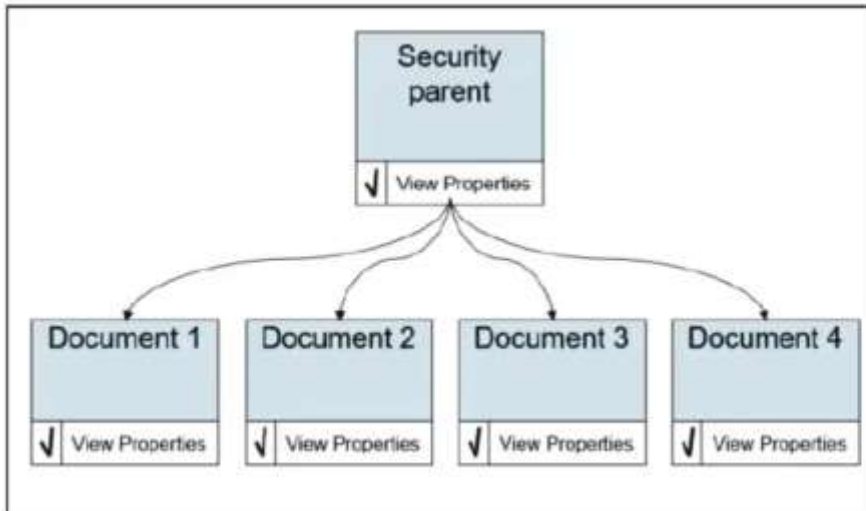


Configure security inheritance

You can configure security to be inherited from other objects. Inherited security is a customizable mechanism and a convenient way to control security on multiple objects from a single point.

Overview of security inheritance

If you specify a security parent for a large group of documents, then you can change permissions on all of these documents by updating the security parent.



In an example scenario, your company has thousands of Invoice documents. A corporate decision mandates that Invoice documents can be viewable by all Finance Clerks. You add Finance Clerks to the security parent for the entire Invoice document class. The new permission is inherited by all Invoice documents. With one change, you gave Finance Clerks access to all Invoice documents.

Definition of terms

Security inheritance

Security inheritance refers to the passing of permissions from a parent object to a child object.

Inheritable depth

A property that determines whether permissions are not to be inherited, inherited only by objects that are immediate children, or inherited by all children

Security parent

Any object from which another object inherits security

Security folder

A folder that is used to provide the security for child documents to inherit

Security proxy

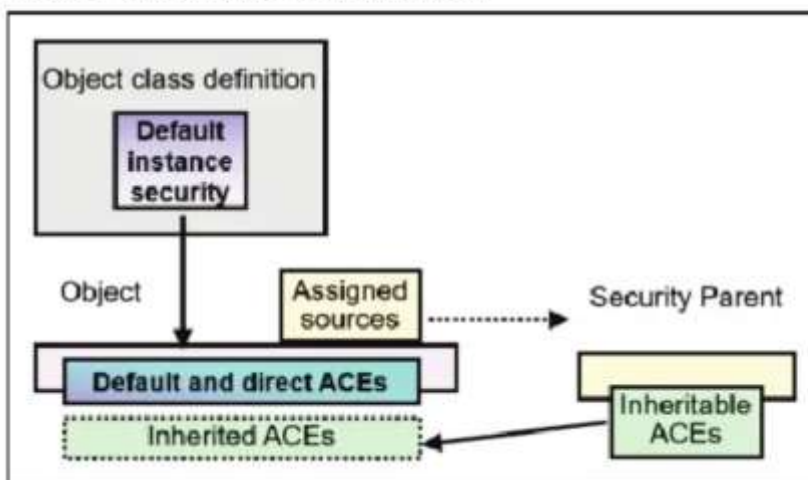
An object that is used to provide the security for other objects to inherit

Security inheritance architecture

An object's security is a combination of its default instance security, direct ACEs, and the ACEs from the security parent.

Security inheritance architecture

An object's security is a combination of its default instance security, direct ACEs, and the ACEs from the security parent.



This diagram illustrates how inherited ACEs are applied to an object:

- The object class definition has default instance security. When an object of that class is created, the default instance security of the class applies.
- In addition to direct ACEs, the object can inherit permissions from a parent object. Inherited permissions are added to existing permissions.
- If you use Denials, direct permissions are evaluated first, then inherited permissions.

When security changes on a security parent, the changes are not immediately reflected on the objects that use the parent as a security source (that is, their ACLs do not change) for performance reasons. Inherited security is computed when the object is accessed. Waiting to check the inherited security until the last step in the process is much more efficient than updating all of the security children each time a security parent is updated.

Characteristics of inherited permissions

The following list shows the characteristics of the inherited permissions:

- If you change inheritable permissions on a security parent, it changes permissions on all versions of a security child.
- You cannot directly modify inherited permissions on the child object.
 - The permissions must be modified on the security source object.
 - Inherited permissions are displayed as disabled (for editing) in security interfaces.
- If you delete a security parent, the inherited permissions are removed from the child objects.

