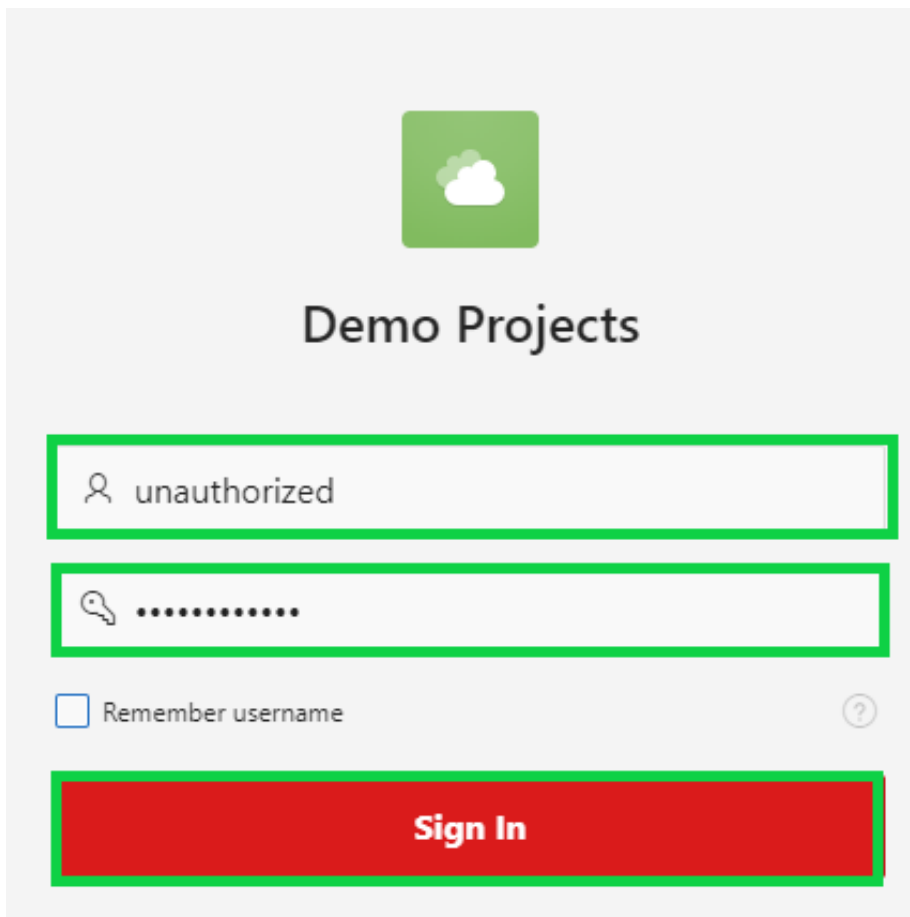
**Password**

\* Password  Passwords are case sensitive ?

\* Confirm Password  ?

Require Change of Password on First Use  ?

11. Navigate to the runtime environment (tab or window). Click **Sign Out** in the navigation bar (top right).
12. On the Log In page, for Username enter **unauthorized**, and for Password enter **unauthorized**. Click **Sign In**.



The image shows a login form titled "Demo Projects". At the top is a green square icon with a white cloud. Below the title are two input fields, both highlighted with a thick green border. The first field contains a person icon and the text "unauthorized". The second field contains a key icon and a series of dots. Below these fields is a checkbox labeled "Remember username" and a help icon (a circle with a question mark). At the bottom is a large red button with the text "Sign In" in white, also highlighted with a thick green border.

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: 8983112094236963691
5. component.name: Team Members
6. error_backtrace:

----- PL/SQL Call Stack -----
   object      line object
   handle      number name
0x157cf2db0    1033 package body APEX_190200.WWV_FLOW_ERROR.INTERNAL_GET_ERROR
0x157cf2db0    1101 package body APEX_190200.WWV_FLOW_ERROR.INTERNAL_ADD_ERROR
0x157cf2db0    1493 package body APEX_190200.WWV_FLOW_ERROR.RAISE_INTERNAL_ERROR
0x138cff300     874 package body APEX_190200.WWV_FLOW_AUTHORIZATION.IS_AUTHORIZED
0x74bb3720    4455 package body APEX_190200.WWV_FLOW.SHOW
0x13725ed30    173 procedure APEX_190200.F
