

## Configure security for IBM FileNet P8 assets

In this section, you will learn about the IBM FileNet P8 Platform provided framework for security and how to control access to IBM FileNet P8 Platform assets on the system.

### What is authentication?

Authentication is the act of verifying a user identity based on credentials (user name and password) that the user presents (who is the user?).

Authentication of individuals through the external authentication mechanism, is key to the security features in IBM FileNet P8 Platform.

The two main authentication standards that are used by IBM FileNet P8 Platform are:

- Java Authentication and Authorization Service (JAAS)  
The JAAS standard forms the framework for security interoperability in the Java EE world.
- Web Services Security  
The Web Services Security standard forms the framework for security interoperability in the heterogeneous world of clients and servers that communicate through web services interfaces.

### Example of an authentication error

A user tries to log into IBM Content Navigator and receives a login error.

- Error message: *The user ID or password is not valid for the server.*  
Causes: User is not a member in the LDAP directory or the LDAP directory service is not reachable.  
Solution: Ensure that LDAP is running and reachable by the Content Platform Engine and check the LDAP directory to verify that the user exists.

### Authentication providers

An authentication provider is a supported LDAP-compliant directory service that provides authentication for the FileNet P8 domain. The authentication provider is identified during IBM FileNet P8 Platform installation through the JAAS configuration.

Supported directory service providers include IBM Security Directory Server, CA Directory, NetIQ eDirectory, Oracle Internet Directory Server, and Microsoft Active Directory.

For a complete list of authentication providers, refer to the Software Product Compatibility Report (SPCR) for IBM FileNet Content Manager that can be generated on the following site:

<https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html>

## **LDAP single entity lookup behavior**

If you have multiple LDAPs configured, a new option is provided through the `com.filenet.engine.directory.DuplicateHandling` JVM argument to control how the server deals with potential duplicate user and group names. This option can be used to improve the performance of user and group lookups when name uniqueness is guaranteed.

For more details on this topic, 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.performance.doc/p8ppt332.htm](https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.performance.doc/p8ppt332.htm)

## **What is authorization?**

Authorization is the act of allowing a user to complete actions on the object based on the user and group memberships (What can the user do?).

Authorization requires prior authentication and uses the security token that is generated during authentication.

When an authenticated security principal (user or group) attempts to access FileNet P8 objects such as an object store, a folder, or a document, Content Platform Engine checks that principal's user and group memberships from the directory service provider against the permissions assigned to the object. If successful, the user is authorized to carry out actions on the object as described by the access rights.

## **Example of an authorization error**

A user tries to log in to IBM Content Navigator and receives a login error. This user is a verified member in the LDAP directory.

- Error message: *You do not have the appropriate permissions to access the following repository: <repository name>*

Cause: User is not authorized to view the object store that is defined for Authentication on the IBM Content Navigator desktop.

Solution: Ensure that the user is authorized to access the object store.



## User roles

Different user roles provide varying level of access to the objects. For example, administrators, solution builders, authors, and users might have different access rights to the same objects.

Even administrators with access to Administration Console for Content Platform Engine can have different levels of access to objects. For example, one administrator might have permission to modify property templates that another administrator has no access.

## User and groups

The directory service defines the security principals (user or group). Users are assigned to groups. Use groups as primary security principals whenever possible.

### #AUTHENTICATED-USERS group

This special group represents all users in the LDAP domain and who have been authenticated by the application server. You use this group if you want to grant access to an object to all users of IBM FileNet P8 Platform. If you do not specify initial users, #AUTHENTICATED-USERS group is added automatically.

In a production environment, configure initial user groups to prevent an object store from being used by all domain users.

In development and test environments, it can be useful to give this group basic rights and then work on refining access within the object store.

## Object ownership

Most objects have an owner who is typically the user who created the object. IBM FileNet P8 Platform automatically applies an internal special user account called the #Creator-Owner and grants full control access on that object.

