<https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#createRole>

This recipe provides a step-by-step guide to implement a sample FileNet Content Manager configuration to allow or prevent users from creating documents and folder instances using role-based security.

Contents

* [Ingredients](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#Ingredients)
* [Introduction](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#introduction)
* [Login to the Administration Console for Content Platform Engine (ACCE)](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#loginAcce)
* [Create and configure the roles classes](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#createRole)
* [Create and configure the roles instances](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#createRoleInstance)
* [Configure the security of Document and Folder classes](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#configSecurity)
* [Test your recipe!](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#Test)
* [Useful resources](https://community.ibm.com/community/user/automation/blogs/massimiliano-carra/2021/09/27/recipe-managing-filenet-documents-and-folders#Resources)

Overview

Skill Level: Intermediate

Some FileNet administrator skills are needed (i.e. creating document/folder classes and configure security)

Ingredients

* FileNet Content Manager v5.5.0 or above;
* a web browser;
* administrator access to a FileNet Object Store;
* three users defined in the LDAP server called bianchi, rossi and verdi (these are the names used in the recipe, feel free to use different names);
* some basic FileNet administration knowledge (i.e. you need to know how to create a document or folder class and to configure their security).

Step-by-step

1. Introduction

FileNet Content Manager v5.5.0 provides FileNet administrators a new feature that allow users to manage access to repository objects in a new way. This feature is called Role-Based Security and allow to assign LDAP users and group to roles managed by FileNet. Role-Based Security provides several benefits, including the following:

* + Role-Based Security allows to modify roles’ membership in FileNet using the Administration Console for Content Platform Engine instead of managing users and groups in the LDAP server which requires additional authorizations and tools;
  + Role-Based Security allows to specify users and groups in a given role dynamically, using a code extension.

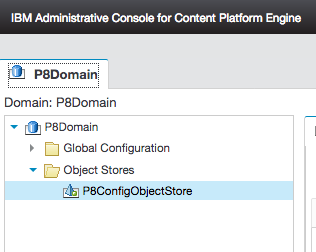
Once your course will be cooked, if you followed the recipe closely, your FileNet system will be configured with 3 users belonging to 3 different roles; based on the roles configuration they will have different privileges on a given Folder and/or Document class.

* + Mario Bianchi (bianchi) user will be able to create new instances of a given Folder and/or Document class.
  + Giuseppe Verdi (verdi) user will be able to see the name of the given class above in the class’ list, but will not be able to create a new instance of the class.
  + Mario Rossi (rossi) will not be able to see the name of the class above in the class’ list (and obviously will not be able to create a new instance).

For more information about FileNet Security Roles, see the [Understanding role-based access](https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psa081.htm) page from the [IBM FileNet P8 Platform V5.5.x documentation](https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8toc.doc/welcome_p8.htm) web site.

1. Login to the Administration Console for Content Platform Engine (ACCE)

Open a browser and type the ACCE URL (usually: [http://servername:port/acce)](http://servernameport/)  
Login as a FileNet administrator  
Open your object store configuration expanding the Object Stores folder and clicking on the object store icon



1. Create and configure the roles classes

Navigate the object store configuration tree and click on the Static Role class.

*TIP: The Static Role class is located at the following path: Data Design > Classes > Other Classes > Role > Static Role*

In the Static Role class tab click on the Actions > New Class button.

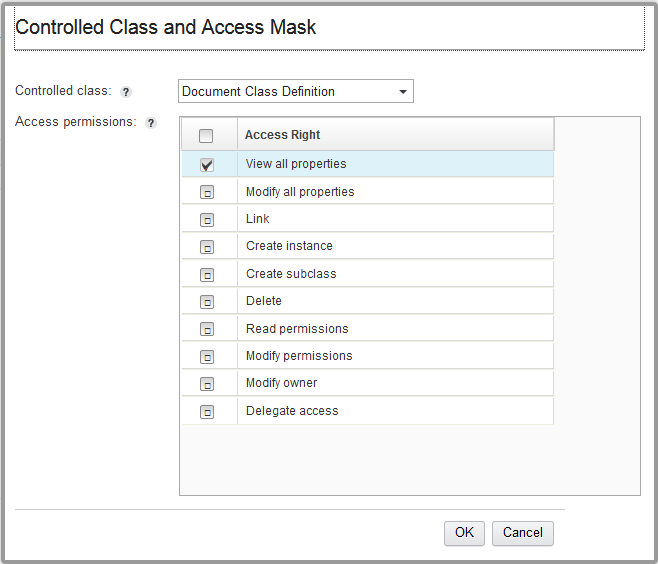
Type “Can Only See Docs And Folders Role” as the name of your role class

