# Secure content with role-based access

A role can define different types of access for different objects. When you create roles, you configure role permissions by specifying classes of objects and the types of access permissions to those objects. For example, an administrator role might grant modify properties and create children (folders and documents) access for folder objects. Security for an object includes any associated roles plus normal access permissions.

## Benefits of role-based access

Role-based access provides the following benefits:

- Multiple role permissions for a single object

  Many roles can be associated with an object. Each role encapsulates a set of access rights. For example, a Content Developer role might have Write access while a Reviewer role might have only Read access. If user is a member of many roles, the rights granted by each role are combined.

  Role permissions can be applied directly, introduced by a security template, inherited, or created as the default access scheme.

- A single role with multiple access definitions

  A single role can define different access to different types of objects. For example, a role can define one set of permissions for Documents and another set of permissions for Folders.

  You can change role-based access without sweeping through all applicable objects. You can easily determine which roles are associated with an object. Role associations are displayed on the Security tab along with other ACL entries.

- The Content Platform Engine (CPE) administrator manages access changes

  Changing LDAP group membership requires LDAP administration permission and tools. With role-based access, a CPE administrator can use the Administration Console for Content Platform Engine to change the membership of a static role. These access updates can also occur more quickly than LDAP updates.

- Introduce Custom logic

  A Dynamic Role offers the opportunity to incorporate custom logic into access control decisions. Dynamic roles enable you to specify the users or groups in the role within a code extension, rather than statically storing them in Content Platform Engine.

- Use in an IBM Content Navigator (ICN) Entry template

  Using role-based access can simplify entry template usage. You can designate a role for the entry template, and the role can be updated with user and group changes without having to update each entry template or existing document added by a template.

  Note: This role capability is exposed only in entry templates in ICN.

## Role classes

Roles are created as classes that exist in and apply to a specific object store.

A default class called Roles provides two subclasses. To create a new role, you must create a new subclass first from either the Static Role subclass or the Dynamic Role subclass.

- Static role

  A static role contains users and groups that are assigned directly to the role. The behavior of a static role is similar to the way ACLs are assigned to an object.

- Dynamic Role

  A dynamic role uses external code to determine whether a user is a member of the role. This approach enables more dynamic role assignments that are based on application use cases. In a dynamic role, the role membership handler, the `isUserInRole` method, returns a Yes or No response to the question of whether the specified user is a member of the role.

## Considerations when implementing roles

Role-based access control works best in an environment where there is a high ratio of controlled objects to role instances. A model in which there are only a few objects controlled by each role will generally perform less well and is not recommended.

For more information on the process of evaluating access with roles, refer to the IBM FileNet P8 Platform V5.5.x Knowledge Center:
https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psa081.htm

# Activity: Configure role-based access

You can create roles that determine what access the users in that role have to objects in your object store. Roles are created as classes and they exist in and apply to a specific object store.

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:

- Preparation: Create a Document class.
- Preparation: Add a folder and a document.
- Test the security of a document before a role is applied.
- Create a role subclass.
- Create a static role.
- Associate the role instance with a document object.
- Test the security of the document after a role is applied.

## Preparation: Create a Document class.

In this task, you will create a property template and a Document class and set the default instance security to use it for the following tasks.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** 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 the **Data Design** node on the left pane, right-click **Property Templates**, and then click **New Property Template**.
- From the **New Property Template** tab on the right pane, type **DocCategory** for the **Display name** field.

  The Symbolic Name and Description fields are automatically populated.
- Click **Next** and then, for the **Data type** field, select **String** from the list.
- Click **Next** two more times and then for the **Single or multi-value** field, select **Single**, and click **Next**.

