

## Configure designer group access

Your business scenario might require you to grant customized access to certain users who only need a subset of administration capabilities that is provided by Administration Console for Content Platform Engine (ACCE). You can create and control access to particular areas of the ACCE by implementing designer groups.

The following two types of designer groups are supported for custom access: Class Designer and Application Designer

The Class Designer group:

- limits administration console access to only the tools and settings that are used to create and modify classes
- is responsible for creating and updating the data models for an application or applications
- does not have more general capabilities, such as creating properties on the system, because changes at that level can impact other applications

The Application Designer group:

- is responsible for the various components related to creating a Content Platform Engine application
- can create properties that can affect a wider set of components (in addition to the data model capabilities of the Class Designer)
- can create and maintain workflow related configuration, including items like Rosters, Queues, Component Queues, and so on

Neither of these groups have permissions to perform Administrator functions such as managing domains and object stores. These capabilities are limited to established IBM FileNet P8 Platform administration users.

To grant custom access to designer groups, you must configure the groups in your directory server first, or designate existing groups to use. You then add the group names to a configuration file that you save to a directory that is accessible to your environment. The file and location are specified by a JVM argument. You can designate only one directory server group for each designer access group.

If you assign the same LDAP group for both designer groups, the LDAP group is given Application Designer access. If no designer group access is configured, the default administrative access persists.

To remove access restrictions from the groups, you can remove the group names from the file, or remove the file from the directory that is specified in the JVM argument.

---

## Activity: Implement designer group access

---

In this activity, you will configure access to specific areas in Administration Console for Content Platform Engine by designating Class Designer and Application Designer groups.

In your directory server, you designate or create the security groups to which you want to grant Class Designer or Application Designer access. You can use groups that are already configured. Two security groups, needed for this activity, are already created on your student system. Both groups are members of an IBM FileNet P8 Platform administration users group. To grant custom access to designer groups, you will add the group names to a configuration file in your environment, specify the file location in a JVM argument and then test the access for the two groups after applying access restrictions.

Important: This activity builds on the previous activities under the Security topics, and so ensure that the previous activities are completed.

In this activity, you will accomplish the following:

- Verify the directory server groups.
- Check the Class Design group access before the restriction is applied.
- Check the Application Design group access before the restriction is applied.
- Observe the configuration properties file.
- Set the JVM argument.
- Verify the group access after the restriction is applied.

### Verify the directory server groups.

Two groups, called ClassDesignGrp and AppDesignGrp, are configured in the directory server of your student system for this activity. Both groups are members of an IBM FileNet P8 Platform administration users group called p8admins which is also created on the student system and by default the two groups has complete access to ACCE.

- Click **Start > Administrative Tools > Active Directory Users and Computers**.

You can also use the Active Directory Users and Computers shortcut on the taskbar.



- From the **Active Directory Users and Computers** window, click the **Users** node on the left pane, and verify that the following groups are listed: **AppDesignGrp** and **ClassDesignGrp**.

Agent	Security Group - Global
AppDesignGrp	Security Group - Global
Approver	Security Group - Global
Case workers	Security Group - Global
ClassDesignGrp	Security Group - Global
Clerks	Security Group - Global

- Right-click **ClassDesignGrp** and select **Properties**.
- From the **Properties** Window, click the **Members** tab, verify that **Cathy** is listed.
- Select the **Member Of** tab, verify that **p8admins** is listed, and then click **Cancel**.
- Repeat the steps to examine the **AppDesignGrp** group and verify that **Arvin** is a member of the group.
- Repeat the steps to examine the **p8admins** group and verify that **ClassDesignGrp** and **AppDesignGrp** are members of the group.

p8admins Properties	
General	Members
Members:	
Name	Active Directory Domain Services Folder
AppDesignGrp	edu.ibm.com/Users
ClassDesignGrp	edu.ibm.com/Users
p8admin	edu.ibm.com/Users

This membership provides Cathy and Arvin complete admin rights.