Click Next, then Finish

Open the “Can Only See Docs And Folders Classes Role” class definition clicking the Open button

Click the Role Access Definitions tab and click Add

In the Access Definition dialog select the “Document Class Definition” class as Controlled Class and the View Properties access rights as Access Permissions (see the image below).

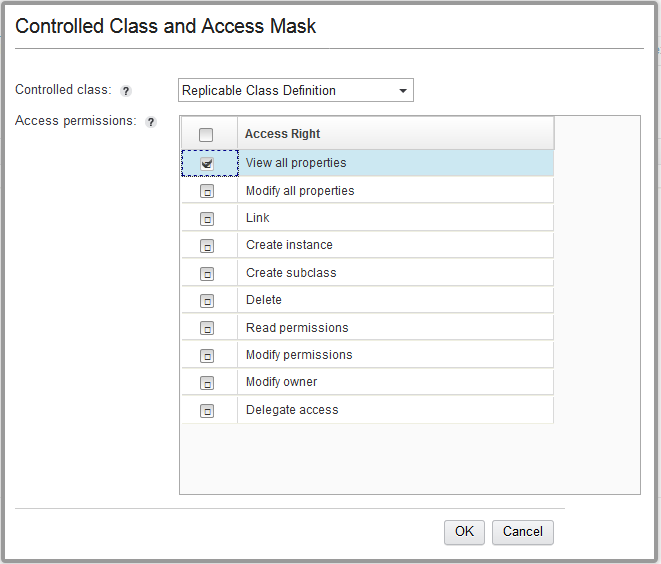


Click OK.

*INFO: The Access Definition you just added will be applied to the Document class and its subclasses (because they are instances of the Document Class Definition class)*

Click Add and select the “Replicable Class Definition” as Controlled Class.

Select the same permission you set at the previous step (as in the following image).



Click OK.

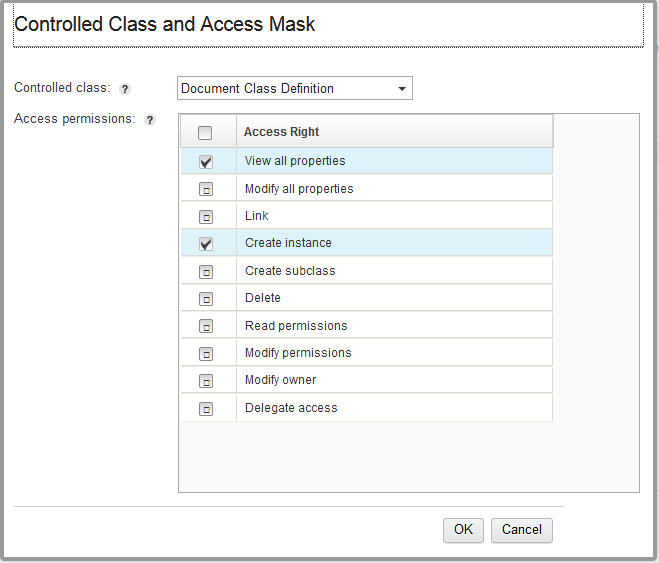
*INFO: The Access Definition you just added will be applied to the Folder class and its subclasses (because they are instances of the Replicable Class Definition class)*