- On the **Summary** page, click **Finish** and then click **Close** on the **Success** page.
- On the **Finance** tab, click **Refresh**.
- Expand the **Data Design > Classes** node on the left pane, right-click **Document** and then click **New Class**.
- On the **New Document Class** tab, type **Finance Docs** for the **Display name** field.
  The Symbolic Name and Description fields are automatically populated.
- Complete the wizard by clicking **Next**, **Finish**, and then **Close**.
- In the **Finance** tab, click **Refresh**.
- On the left pane, expand the **Data Design** > **Classes** > **Document** node, and then click **Finance Docs**.
- From the **Finance Docs** tab on the right pane, click the **Property Definitions** subtab and then click **Add**.
- On the **Add Properties** page, type **DocCategory** in the filter field to select the property template that you added.
- Select **DocCategory**, scroll down, and then click **OK** to close the **Add Properties** page.
- On the **Finance Docs** tab, verify that **DocCategory** is listed and then click **Save**.
- Click **Refresh**, open the **Default Instance Security** subtab, remove all the users and groups except **p8admins** and **p8admin**.
- Click **Add Permissions** and then select **Add User/Group Permission**.
- On the **Add Users and Groups** page, search for **Finance managers**, select it from the **Available Users and Groups** pane, and move the group to the **Selected Users and Groups** pane by clicking the forward arrow.
- Select **Finance managers** the **Selected Users and Groups** pane, scroll down to the **Permissions** section, select **Full Control** for the **Permission group** field, and then click **OK**.
- On the **Finance Docs** tab, click **Save**.
- Repeat the steps to add **Finance clerks and Finance reviewers** with **View content <Default>** for the **Permission group.**
- On the **Finance Docs** tab, click **Save**.

- Under the **Access Permissions** section, verify that the security groups are listed with the Permission Group you configured.

| Name | Source | Permission Type | Permission Group |
|---|---|---|---|
| Finance clerks | Direct | Allow | View content <Default> |
| Finance managers | Direct | Allow | Full Control |
| Finance reviewers | Direct | Allow | View content <Default> |
| p8admins | Direct | Allow | Full Control |
| p8admin | Direct | Allow | Full Control |

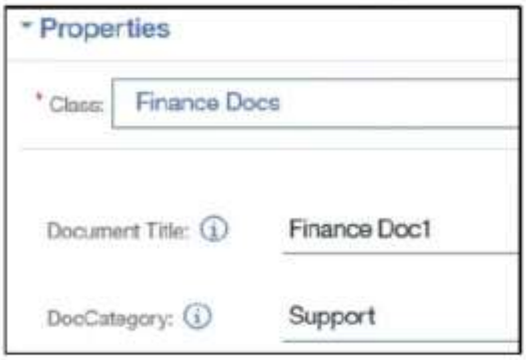
- Log out of the Administration console and close the browser.

## Preparation: Add a folder and a document.

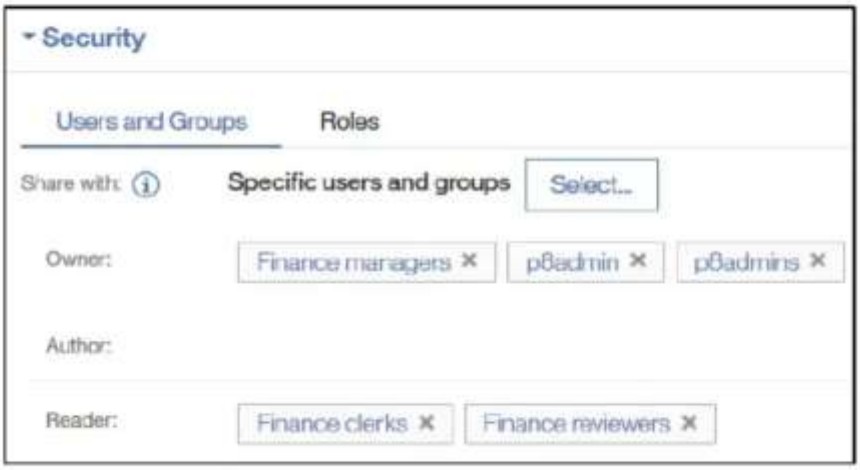
In this task, you will log in to the IBM Content Navigator (ICN) desktop as P8admin, add a folder and a document to test the access in the following tasks.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **P8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the **Browse** page, click **New Folder** from the toolbar.
- On the **New Folder** page, type **Finance Docs** for the **Folder Name** field.
- Under the **Security** section, for the **Reader** field, leave **p8users** and remove the other groups.
- Click **Select** next to **Specific users and groups**.
- On the **Add permissions** page, select **Groups** for the search for field, and then search for the **Finance admins** group.
- Select **Finance admins** from the **Available** pane and then move the group to the **Selected** pane by clicking the forward arrow.
- Scroll down, select **Owner** for the **Permissions** field, and then click **Add**.
- Repeat the steps to add **Finance reviewers and Finance clerks** with **Reader** level permissions.
- On the **New Folder** page, click **Add** in the lower right to create the folder.