## IBM FileNet P8 object security terms

Object access rights (which are also called permissions) determine which users can access the objects and what kind of tasks the users can do. Following are the key terms used in the IBM FileNet P8 Platform security:

- Access Control List (ACL)

Each securable Content Platform Engine object has an associated security descriptor, part of which is the Access Control List (ACL). An ACL is a collection of all the Access Control Entries (ACEs) on an object.

- Access Control Entry (ACE)

An ACL consists of a set of Access Control Entries (ACEs) which are also called permissions. ACEs define who can do what.

- Security Identifier (SID)

Each ACE consists of a globally unique Security Identifier (SID). It uniquely identifies a security principal which is a user or group that Content Platform Engine grants or denies access to.

Each permission specifies one security principal (user or group) through a SID, and an access mask for that SID. The access mask defines the specific operations that the grantee identified by the SID is allowed to perform. Each bit in the mask corresponds to a specific operation. If the bit is set, the security principal is authorized to perform that operation.

---

## Security sources of ACE

Every ACE has a source either Default Security, Direct Instance Security, Security Inheritance or Security Template. You can view the source types of ACE in the security editor of Administration Console for Content Platform Engine (ACCE).

- Direct Instance Security

These permissions are directly added to an object and the ACEs are directly editable. You can view the access control entries (ACE) for a document in its Security tab in ACCE. All the ACEs in the list make up the ACL of that document.

- Default Security

Default permissions are placed on an object (Example: document or folder) by the default instance security ACL of its class (Example: Document class or Folder class) as well as permissions placed on a subclass by its parent class.

Default ACEs are directly editable, but if you edit an ACE, then its source type becomes Direct.

You can view the ACL for a Document class in its Default Instance Security tab in ACCE. ACL on this tab will show up in the security tab of the documents that belong to this class.

- Security Inheritance

In this scenario, permissions are passed from a parent object to a child object. For example, a folder could be a parent of a subfolder or a document. Because of the security inheritance, an administrator can apply security permissions to many objects in one operation by setting the permissions at the parent level.

- Security Template

Template permissions are assigned to the objects by a security policy. Security policies along with document versioning states allow an administrator to configure the system to automatically modify ACLs on documents when their versioning state changes. For example, the administrator can configure a system to automatically grant access to a document to a wide audience when it is released.



## **Order in which security source permissions are granted**

Each ACE has one access type either allow or deny. When evaluating the access granted by a particular ACL, the current system applies ACEs in the following order:

- Direct/Default - Deny
- Direct/Default - Allow
- Template - Deny
- Template - Allow
- Inherit - Deny
- Inherit - Allow

Higher on the list takes precedence over the lower items. Deny takes precedence over allow within each category. For example, if you explicitly deny an access right to a group and explicitly allow it to a member of that group, the access right will be denied to the member.

## **Independent and dependent security**

Most objects have Access Control Lists (ACLs) that can be independently set. These objects are called independently securable.

Dependently securable objects depend on their parent object for their access rights. They are secured through the parent object.

Examples of dependently securable objects:

- Content elements, which have the same security as the associated document
- The individual choices in a choice list, which have the same security as the object that the choice list is assigned to
- A lifecycle state in a lifecycle policy

## **Designing a secure system**

Security is more than securing documents and folders. The security of the system design determines which objects are securable by which users. For example, administrators might be responsible for securing the domain root and the object stores. Application builders might be responsible for securing classes, instances like stored searches and entry templates, and property templates. Authors might be responsible for securing folders and documents.

The design also includes the security of the servers, databases, as well as the object store content. For example, security must be configured on the shared directory location under which file storage areas, fixed storage area staging directories, advanced storage area file system devices, and content cache areas will be created.

## IBM Content Navigator Desktop security

A desktop is configured to authenticate users against a specific repository in your environment. Users who want to access this desktop must be defined as having access to that repository. Also, you can limit access to the desktop to a specific set of users and groups in your repository.

A user can log in to Administration Console for Content Platform Engine but be unable to log in to the IBM Content Navigator (ICN) Desktop if that user is not authorized to access that specific object store.