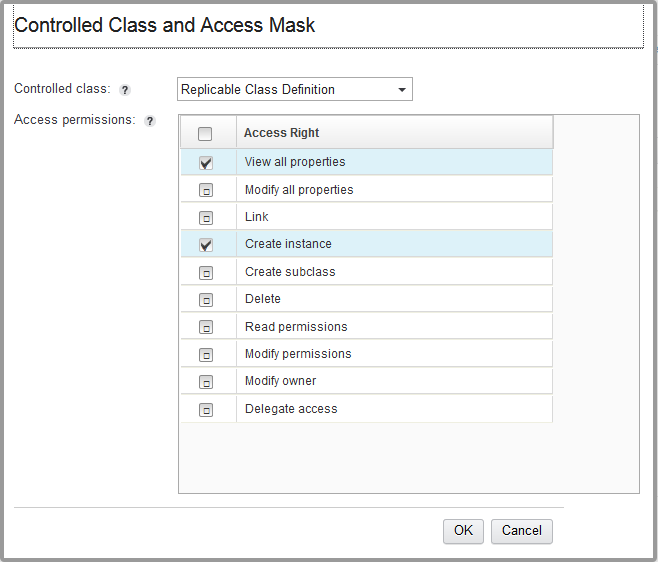
Click the Save button

Create another Static Role class repeating the steps above using the following information.

* + Class name: Can Create Docs And Folders Role
  + Controlled Classes: “Document Class Definition” and “Replicable Class Definition”
  + Access Permissions: View all properties, Create instance”

The access permissions for Can Create Docs And Folders Role should be configured as in the following images



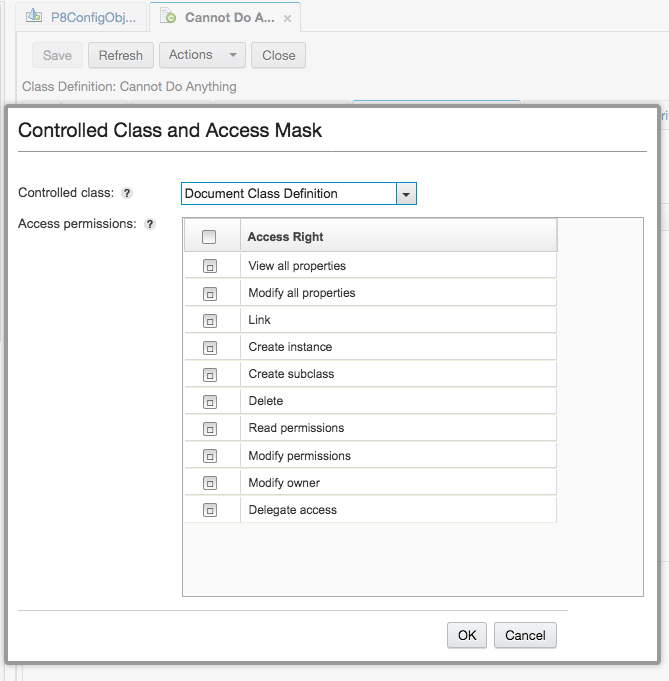


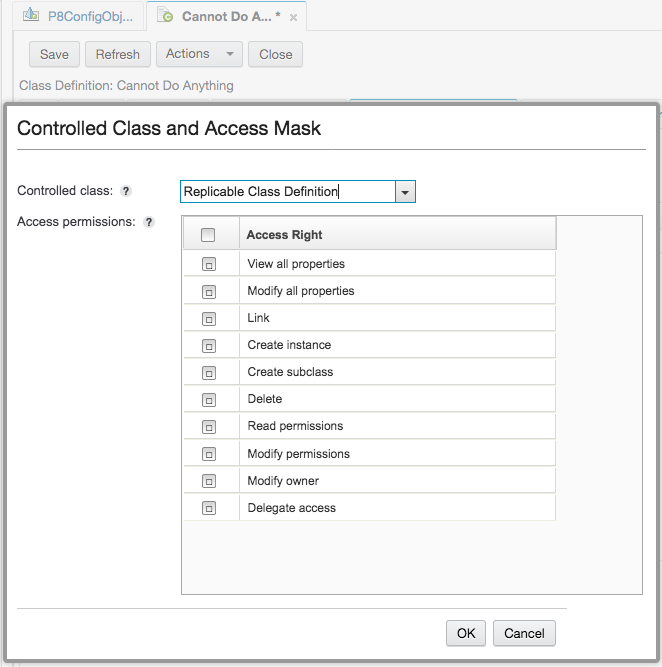
Do not forget to click the Save button!