- Make a note of the two group names: **AppDesignGrp** and **ClassDesignGrp**

## Check the Class Design group access before the restriction is applied.

In this task, you will sign in as the member of ClassDesignGrp (Cathy) and check her access to the ACCE features and verify her admin rights before the restrictions are applied.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**

- Type **Cathy** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

After the restriction is applied, Cathy will not be able to perform many of the administration actions, creating and configuring property templates, subscriptions, and sweep policies, and any workflow related configurations.

In the following steps, you will check that Cathy is able to perform the actions now before the restrictions are applied. Since the objective is to test the access to these actions, completing the configuration or creating an object is not required. But you can optionally complete the configuration using the tasks that you learned throughout this course.

- On the left pane of the **EDU\_P8** tab, expand the **Object Stores** folder click the **Finance** object store.

As admin users, Cathy and Arvin have complete access to all the object stores and all the admin actions same as p8admin.

- From the **Finance** tab, expand the **Finance > Administrative** node on the left pane, and verify that this node and sub-nodes are accessible to **Cathy**.
- From the **Finance** tab, collapse the **Administrative** node, expand the **Finance > Data Design** node on the left pane, right-click **Property Templates** and select **New Property Template** from the list.

This step verifies that Cathy has access to create a property template.

- Click **Cancel** to close **New Property Template** tab.
- On the left pane, collapse the **Data Design** node, expand the **Finance > Events, Actions, Processes** node, right-click **Subscriptions** and select **New Subscription** from the list.

This step verifies that Cathy has access to create a Subscription.

- Click **Cancel** to close the **New Subscription** tab.
- On the left pane, collapse the **Data Design**, and verify that Cathy has access to **Sweep Management** configuration.

You will learn more about Sweep Management in a later activity.

- Log out of Administration Console for Content Platform Engine and close the browser.

## Check the Application Design group access before the restriction is applied.

In this task, you will sign in as the member of AppDesignGrp (Arvin) and check his access to the ACCE features and verify his admin rights before the restrictions are applied.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **Arvin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU\_P8** tab, expand the **Object Stores** folder click the **Finance** object store.
- From the **Finance** tab, expand many nodes on the left pane and observe that Arvin has access to all the nodes and actions.

- Expand the **Finance > Administrative** node on the left pane, right-click **Workflow System** and select **New** from the list.

Since only one Workflow system can be created per object store, do not complete the wizard now, so that you can test it later.

After the restriction is applied, Arvin will not be able to perform some of the admin actions such as configuring a Workflow System.

- Click **Cancel** to close the **New Workflow System** tab.
- Log out of Administration Console for Content Platform Engine and close the browser.

## Observe the configuration properties file.

In this task, you observe the configuration properties file that contains the LDAP directory security groups that you want to use for designer groups. This file is already created for your student system.

- In **Windows Explorer**, navigate to the **C:\Training\F2810G** folder, right-click the **restrictedGroups.properties** file and select **Edit with Notepad++** from the list.
- Observe the following text in the file:

```
#Specify LDAP group names for ClassDesigner and
ApplicationDesigner
ClassDesigner=ClassDesignGrp
ApplicationDesigner=AppDesignGrp
```



Recall the Active Directory group names that you checked:

- AppDesignGrp is your designated LDAP Group for Application Designers
- ClassDesignGrp is your designated LDAP Group for Class Designers

You can designate only one directory server group for each designer group.

If Content Platform Engine is in a cluster environment, the file must be available to every node. In this scenario, a location on a shared network drive is recommended to keep access groups in synch.

- Close the file.

## Set the JVM argument.

In this task, you will set generic Java Virtual Machine (JVM) arguments in the administration console for WebSphere Application Server. The generic JVM arguments are used to configure and adjust how the JVM executes. Once changes are made and saved to the master configuration, the JVM requires a restart for the arguments to take effect.