0x5a7e46ac0     2 anonymous block

```

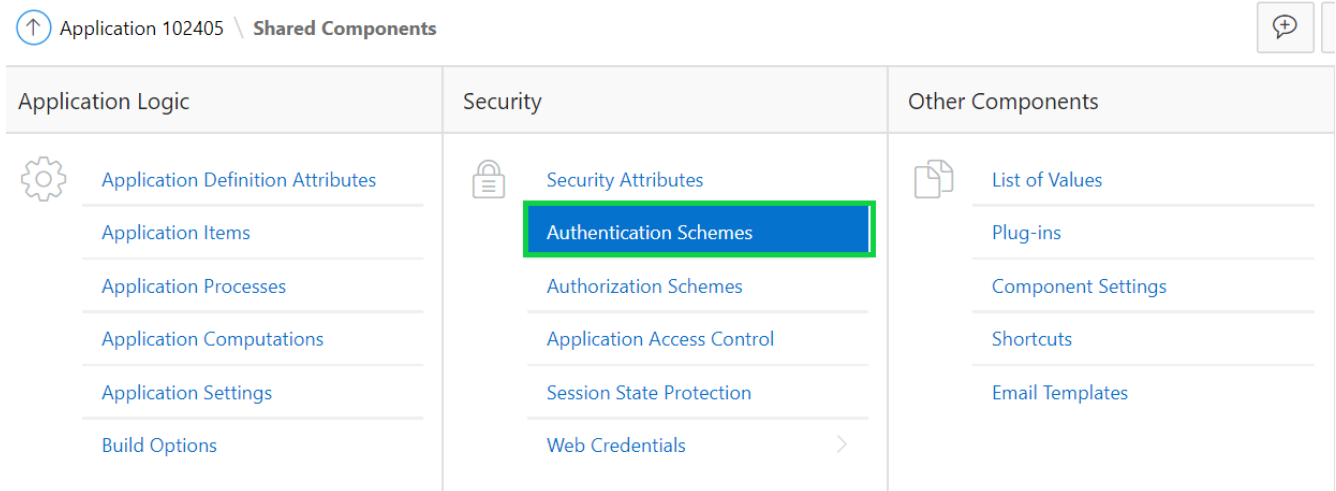
**OK**

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

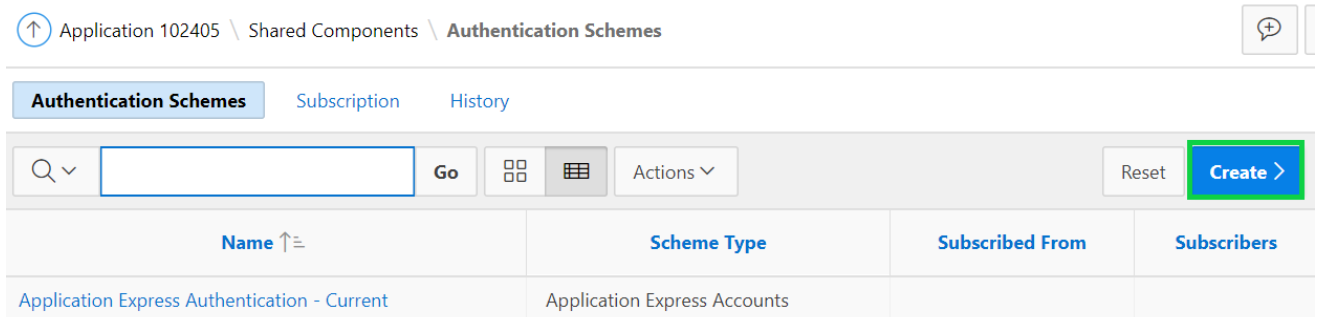
## HOL 13-2: Creating and Using an Authentication Scheme

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**.



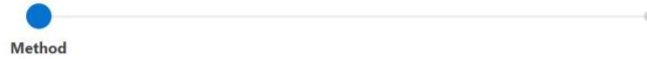
3. You want to create an authentication scheme. Click **Create**.



1 - 1

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

## Create Authentication Scheme



When you create a new authentication scheme, you have several options. Most let you reuse implementations that already exist in your application or in other applications within your workspace. There are even some pretested schemes you can copy to get you up and running immediately.

Create Scheme: ☒ Based on a pre-configured scheme from the gallery ☐ As a copy of an existing authentication scheme

> Information

Cancel

Next >

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

Application 102405 \ Shared Components \ Authentication Schemes \ Create / Edit

< Authentication Scheme Cancel Create Authentication Scheme

Name

\* Name Open Door Credentials ?

\* Scheme Type Open Door Credentials ?

- In the toolbar, click the **Run Page** icon.  
If you are already logged in, then click Sign Out to perform the next step.
- Enter your Username and click **Login**.

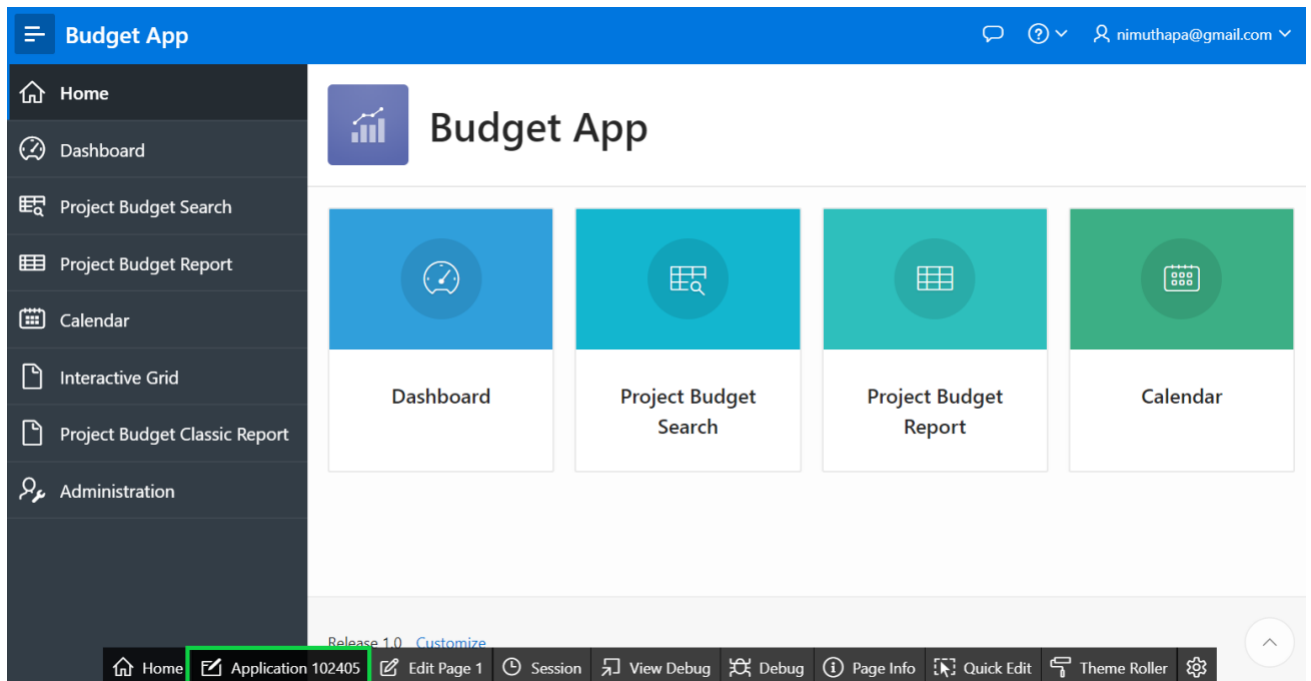
## Log In to Application 102405

Enter your credentials in this form to start a new session in this Application Express application.