Methods for configuring security inheritance

The following two methods are available for setting up security inheritance in an object store:

- Security folder
 - The security folder method uses folders to set security on objects
 - Inheriting objects have one folder as the security parent
 - The security folder property is set on the inheriting object
- Security proxy
 - The security proxy method can use any class of object as a security parent
 - Inheriting objects can have multiple security sources of this type
 - The security proxy type property is set on the inheriting object

Use a security folder

You can set the security folder property in one of the following ways:

- Inherit security from folder

The inherit security from folder method requires that the object is filed in that folder, but does not require that you copy the object reference.
- Security folder

The security folder property method requires you to copy and paste an object reference, but does not require that the object is filed in that folder.

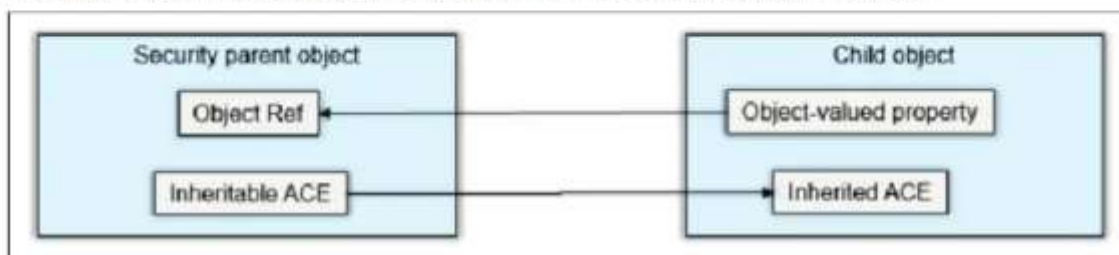
Folder security inheritance can be automated by using a custom application and the Security Folder property value can be assigned to documents automatically.

Following are the consequences of deleting folders or moving child objects:

- If a security folder is deleted, those documents that had that folder as their security parent in the object store no longer have a setting for security folder. They can be reassigned to another security folder.
- If an object that has a security parent is moved out of that folder, the security parent relationship is maintained.

Use an object as a security proxy

This method is more complex than using the security folder method, but it provides more flexibility. You can specify as many security parents as you need, and the security sources are not limited to being folders. For some business applications, the freedom to use other objects besides folders might allow for a more natural and simpler solution. This method can also be combined with the security folder method so that the final security on an object includes the inherited security from all sources.



The following are the high-level steps to create a security proxy:

- Create a security parent object with inheritable permissions
- Create a custom object-valued property (OVP)
 - Single-valued
 - Security proxy type is inherited
- Add a custom property to the child class
 - For required class, select the exact class of the parent object
- Assign the security parent in one of these ways:
 - Specify the value of the OVP on the child object
 - Specify the default value of the OVP on the child object class

When the security parent object is deleted, the inherited security is removed from the object.

Example scenario

A legal requirement exists for contracts that are used in the Finance department. From time to time, contracts must be viewable by auditors, who do not usually have access to the contracts. You want to be able to change the security on all of the contracts to allow auditors to access them, and then to remove that access when the audit ends.

Many folders act as security sources for the contracts that are filed within them, and other document types are also filed in these same folders and inherit security from them. You do not want to manually change the security on all of the folders, and you do not want the auditors to have access to the other documents that are filed in those folders. Therefore, you cannot change the security on the folders when the auditors need access to the contracts.

You can set up a custom property on a document class so that all contracts have a property that specifies the security proxy from which to inherit security. In this way, you can allow the documents to use their folder as a security parent, and provide an extra level of access that can be disabled or modified when needed.

Activity: Configure security inheritance

Your business solution requires that the security of some documents must be determined by the security of a folder or another object. In this activity, you will create a folder and use folder inheritance to secure documents.

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.
- Create a parent folder.
- Create and configure a document to inherit security.
- Test security inheritance.

Preparation: Create a document class.

To have security that is completely controlled by inheritance, you must eliminate the default instance permissions. To set up the tasks for this activity, you will create a document class that has no default instance permissions.

- 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 > Classes** node on the left pane, right-click **Document** and then click **New Class**.

- On the **New Document Class** tab on the right pane, type **Receipt** for the **Display name** field and then click **Next**.
- Click **Finish**, and then click **Open** to open the class for editing.
- Open the **Default Instance Security** subtab and then click **Refresh**.
- Under the **Access Permissions** section, select all entries except **p8admin** and **P8admins**, click **Remove**, and then click **Save**.
- Click **Refresh**, verify that only **p8admin** and **p8admins** are listed, and then close the **Receipt** tab.

Create a parent folder.

In this task, you will create the folder from which the receipts documents inherit permissions, and add inheritable security settings.