For more information on the content security and ICN, refer to the ICN Knowledge Center:

[https://www.ibm.com/support/knowledgecenter/SSEUEX\\_3.0.5/com.ibm.usingeuc.doc/euche014.htm](https://www.ibm.com/support/knowledgecenter/SSEUEX_3.0.5/com.ibm.usingeuc.doc/euche014.htm)

### Important Note: requirement for the activities

Following activities (lab exercises) in the Security section builds on their previous activities. For the activities to work correctly, it is important that they are done in the order it is presented and not to skip any of them.

---

## Activity: Identify access issues

---

IBM Content Navigator (ICN) is the primary client through which users access the contents of the IBM FileNet Content Manager repositories. In this activity, you will log in to ICN as different users and identify a few scenarios where a login failure happens or access is denied.

In this activity, you will accomplish the following:

- Examine the authentication login error.
- Log in as an unauthorized user.
- Observe object store access.
- Check the security in the ICN admin desktop.

### Examine the authentication login error.

In this activity, you will attempt to log in to IBM Content Navigator as a user who is not a member of the LDAP directory and examine the error when authentication fails.

- Ensure that the IBM FileNet P8 Platform components are started.

If you have not started them earlier, start the components by using the earlier activity: *Prepare your system - Start IBM FileNet P8 Platform*.



- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**
- Type **Jayda** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Notice that you get the following error: *The user ID or password is not valid for the server.*
- Verify that the **Content Engine Startup Context (Ping Page)** is running by entering the following URL in a separate browser tab:  
**http://ecmedu01:9080/FileNet/Engine**

You can also use the bookmark (Bookmarks menu > System Health > CE Ping).

When the ping page is displayed, you have verified that the Content Platform Engine is running.

Optionally, you can open the active directory and verify that this user (Jayda) does not exist.

Similar errors can also occur if the LDAP directory service is not reachable. In a scenario where the user exists in the LDAP directory and you still get this error, you must look at the error logs to check if the LDAP service is reachable.

- Close the browser.

### **Log in as an unauthorized user.**

A user, in addition to being a member of the LDAP directory, must have permission (authorization) on the object store (that is used for authentication) in order to log in to the IBM Content Navigator (ICN) client. The student system already has a user called Scott who is a verified member in LDAP but does not have permission to access the object store that is used for authentication. In this task, you will attempt to log in as this user and examine the error when authorization fails.

Note that if an object store is configured to provide access to the #AUTHENTICATED USERS group, then anyone who can log in to the domain can have access to that object store. The student system does not have this configuration, so only users who have explicit permission can access the object store.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Scott** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

- Verify that you cannot log in and get the following error: *You do not have the appropriate permissions to access the following repository: <repository name>*

Notice that this time, the error message is different from the one that you got in the previous task. It provides a clue about the underlying cause of the login failure.

Scott does not have access to the object store that is defined for authentication for this ICN desktop. A user must have access to the object store that ICN uses for authentication to log in. In some cases, an authorization problem might appear to be an authentication problem.

- Close the browser.

### **Check the security in ICN admin desktop.**

A desktop is configured to authenticate users against a specific repository in your environment. Users who want to access this desktop must be defined in the repository. In this task, you will log in to the ICN admin desktop and check some of the security features that control access to FileNet P8 assets.

- In the **Mozilla Firefox** browser, click the **ICN Admin** bookmark or enter the following URL: **<http://vclassbase:9081/navigator/?desktop=admin>**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

The ICN admin desktop opens.

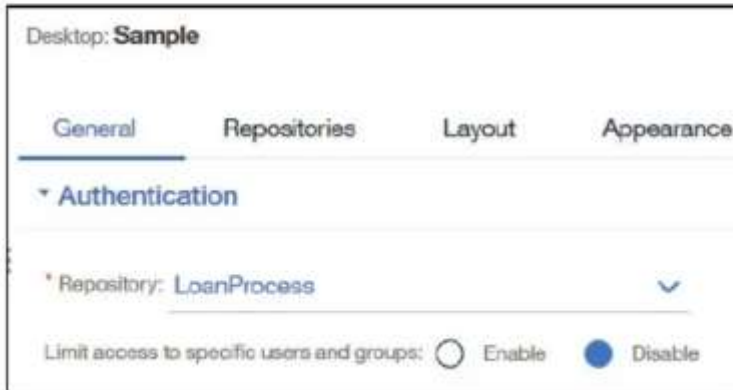
On the Desktops tab, the available desktops for this ICN instance are listed. From this admin client, you can configure all the ICN features for your desktops.