\* Username

Login

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



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.

Application 102405 \ Shared Components \ **Authentication Schemes**

**Authentication Schemes** Subscription History

Q v Go Actions v Reset Create >

Name ↑	Scheme Type	Subscribed From	Subscribers
<b>Application Express Authentication</b>	Application Express Accounts		
Open Door Credentials - Current	Open Door Credentials		

1 - 2

12. Click **Make Current Scheme**.

Application 102405 \ Shared Components \ Authentication Schemes \ **Create / Edit**

**Authentication Scheme** Cancel Delete **Make Current Scheme** **Apply Changes**

Show All Name Subscription Source Session Not V... Login Process... Post-Logout ... Session Sharing Comments

Name

\* Name Application Express Authentication ?

\* Scheme Type Application Express Accounts ?



Subscription

13. Click **OK**.

Would you like to make 'Application Express Authentication' the current authentication scheme of the application?

Cancel **OK**

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

 Authentication scheme activated as current authentication scheme. 

Authentication Schemes

Subscription

History

Q

▼

Go

□

□

□

□

≡

Actions ▼


Reset

Create >


Name ↑≡	Scheme Type	Subscribed From	Subscribers
Application Express Authentication - Current	Application Express Accounts		
Open Door Credentials	Open Door Credentials		


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**.



## Budget App



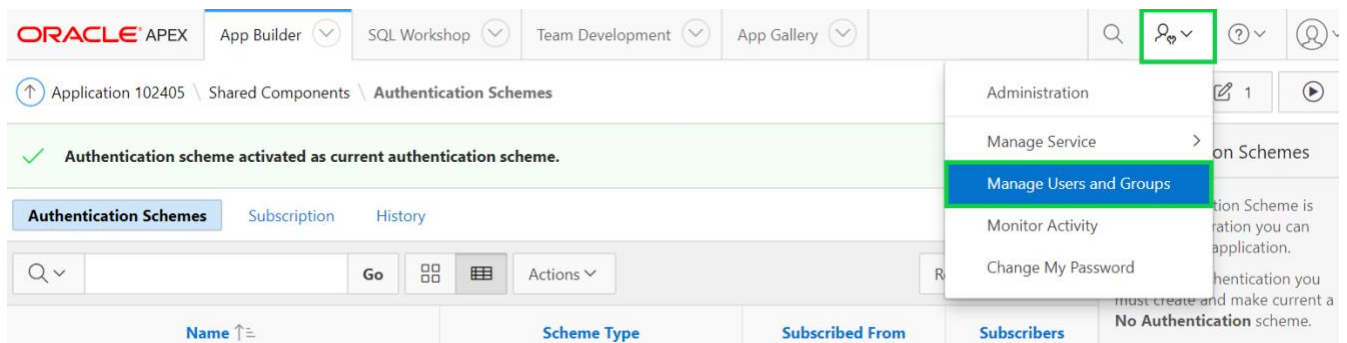
☐ Remember username 

**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.



[Show All](#)
[User Identification](#)
[Account Privileges](#)
[Password](#)
[Group Assignments](#)

### User Identification

\* Username  ?  
 \* Email Address  ?  
 First Name  ?  
 Last Name  ?

[Create User](#)
[Cancel](#)
[Create and Create Another](#)

[Show All](#)
[User Identification](#)
[Account Privileges](#)
[Password](#)
[Group Assignments](#)

### Account Privileges

Default Schema  ?  
 Accessible Schemas (null for all)  ?  
 User is a workspace administrator: ☒ Yes ☐ No ?  
 User is a developer: ☒ Yes ☐ No ?  
 App Builder Access  ?  
 SQL Workshop Access  ?  
 Team Development Access  ?  
 Set Account Availability  ?

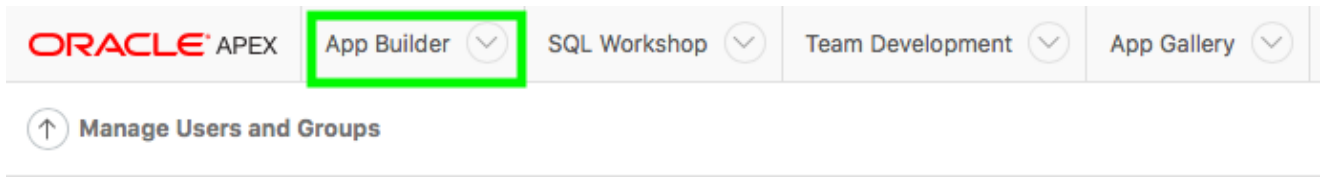
### Password

\* Password  Passwords are case sensitive ?  