Create the last Static Role class using the following information

* + Class name: Cannot Do Anything Role
  + Controlled Classes: “Document Class Definition” and “Replicable Class Definition”
  + Access Permissions: none

The access permissions for Cannot Do Anything Role should be configured as in the following images

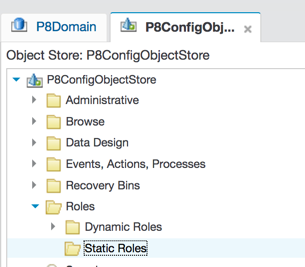




Click Save.

1. Create and configure the roles instances

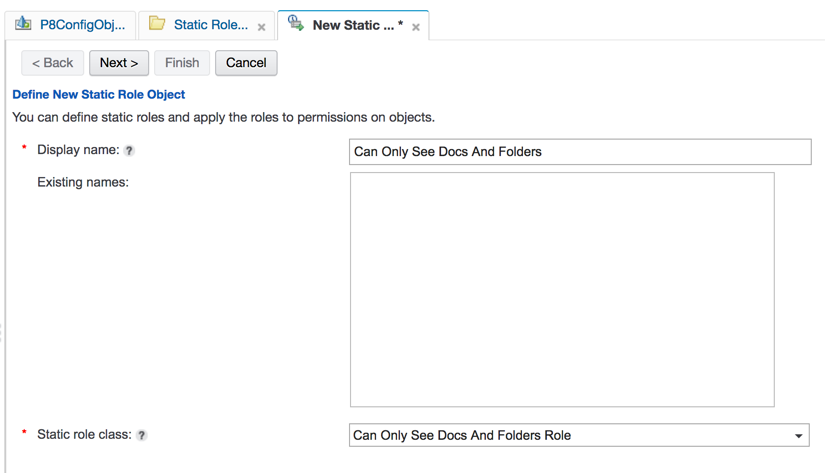
Navigate the object store configuration tree and select the Static Roles folder.



Click the “New” button

Type “Can Only See Docs And Folders” as Display Name of the role instance.