- Click **Repositories** from the left navigation pane.
- From the **Repositories** tab on the right pane, notice the list of repositories.

The Server Type column shows that all these repositories are of IBM FileNet Content Manager type. You can also configure other type of repositories. You must configure a FileNet P8 object store in this tab by using the Server URL to be able to access the content for that object store.



- Close the **Repositories** tab.
- On the **Desktops** tab, select **Sample** and click **Edit**.  
This is the Sample Desktop that you were using for the earlier activities.
- On the **Sample** tab > **General** subtab, scroll down and then verify that **LoanProcess** repository is listed under the **Authentication** section.



When users log in to Sample desktop, ICN authenticates the users against the LoanProcess object store. If the user does not have access to this object store, the access to the ICN desktop is denied.

- On the **Sample** tab, select the **Repositories** subtab and observe the list of repositories.  
Recall that these repositories were displayed on the Sample desktop in the previous tasks and authorized users were able to access content.  
You can learn more on configuring repositories and desktops in the IBM Content Navigator courses.
- Log out of IBM Content Navigator and then close the browser.

### Observe object store access.

Object stores are usually secured by using group memberships. Users who have access to object stores can log in and use the object stores. Each user, depending on their role, has access to some but not necessarily all the object stores in an IBM Content Navigator (ICN) desktop. In this task, you will sign in as Mary and verify that Mary is able to access the LoanProcess object store but not the other object stores that are available in the ICN desktop.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Mary** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that Mary is able to access the folders and documents in the **LoanProcess** object store.
- Double-click the folders in the right pane to open them.  
You can also click the folders from the left navigation pane.

- To open another repository, click the down arrow next to **LoanProcess** on the upper right.  
All the repositories that are available for this desktop are shown in the list: LoanProcess, Sales, LoanProcessQA, and SalesQA
- Attempt to open each of the object stores in the list by clicking it and verify that Mary is denied access to the other repositories.
- Log out of IBM Content Navigator and then close the browser.

## Activity: Explore the security settings in ACCE

In this activity, you will explore some of the security concepts that you learned earlier in this course. You will log in as the user P8Admin who has been given full access to the objects in the IBM FileNet Content Manager repositories. This user has already been created and configured on the student system to complete these activities.

In this activity, you will accomplish the following:

- Check the security settings.

### Check the security settings.

In this activity, you will log in to Administration Console for Content Platform Engine (ACCE) and check the security settings.

- 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 and then click the **LoanProcess** object store.
- From the **LoanProcess** tab, on the left pane, expand the **LoanProcess > Browse > Root Folder** node and then click **Loans**.
- From the **Loans** tab on the right pane, click any document (Example: **J Jones' Loan**)
- From the **J Jones' Loan** tab, select the **Security** subtab.

Use the forward arrow on the right to scroll to find the tab. You can also use the down arrow to select the subtab from the list.

If the contents of the tab is not displayed, click Refresh and the content will be refreshed.

In the Security subtab, under the Access Permissions section, each row with a security user or group name is an Access Control Entry (ACE). All the rows collectively form the Access Control List (ACL) for the document.

Notice that the ACEs are editable. If you select a row in the list, the Edit and Delete buttons are enabled.

Observe that each row has the value Direct for the Source column. It indicates that the security source is Direct Instance Security.



- From the **J Jones' Loan** tab, select the **General** subtab, scroll down, and observe the **Inherit Security from folder** field.

If a value is assigned to this field, it indicates the folder object (security parent) from which this document inherits security.