 \* Confirm Password  ?  
 Require Change of Password on First Use  ?

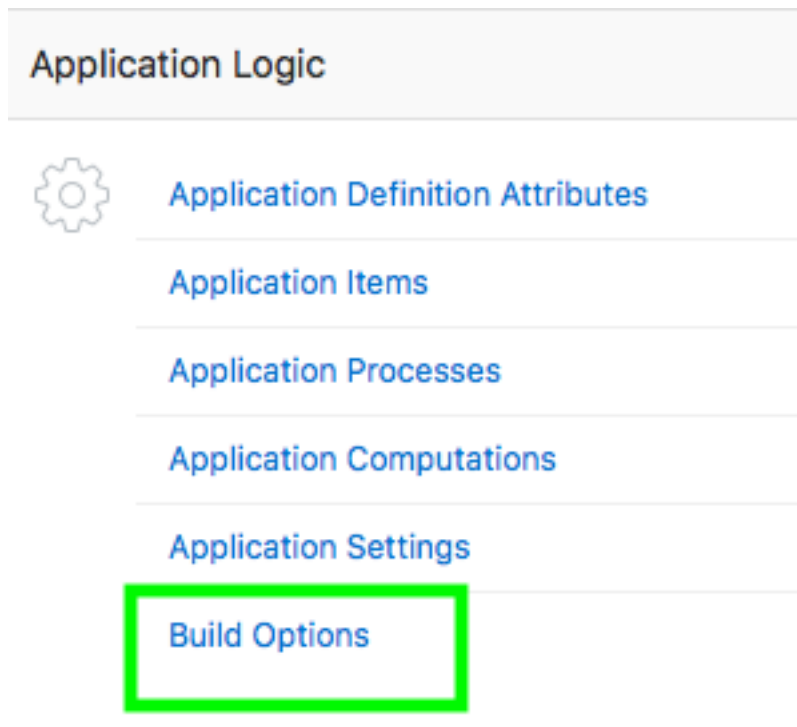
5. Enter the following information and click **Create and Create Another**.

- 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**.



8. In the report, click the **Budget App** application.
9. You must first remove the feature that already exists in this application. You must remove the existing page(s), shared components and Feature: Access Control build option. Perform the following steps:
  - a) Go to Shared Components
  - b) Go to Application Logic > Build Options.



c) Click **Feature: Access Control**.

Build Options   Utilization   History								
Q v		Go			Actions v		Reset	Create >
Name ↑	Application	Status	Default on Export	On Upgrade Keep Status	Comment	Updated By	Created	Updated
<a href="#">Feature: About Page</a>	42700	Include	Include	No	About this application page.	LOWCODE	4 weeks ago	4 weeks ago
<b>Feature: Access Control</b>	42700	Include	Include	No	Incorporate role based user authentication within your application and manage username mappings to application roles.	LOWCODE	4 weeks ago	4 weeks ago

d) Click **Remove Components**.

Build Option

Cancel   Delete   **Apply Changes**

Show All

Attributes

Associated Components

Attributes

Application 42700 Budget App

Build Option Feature: Access Control

Status Include

Default on Export - Same as Current Status -

On Upgrade Keep Status

Comments
Incorporate role based user authentication within your application and manage username mappings to application roles.

Associated Components

Remove Components

Component ↑

Component Name

Build Option


Page Number

Build Options

Use Build Options to enable or disable functionality within an application.

- e) Click the checkbox for **Yes – remove components**.

## Remove Components



Are you sure you want to permanently remove all application components associated with this build option?

Build Option	Feature: Access Control
	<input checked="" type="checkbox"/> <b>Yes - remove components</b>

**Remove Components**

- f) Click **Remove Components**.
- g) On Create / Edit Build Option, Click **Delete**.
- h) Click **Delete Build Option**.
- i) Click Application <n> link to navigate to the application home page.