- From the **Finance** tab, expand the **Browse** node on the left pane, right-click **Root Folder** and then click **New Folder**.
- On the **New Folder** tab, type **Receipts** for the **Folder name** field, and then click **Next** two times.
Leave default values for all other fields.
- Click **Finish**, click **Open** to open the class for editing, and then click **Refresh**.
- Open the **Security** subtab for the folder and then click **Add Permissions > Add User/Group Permission**.
- On the **Add Users and Groups** page, search for **Finance**, select **Finance managers** from the **Available Users and Groups** pane, and then move it to the **Selected Users and Groups**.
- Select **Finance managers**, scroll down to **Permissions** section, and then verify that **Allow** is selected for the **Permission type** field.
If it is not already selected, select **Allow** from the list.
- For the **Apply to** field, select **All children, but not this object** from the list.
- For the **Permission group** field, select **Full Control** and then click **OK**.
- Back on the **Receipts** tab, click **Save** and then click **Refresh**.
- Verify that the **Finance managers** row is listed and shows **Full Control** for the **Permission group** field.
- Repeat the steps to add the **Finance admins** group, and select **Full Control** for the **Permission group** field.
- Click **Save** and then click **Refresh**.

- Verify that the Finance admins and Finance managers groups have full control.

<input type="checkbox"/>	Name	Source	Permission Type	Permission Group	Apply To
<input type="checkbox"/>	Finance admins	Direct	Allow	Full Control	All children, but not this object
<input type="checkbox"/>	Finance managers	Direct	Allow	Full Control	All children, but not this object
<input type="checkbox"/>	p8admins	Direct	Allow	Full Control	This object only
<input type="checkbox"/>	p8admin	Direct	Allow	Full Control	This object only
<input type="checkbox"/>	p8users	Direct	Allow	View properties <Default>	This object only
<input type="checkbox"/>	Script testers	Direct	Allow	View properties <Default>	This object only

- Leave the administration console open for the next activity.

Create and configure a document to inherit security.

In this task, you will add a document of the Receipt class and configure it for the security inheritance.

- On the **Receipts** tab, click **Actions > New Document**.
- From the **New Document** tab, type **Test Receipt** for the **Document title** field and then select **Receipt** for the **Class** field.
- Verify that the **With content** option is selected and then click **Next**.

* Document title: ⓘ	Test Receipt
* Class: ⓘ	Receipt
	<input checked="" type="checkbox"/> With content ⓘ




- On the **Document Content Source** page, click **Add** and then click **Browse** on the **Add Content Element** page.
- On the **File Upload** page, navigate to the **C:\Training\F2810G\SampleDocs** folder, select a file (For example, **MarketingPlan1.pdf**), and then click **Open**.
- Back on the **Add Content Element** page, click **Add Content**.
- Back on the **New Document** tab, click **Next** several times and then click **Finish**. Leave the default settings for all other fields.
- On the **Success** page, click **Open** to open the **Test Receipt** document properties page and then click **Refresh**.

- Open the **Security** tab and then verify that the only ACEs listed are **P8admins** and **P8admin** as you configured earlier for this document class.
- On the **Test Receipt** tab, open the **General** subtab, scroll down, and then select **Receipts** from the list for the **Inherit security from folder** field.

inherit security from folder : ⓘ

Receipts

- Click **Save** and then open the **Security** subtab of the **Test Receipt** document.
- Click **Refresh** and then verify that **Finance admins** and **Finance managers** have inherited permissions and the **Source** column has **Inherited** as the value.

<div> <div>Add Permissions... ▼</div> <div>Edit...</div> <div>Remove</div> </div>				
<input type="checkbox"/>	Name	Source	Permission Type	Permission Group
<input type="checkbox"/>	 Finance admins	Inherited	Allow	Custom
<input type="checkbox"/>	 Finance managers	Inherited	Allow	Custom
<input type="checkbox"/>	 p8admins	Default	Allow	Full Control
<input type="checkbox"/>	 p8admin	Default	Allow	Full Control

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

Test security inheritance.

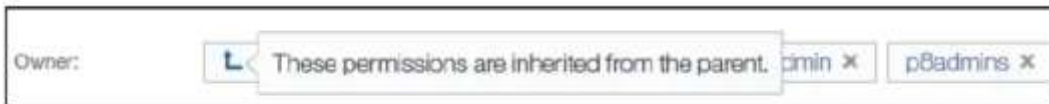
In this task, you will check the security inheritance of the document in the IBM Content Navigator (ICN) desktop by logging in as Adam, who is a member of the Finance admins group.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or type the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **Adam** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the **Browse** page, expand **Finance**, and then click the **Receipts** folder.
- Right-click the **Test Receipt** document and then select **Properties** from the list.

- Open the **Security** tab and then verify that **Finance managers**, **Finance admins**, **p8admin** and **p8admins** are all owners.



- Hover the mouse over **Finance admins** or **Finance Manager** (near the upward arrow) to verify that the permissions are inherited from the parent. The groups also have an inheritance indicator (Blue arrow).



- Click **Cancel**, log out of ICN **Finance Desktop**, and then close the browser.