- Back on the **Browse** page, double-click **Finance Docs** to open the folder and then click **Add Document** from the toolbar.
- On the **Add Document** page, for the **What do you want to save?** field, select **Local Document** from the list and then click **Browse**.
- On the **File Upload** page, select any file (Example: **MarketingPlan5.pdf**) from the **C:\Training\F2810G\SampleDocs** folder and then click **Open**.
- Back on the **Add Document** page, Select **Finance Docs** for the **Class** field.
- For the **Document Title** field, change the text to **Finance Doc1** and then type **Support** for the **DocCategory** field.




- Under the **Security** section, verify that this document has the default instant security from the Document class that you created earlier.




- Verify that the **Finance clerks** and **Finance reviewers** have **Reader** access.

You will be changing this security through role-based access.

- Click **Add** in the lower right corner and then back on the **Browse** page, verify that the new document is listed.
- Log out of ICN **Finance Desktop** and then close the browser.

## Test the security of a document before a role is applied.

In this task, you will log in as a member of the Finance clerks group (Carol) to test the access to a document in the ICN desktop before applying role permissions to the document.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or type the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **Carol** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the **Browse** page, double-click **Finance Docs** to open the folder.
- Right-click the **Finance Doc1** document that you added and then verify that Carol does not have permissions to check out the documents.

  The actions are grayed out (not enabled) in the list in contrast to Download, Add to Favorites, or Export for which Carol has permissions.

  Finance clerks group (Carol) has **Reader** access and so they cannot check out a document.
- Log out of ICN **Finance Desktop** and then close the browser.

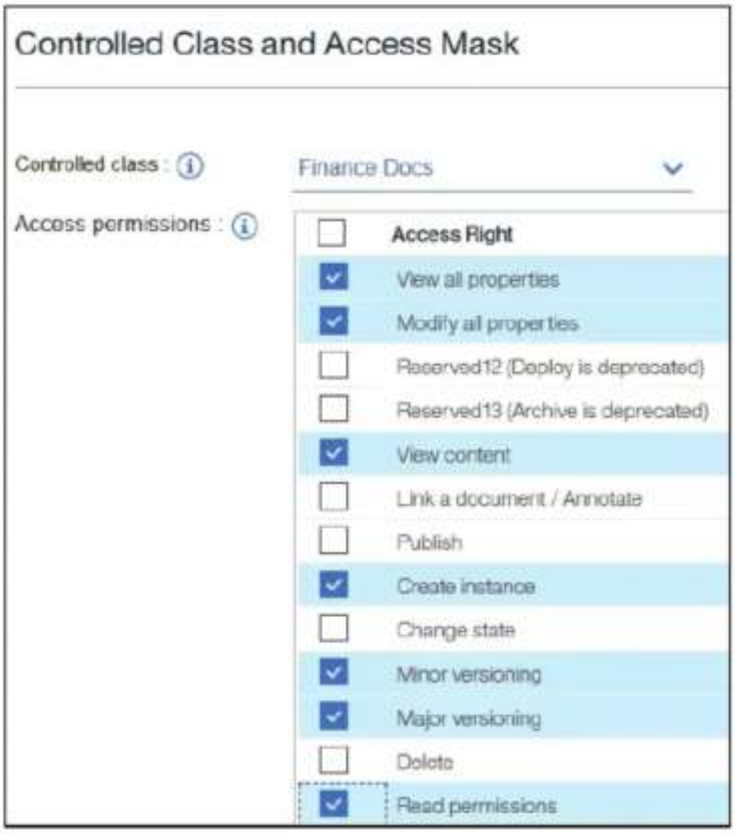
## Create a role subclass.

To create an instance of a role, you must first create a subclass of the Role class. In this task, you will create a subclass for the role. You will specify the document class on which this role is applied, and the access rights.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** 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 the **Finance** > **Data Design** > **Classes** > **Other Classes** > **Role** node on the left pane.
- Right-click **Static Role** and select **New Class** from the list.
- On the **New Static Role Class** tab, type **EduRole** for the **Display name** field and press enter.

  Verify that the Symbolic name and the Description fields are automatically populated.
- Click **Next** and then click **Finish** in the **Summary** page.
- On the **Success** page, click **Open** to open the new Role class that you created.

  You will edit this class to add access definitions in the next step.
- In the **EduRole** tab, click **Refresh**, select the **Role Access Definitions** subtab, and then click **Add**.
- In the **Controlled Class and Access Mask** page, select **Finance Docs** for the **Controlled class** field and then select the following access rights for the **Access permissions** field:
  - **View all properties**
  - **Modify all properties**
  - **View content**
  - **Create instance**
  - **Minor versioning**
  - **Major versioning**
  - **Read Permissions**




- Scroll down and then click **OK**.