Application 42700 Shared Components \ Build Options

✓ Build Option Removed. ×

Build Options Utilization History

Q v | Go [ ] [ ] Actions v Reset Create >

Name ↑	Application	Status	Default on Export	On Upgrade Keep Status	Comment	Updated By	Created	Updated
Feature: About Page	42700	Include	Include	No	About this application page.	LOWCODE	4 weeks ago	4 weeks ago
Feature: Activity Reporting	42700	Include	Include	No	Include numerous reports and charts on end user activity.	LOWCODE	4 weeks ago	4 weeks ago
Feature: Configuration Options	42700	Include	Include	No	Allow application administrators to enable or disable specific functionality, associated with an Application Express build option, from within the application.	LOWCODE	4 weeks ago	4 weeks ago
Feature: Feedback	42700	Include	Include	No	Provide a mechanism for end users to post general comments back to the application administrators and developers.	LOWCODE	4 weeks ago	4 weeks ago
Feature: Theme Style Selection	42700	Include	Include	No	Allow administrators to select a default color scheme (theme style) for the application. Administrators can also choose to allow end users to choose their own theme style.	LOWCODE	4 weeks ago	4 weeks ago

1 - 5

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

ORACLE APEX App Builder SQL Workshop Team Development App Gallery

Application 102405

Application 102405 - Budget App [Edit Application Properties](#)

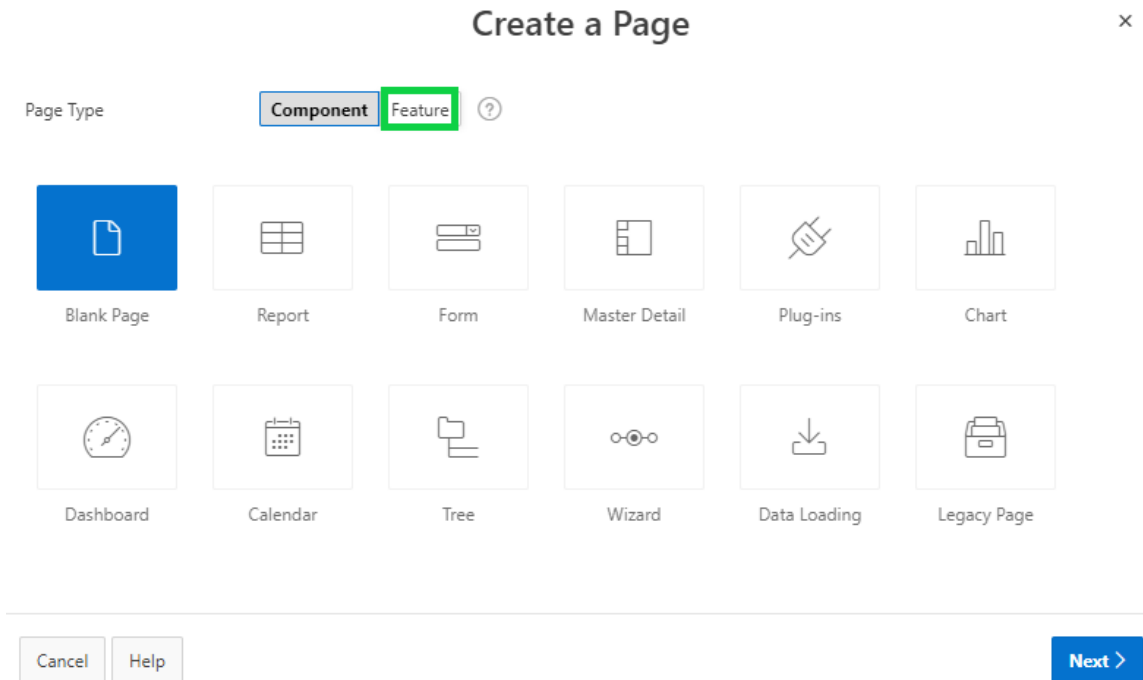
Run Application Supporting Objects Shared Components Utilities Export / Import

Q Go Actions [Create Page >](#)

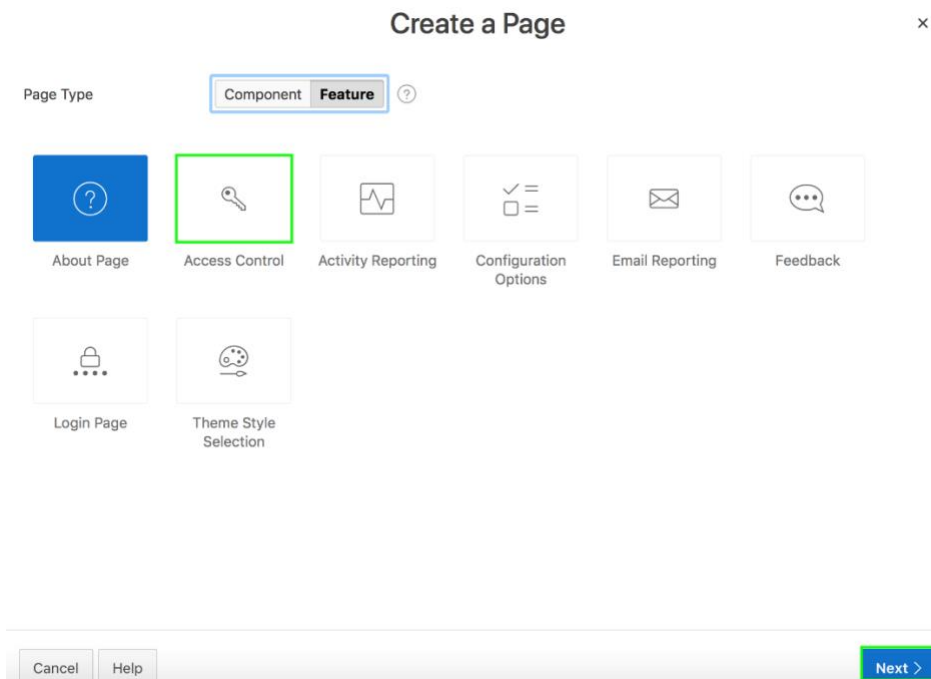
0 - Global Page - Desktop 1 - Home 2 - Dashboard 3 - Project Budget Search 4 - Project Budget Report

5 - Project Budget 6 - Calendar 7 - Project Budget Interac... 8 - Project Budget Classic ... 9 - Project Budget Classic ...

## 11. Select **Feature**.



12. Select **Access Control** for Page Type.



13. 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**.

### Create Access Control Pages ×

This wizard creates pages to manage an access control list. Use the Application Access Control shared component to associate application roles with application users. This wizard also adds a **reader**, **contributor** and **administrator** role and corresponding authorization scheme to your application. Apply these authorization schemes to pages and page components to manage access by user and role.

\* Starting Page Number  ?

Page Group  ?

Build Option **Feature: Access Control** ?

\* Administration Page Preference ☒ **Create a new page** ?  
☐ Identify an existing page

\* Administration Page Number  ?

\* Administration Page Name  ?