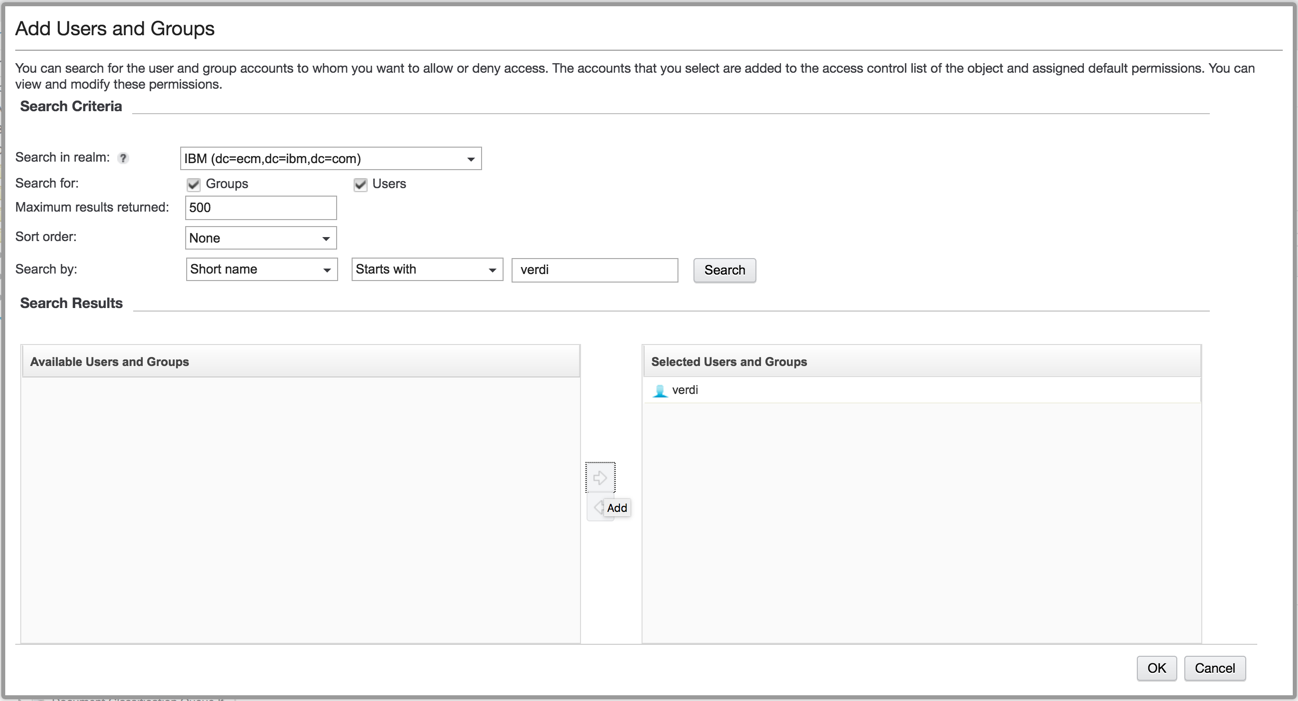
Set the “Can Only See Docs And Folders Role” as Static role class



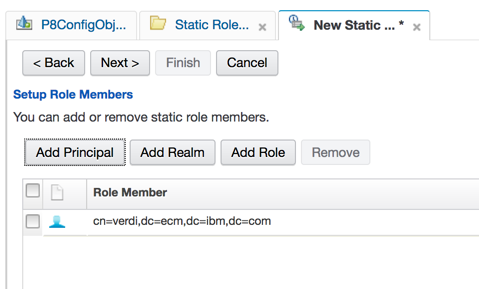
Click Next

Click the Add Principal button

Search verdi user and add him to the Selected Users and Groups



Click OK



Click Next, then Finish.

Repeat the steps above to create another role instance using the following data.

* + Display Name: Cannot Do Anything
  + Static role class: Cannot Do Anything Role
  + User: rossi

Create the last role instance using the following data:

* + Display Name: Can Create Docs And Folders
  + Static role class: Can Create Docs And Folders Role
  + User: bianchi

*INFO: you have just finished to create the concrete objects of the roles classes that you are going to apply to the document/folder classes you wish to secure using these roles.*

1. Configure the security of Document and Folder classes

Create a subclass of the Document or Folder class and open it (give it the name you prefer, I named it “Test Security Role”).