- In the **Mozilla Firefox** browser, click the **WAS** bookmark or enter the following URL: **<https://vclassbase:9043/ibm/console/logon.jsp>**
- Type the following values for user ID and password and then click **Log In**.
  - User name: **wasadmin**
  - Password: **FileNet1**
- Click **Log In**.
- In **WebSphere Integrated Solutions Console**, on the left pane, expand **Servers** > **Server Types** and then select **WebSphere application servers**.
- On the right pane, click the **server1** link.

This is the server for Content Platform Engine.
- On the **server1** page > **Configuration** tab, scroll down, under the **Server Infrastructure** section on the right pane, expand **Java and Process Management** and then select **Process definition**.
- Under the **Additional Properties** section on the right, click **Java Virtual Machine**.
- Scroll down to the textbox for **Generic JVM arguments** and notice that the following entries are already listed.

-Duser.language=en -Duser.region=US -Duser.country=US

Each JVM argument is separated by a space (delimiter).

- Enter a space and then type the following text in the textbox.

`-DrestrictedGroups=C:/Training/F2810G/restrictedGroups.properties`

Generic JVM arguments
<code>-Duser.language=en -Duser.region=US -Duser.country=US</code> <code>-DrestrictedGroups=C:/Training/F2810G/restrictedGroups.properties</code>

- Scroll down and click **OK**.
- When the **Save** link becomes available at the top of the page, click **Save** to save it to master configuration.

You will restart the server in the following steps.

- On the left pane, expand **Servers > Server Types** and then select **WebSphere application servers**.
- From the **Application servers** page on the right pane, select **server1** row by selecting the checkbox on the **Select** column and then click **Stop**.

- When you are prompted to stop the server, click **OK**, wait for the server to stop, and then click **OK** again to close the page.

On the Application servers page, the stop status for server1 is shown with a red X icon on the Status column.

- Select **server1** row again by clicking the checkbox on the **Select** column and then click **Start**.

Wait for the server to start. On the Application servers page, the start status for server1 is shown with a green forward arrow icon.

Occasionally, after a JVM configuration change, you might find that there is a long delay to start the server. If this happens, refresh the page and start the server again.

- Log out of the administration console and close the browser.

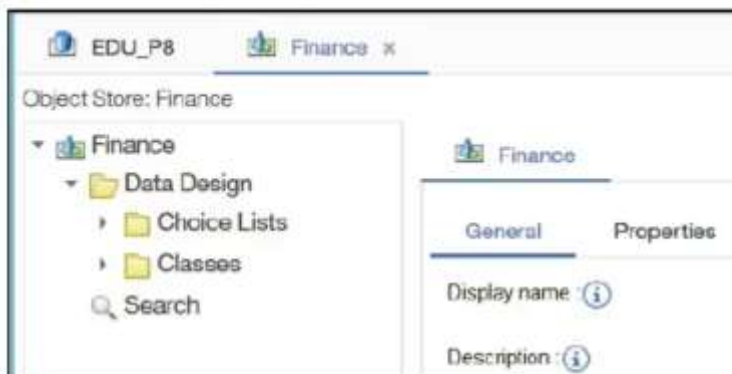
## Verify the group access after the restriction is applied.

In this task, you will sign in as members of the ClassDesignGrp (Cathy) and AppDesignGrp (Arvin) groups and check their group access to the design capabilities of ACCE.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **Cathy** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU\_P8** tab, expand the **Object Stores** folder and click the **Finance** object store.
- On the **Finance** tab, verify that you only view the **Finance > Data Design** node and **Search** on the left pane.

Recall that the same user was able to view all other features before applying the restrictions, including the actions under the Administrative, Events, Actions, Processes, and Sweep Management nodes.

- In the **Finance** tab, expand the **Finance > Data Design** node and verify that only **Classes** and **Choice Lists** node are shown.



Recall that the same user was able to create property templates under the Data Design node.

Observe that on the right pane, only two subtabs are accessible: General and Properties. Most other subtabs that help in administration of this object store is not available to this group.