Administration Page Navigation Preference ☐ Do not associate this page with a navigation menu entry ?  
☒ **Create a new navigation menu entry** ?  
☐ Identify an existing navigation menu entry for this page

\* New Navigation Menu Entry  ?

Parent Navigation Menu Entry  ?

**Next**

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



## Create Access Control Pages - Confirmation

✕

You have requested to create a page with the following attributes. Please confirm your selections.

- Multiple pages will be created, starting with Page: 10010
- A new Administration page will be added, Page: 10000 - Access Control
- The following Application Access Role(s) will be created:
  - Administrator
  - Contributor
  - Reader
- The following Authorization Scheme(s) will be created:
  - Administration Rights
  - Contribution Rights
  - Reader Rights
- The following Build Option(s) will be created:
  - Feature: Access Control
- The following Application Setting(s) will be created:
  - ACCESS\_CONTROL\_SCOPE

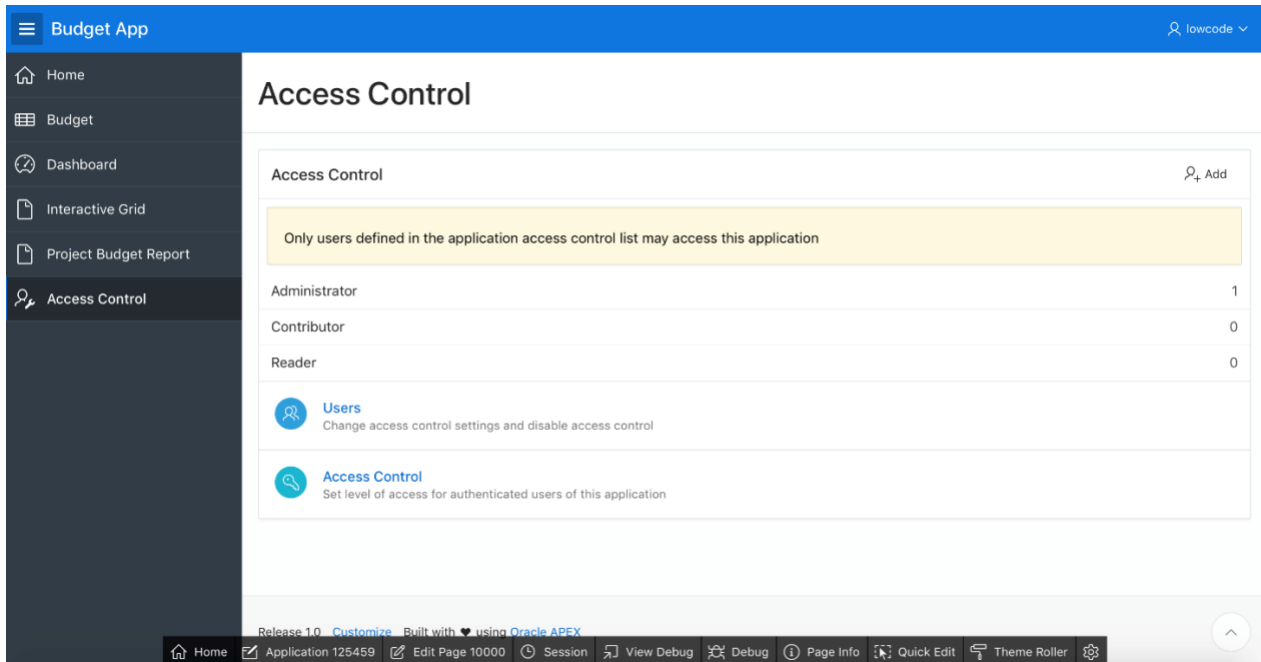


Cancel

Create

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

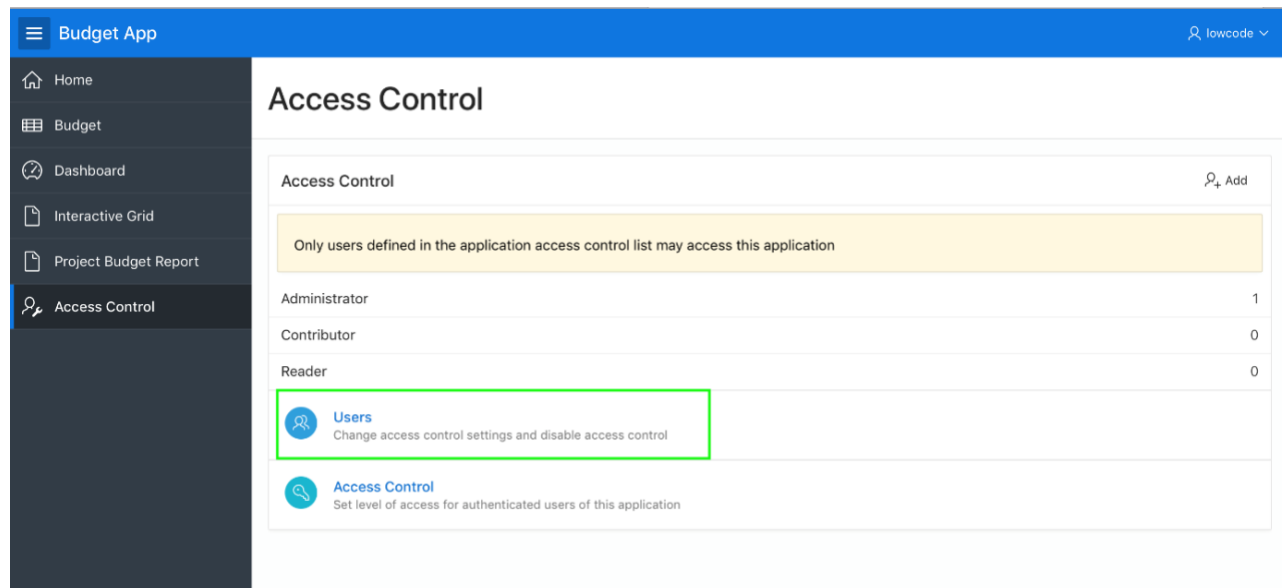
16. The Access Control page is displayed. Only users defined in the access control list may access this application.



17. 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**.