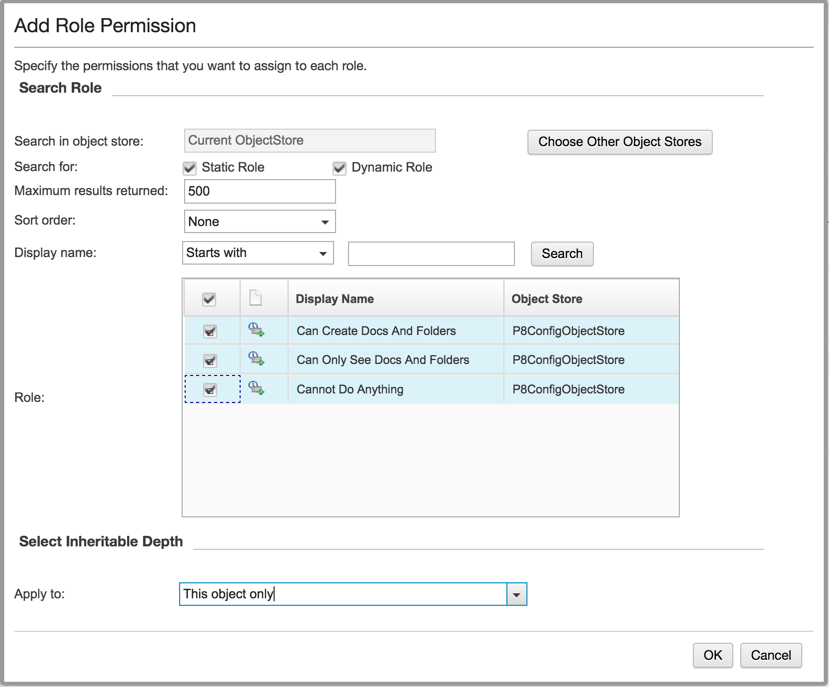
Select the Security tab

Check that the users rossi, bianchi and verdi (or any group they are part of) don’t have any privilege on the class, removing users/groups permissions if needed

Click Add Role Permissions…

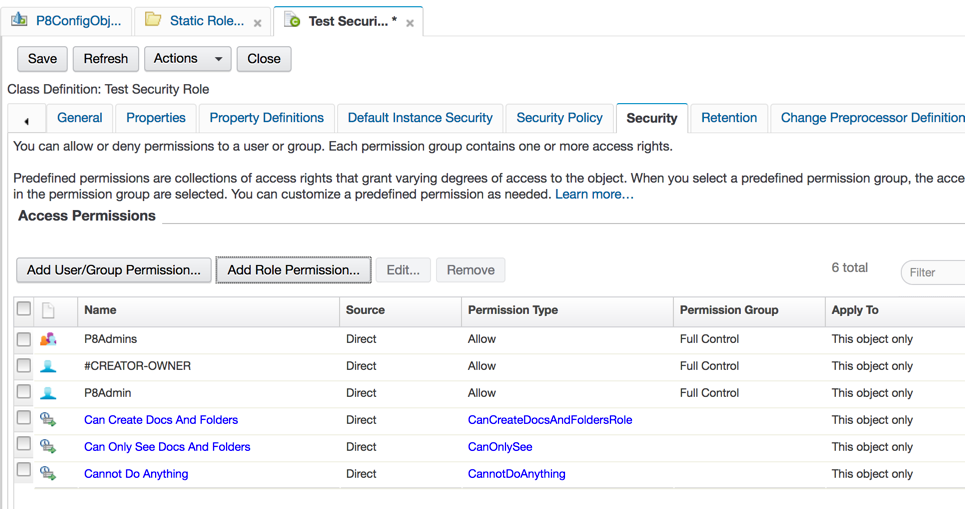
Click the Search button and select the roles instances you created.

In the Select Inheritable Depth section select any depth that include “This object” (i.e. This object only)



Click OK

The class’s Security tab should list the roles you just added.



Click Save.

1. Test your recipe!

Open Content Navigator in your browser and login as verdi user.

Open a folder and add a new document or folder of the class configured to be secured with the roles (if you used the names in the recipe, you’re going to ad a document of Test Security Role class).

*INFO: if the system is correctly configured, verdi user can see the class in the class selector but when try to add a new document or folder because an error is raised because verdi user is part of a role that it isn’t allowed to perform the create instance action.*

Logout from the Navigator and login as rossi user

Click the Add Document or Add Folder button

*INFO: based on the role configuration, rossi user doesn’t have any privilege on the class, so he doesn’t see the class name in the class selector.*

Logout from the navigator, log in as bianchi user

Add a new document or folder of the class configured to be secured with the roles

*INFO: based on the role configuration bianchi user can see the class in the class selector and can also create a document of the class.*

1. Useful resources

Here are the links to some documentation pages related with the recipe.  
[Understanding role-based access](https://www.ibm.com/docs/en/filenet-p8-platform/5.5.x?topic=authorization-understanding-role-based-access)  
[Configure role-based access](https://www.ibm.com/docs/en/filenet-p8-platform/5.5.x?topic=how-configure-role-based-access)