  You can add more access definitions or remove any of the existing ones.

- On the **EduRole** tab, click **Save** and then click **Close.**
- From the **Finance** tab, click **Refresh** and then verify that the new class **(EduRole)** is added under **Data Design** > **Classes** > **Other Classes** > **Role** > **Static Role** node.

  This class is now available to create instances of roles.

## Create a static role.

In this task, you will create a role instance from the Static Role subclass (that you created in the previous task) and add role members.

- On the left pane, collapse the **Data Design** node, and then expand the **Roles** node.
- Right-click the **Static Roles** node and then select **New Static Role** from the list.
- From the **New Static Role** tab on the right pane, type **Content Dev Role** for the **Display name** field and then scroll down.
- Scroll down, for the **Static role class** field, if it is already not selected, select **EduRole** from the list, and then click **Next**.

  On the Setup Role Members page, you can add users and groups (principal), add a realm, or add a nested role. For a nested role, you can add an existing role to this one.
- On the **Setup Role Members** page, click **Add Principal**.
- In the **Add Users and Groups** page, type **Carol** in the **Search by** field and then click **Search**.
- Select **Carol** from the **Available Users and Groups** pane, click the forward arrow to move to **Selected Users and Groups**, and then click **OK**.
- On the **Setup Role Members** page, verify that **carol@edu.ibm.com** is added under the **Role Member** section.

  You can add many members to this role. You can also add groups. For this activity, you are adding one of members of the Finance clerks group.
- Click **Next**, click **Finish** on the **Summary** page, and then click **Close** on the **Success** page.

  The role instance that you created in this task grants the permissions to the specified classes that you configured on the role class.
- On the **Finance** tab, click **Refresh**.

## Associate the role instance with a document object.

You created a role instance in the previous task. In this task, you will assign this role instance to a document object to secure it with role-based access control.

- On the left pane, expand the **Finance** > **Browse** > **Root Folder** node and click the **Finance Docs** folder.
- From the **Finance Docs** > **Contents** subtab on right pane, click the **Finance Doc1** document link.
- On the **Finance Doc1** tab, click **Refresh** and then select the **Security** subtab.

  Notice that the Finance clerks group (with View content permissions) is already listed for this document. Carol is a member of Finance clerks. Finance clerks do not have permission to check out the documents as you verified for Carol before. Carol will be able to do these tasks after the role access is added.
- From the **Security** subtab, click **Add Permissions** and then select **Add Role Permission** from the list.
- In the **Add Role Permission** page, type **Content Dev Role** in the **Display name** field, click **Search** and then select **Content Dev Role** (by selecting the checkbox next to it).
- Scroll down, select **This Object only** for the **Apply to** field, and then click **OK**.
- On the **Finance Doc1** tab, verify that the **Content Dev Role** is added to the **Access Permissions** list and the **Permission Type** column shows **EduRole**.

| Name | Source | Permission Type | Permission Group |
|---|---|---|---|
| Finance clerks | Direct | Allow | View content <Default> |
| Finance managers | Direct | Allow | Full Control |
| Finance reviewers | Direct | Allow | View content <Default> |
| p8admins | Direct | Allow | Full Control |
| Content Dev Role | Direct | EduRole | |

- Click **Save** and then click **Close**.
- Log out of the administration console and close the browser.

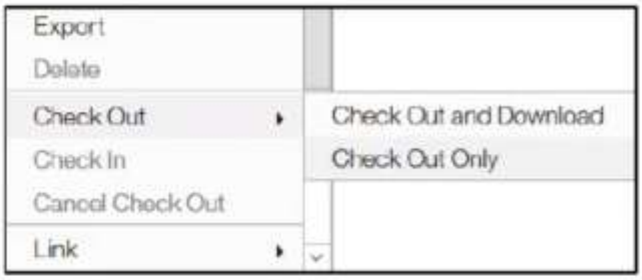
## Test the security of the document after a role is applied.

In this task, you will log in as Carol to test the access to a document in the ICN desktop after applying role permissions to the document.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or type the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **Carol** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the **Browse** page, double-click **Finance Docs** to open the folder.
- Right-click the **Finance Doc1** document and then verify that Carol now has permissions to check out the documents.

  The checkout action is not grayed out and it is enabled now.

  This is the same document you used to test the security before applying the role permission.




- Log out of ICN **Finance Desktop** and then close the browser.