18. Click **Add User**.

Manage User Access ✕

	Username	Roles
	lowcode	Administrator

1 - 1

19. Enter **apex\_admin** for Username, select **Administrator** for Role and click **Add User**.20. Click **Add User** again.





Enter **apex\_dev** for Username, select **Contributor** for Role and click **Add User**.

## 21. Click Add User again.

Enter **apex\_user** for Username, select **Reader** for Role and click **Add User**.

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

Manage User Access ✕

	Username	Roles
	apex_admin	Administrator
	apex_dev	Contributor
	apex_user	Reader
	lowcode	Administrator

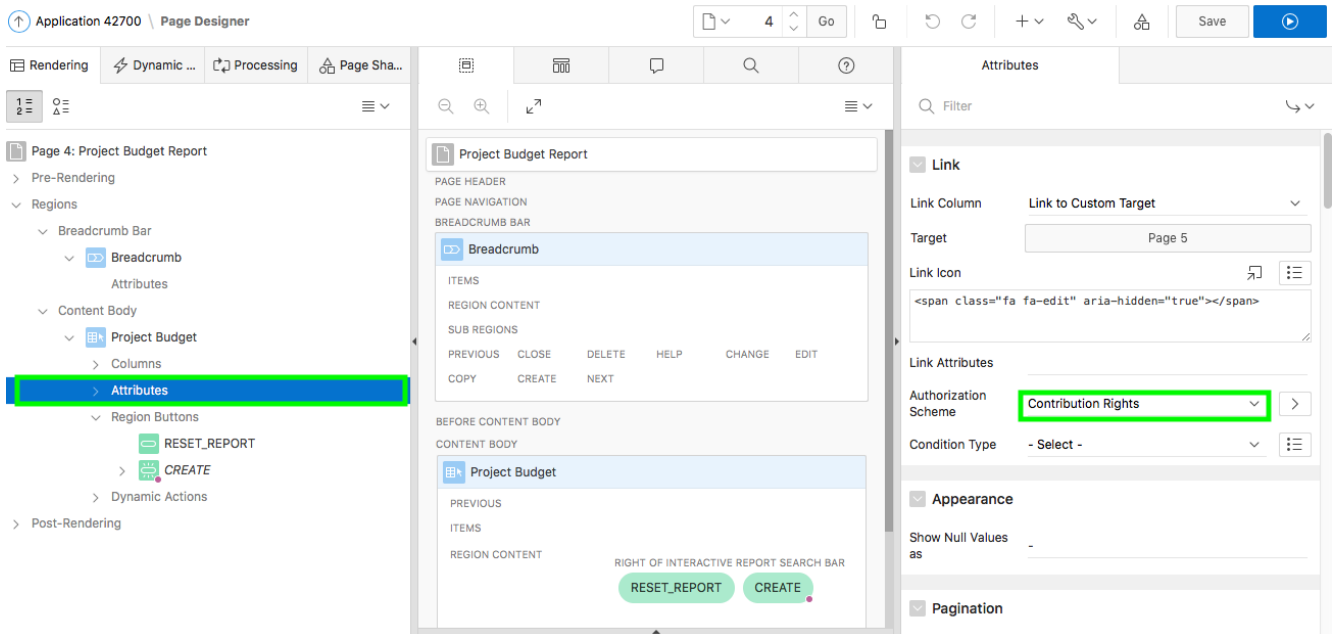
1 - 4

## 23. Now, you are ready to define and apply the authorization schemes to each application component.

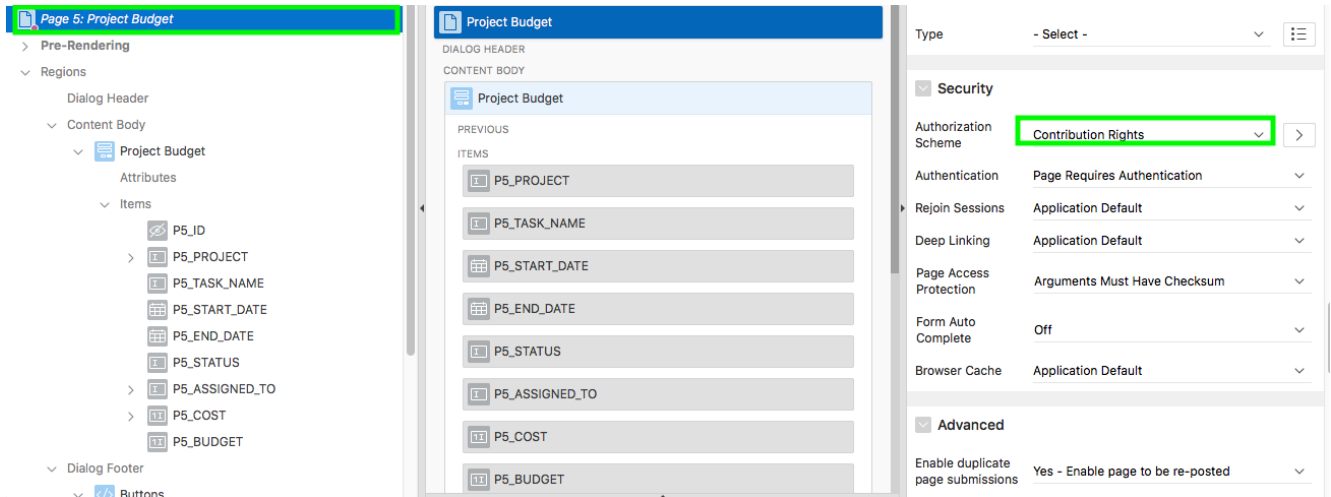
- Users with the Administrator privilege can make any changes, including administering the Budget App application
- Users with the Contributor privilege can modify the data in the report but cannot make changes to the application mode and the access control list.