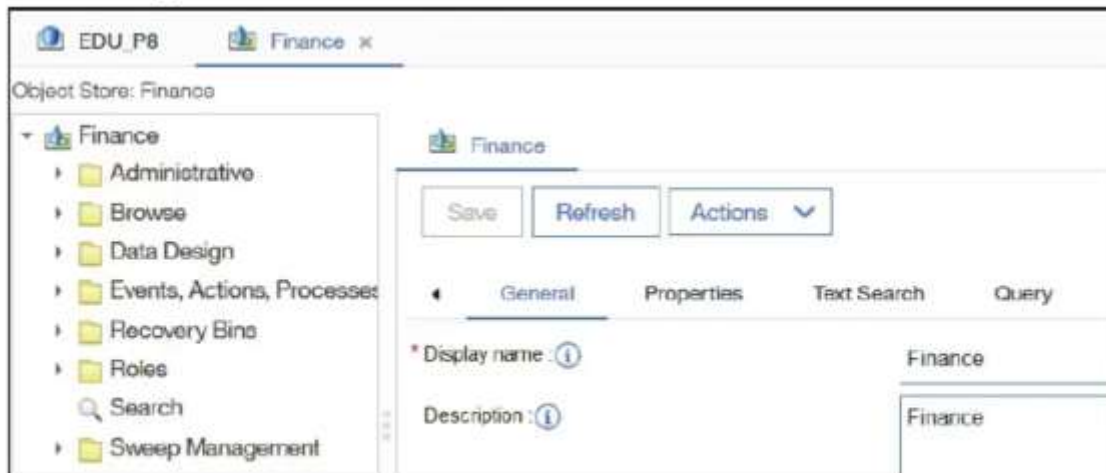
Class Designers group (ClassDesignGrp) are allowed to perform only the data design tasks and will not be able to perform the administration tasks.

- Log out of the administration console, log back in as **Arvin** (Password: **FileNet1**).
- On the left pane of the **EDU\_P8** tab, expand the **Object Stores** folder and click the **Finance** object store.
- On the **Finance** tab, verify that many nodes are accessible on the left pane, under the **Finance** node.

Application Designers group (AppDesignGrp) are allowed to perform many administration tasks, in addition to data design, as compared to the Class Designers group (ClassDesignGrp).

Observe that on the right pane, many subtabs are accessible to Arvin as compare to the Cathy.





- From the **Finance** tab, expand the **Finance > Administrative** node on the left pane, right-click **Workflow System** and select **New** from the list.

The Workflow topic is discussed in a separate course. For this activity, the objective is to test the access to this feature for an Application Designer.

- On the **New Workflow System** tab, under the **Table Spaces** section, type **OS\_DB\_TS** for the **Data** field.
- Under the **Workflow System Security Groups** section, click **Browse** next to the **Administration group**.
- On the **Add Users and Groups** page, search for **P8admins**, move it to the **Selected Users and Groups** pane, and then click **OK**.
- Back on the **New Workflow System** tab, click **Next**.
- For the **Connection point name** field, type **FinanceCP3** and then click **Next**.
- For the **Isolated region name** field, type **FinanceRegion**, scroll down to the **Isolated region number** field, and then type **3**.
- Click **Next** and then on the **Specify Isolated Region Table Space (Optional)** page, click **Next** again.

- On the **Summary** page, click **Finish**.

Observe that you get an error with the message: the requester has insufficient access rights to perform the requested operation.

Error
<b>FNRAC1001E</b> An unexpected error occurred.
<b>User response:</b> Check the error details for more information and contact IBM Software Support if necessary.
<b>Exception details:</b>
 The requester has insufficient access rights to perform the requested operation.

Because of the restrictions applied, Arvin cannot configure a Workflow system.

- Click **OK** to close the Error page and then click **Cancel** to close **New Workflow System** tab.
- Log out of the administration console and then close the browser.

Optionally, you can further the testing by removing the restriction and verifying if Arvin is able to create a Workflow system.

To remove access restrictions from the groups, remove the group names from the file, or remove the file from the directory that is specified in the JVM argument.