- Users with the Reader privilege can review the interactive report but cannot modify the data.

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

24. Under Rendering, expand **Regions**. Under the **Project Budget** region, select **Attributes**. In the property editor, locate **Authorization Scheme** and make sure that **Contribution Rights** is selected from the list.



25. 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 make sure that **Contribution Rights** is selected for Authorization Scheme. Click **Save**.
26. You also want to protect against direct access to the Project Budget form dialog page. Though you restrict end users from editing the interactive report on the Home page, they can still access the Project 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 Project Budget form page in page designer.
27. Under Rendering, select **Page 5: Project Budget**. In the Property Editor, navigate to **Security** and make sure **Contribution Rights** is selected for Authorization Scheme. Click **Save**.



28. In the page designer, enter **4** in the Page Finder and click **Go**.
29. In the page designer, click **Save and Run Page**.  
If you are logged in, click **Sign Out** before performing the next step.
30. Enter **apex\_dev** for Username and **apexdev123\$** for Password and click **Sign In**.
31. In the navigation menu, click **Project Budget Report**.  
Notice that apex\_dev can edit the interactive report, and also create a new project.

Project	Task Name	Start Date	End Date	Status	Assigned To	Cost	Budget
ACME Web Express Configuration	Identify server requirements	1/26/2019	1/27/2019	Closed	JOHN WATSON	300	500
ACME Web Express Configuration	Determine Web listener configuration(s)	1/28/2019	1/28/2019	Closed	James Cassidy	600	800
ACME Web Express Configuration	Run installation	1/31/2019	1/31/2019	Closed	James Cassidy	200	200
ACME Web Express Configuration	Create pilot workspace	2/2/2019	2/2/2019	Closed	John Watson	100	100
ACME Web Express Configuration	Specify security authentication scheme(s)	2/7/2019	2/7/2019	Open	John Watson	200	300
ACME Web Express Configuration	Configure Workspace provisioning	2/8/2019	2/8/2019	Open	John Watson	200	100
ACME Web Express Configuration	Select servers for Development, Test, Production	2/11/2019	2/13/2019	Open	James Cassidy	200	600

32. In the navigation menu, click **Access Control**.
33. Notice that you receive an error as you need the Administrator privilege to use the Access Control Administration page.  
Click **OK**.



## Insufficient privileges, user is not an Administrator

Access denied by Page 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: 12152948290827462625
5. component.name: Administration Rights
6. error\_backtrace:

----- PL/SQL Call Stack -----

object handle	line number	object name
0x4b84baa48	1033	package body APEX_190200.WWV_FLOW_ERROR.INTERNAL_GET_ERROR
0x4b84baa48	1101	package body APEX_190200.WWV_FLOW_ERROR.INTERNAL_ADD_ERROR
0x4b84baa48	1493	package body APEX_190200.WWV_FLOW_ERROR.RAISE_INTERNAL_ERROR
0x5069299a8	874	package body APEX_190200.WWV_FLOW_AUTHORIZATION.IS_AUTHORIZED
0x4eaa88970	4578	package body APEX_190200.WWV_FLOW.SHOW
0x506d034d8	173	procedure APEX_190200.F
0x53d5b6d20	2	anonymous block

OK

34. Click **Sign Out**.

35. Now sign in by entering **apex\_user** for Username and **lowcode123\$** for password.

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

### Project Budget Report

Project	Task Name	Start Date	End Date	Status	Assigned To	Cost	Budget
ACME Web Express Configuration	Identify server requirements	1/26/2019	1/27/2019	Closed	JOHN WATSON	300	500
ACME Web Express Configuration	Determine Web listener configuration(s)	1/28/2019	1/28/2019	Closed	James Cassidy	600	800
ACME Web Express Configuration	Run installation	1/31/2019	1/31/2019	Closed	James Cassidy	200	200
ACME Web Express Configuration	Create pilot workspace	2/2/2019	2/2/2019	Closed	John Watson	100	100
ACME Web Express Configuration	Specify security authentication scheme(s)	2/7/2019	2/7/2019	Open	John Watson	200	300
ACME Web Express Configuration	Configure Workspace provisioning	2/8/2019	2/8/2019	Open	John Watson	200	100
ACME Web Express Configuration	Select servers for Development, Test, Production	2/11/2019	2/13/2019	Open	James Cassidy	200	600

37. Click **Sign Out**.

38. Now sign in by entering **apex\_admin** for Username and **apexadmin** for password.

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

40. Notice that you can now edit the interactive report, and also create a project.

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

### Budget App

Dashboard

Project Budget Search

Project Budget Report

Calendar

Access Control

41. 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 © 2020, 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.