You will learn about security inheritance and other security concepts in a later section.

- Close the **J Jones' Loan** tab and the **Loans** tab.
- From the **LoanProcess** tab, on the left pane, collapse the **Browse** node, expand the **Data Design > Classes** node and click the **Document** class.
- From the **Document** tab on the right pane, select the **Default Instance Security** subtab.

In the Default Instance Security subtab, the ACL list that is under the Access Permissions section, will become the default security for the documents that belong to this Document class.

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

---

## Activity: Change direct security of an object

---

When you first create an object, typically, it acquires the default security settings that is defined for the class. These settings identify which users and groups can access the object. The default security for an object can also be determined by other sources such as an entry template, a security policy, folder inheritance, and so on.

In IBM Content Navigator, you can specify security on a document by using the following predefined security roles: Owner, Author, Reader, and No access. Each of these groups has a predefined set of access rights.

The list of available security settings is different in IBM Content Navigator (ICN) as compared to Administration Console for Content Platform Engine (ACCE). ICN presents some aggregations of security settings to give end users a more intuitive set of options, whereas ACCE provides a much more granular set of options.

In this activity, you will create a document and observe its default instance security. You will then modify its security directly for the group access, access level, and ownership in IBM Content Navigator.

In this activity, you will accomplish the following:

- Add a folder and a document.
- Verify access to the document by a different user.

- Remove group access to the document.
- Verify that access is removed.
- Change access level.
- Change ownership.
- Verify the change in ownership.
- Examine the ownership.

### **Add a folder and a document.**

Mary and Matt are the members of the Loan Managers group. In this task, you will log in as the user Mary, create a folder and a document, and check who has access to the newly created items.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Mary** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, click **New Folder** from the toolbar.
- On the **New Folder** page, type **Security Test** for the **Folder Name** field, observe the default security for the folder, and then click **Add**.
- Back on the **Browse** page, double-click **Security Test** to open the folder and then click **Add Document** from the toolbar.
- On the **Add Document** page, type **Access Loan** for the **Document Title** field.
- For the **What do you want to save?** field, click **Browse**.
- On the **File Upload** page, navigate to the **C:\Training\F2810G\SampleDocs** folder, select any file (Example: **MarketingPlan5.pdf**), and then click **Open**.
- In the **Add Document** page, leave the default for all the other fields and observe the security that is assigned to this document.  
The Owner group has the following members: P8Admin, P8Admins, and Mary  
The Readers group has the following members: Loan managers, Loan officers, Loan processors, and Loan underwriters
- Click **Add** and then, on the **Browse** page, verify that the new document is listed.
- Click the head and shoulder icon in the banner, click **Log Out** to log out of **IBM Content Navigator** and then close the browser.



For all the following tasks, when you log out as one user and before signing in as another user, close the browser to avoid any caching issue.

### **Verify access to the document by a different user.**

Since Matt is a member of the Loan managers group which is authorized to view the document created in the previous task, Matt should be able to access the document that Mary created. In this task, you will verify the access by logging in as Matt.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Matt** for **User name**, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, double-click the **Security Test** folder to open it and then verify that you can access the **Access Loan** document.
- Right-click the document and then verify that user **Matt** has access to open, preview, properties, or download the document (these actions are enabled) but he cannot delete this document (action is grayed out) since he is not the owner of this document.

Matt also cannot check out the document because the Loan managers have only Reader access. In a later task, you will change Matt to be the owner of the document.

- Log out of **IBM Content Navigator**.

### **Remove group access to the document.**

In your business scenario, you determine that the Loan processors group no longer needs access to your document. In this task, you will verify that Peter who is a member of the Loan processors group is able to view the document. You will then remove the Loan processors group access to the document and verify that Peter can no longer access the document.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Peter** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, open the **Security Test** folder and then verify that the **Access Loan** document is displayed.
- Log out of **Sample Desktop** and close the browser.
- Log in to the **Sample Desktop** as **Mary** (Password: **FileNet1**).
- Open the **Security Test** folder, right-click the **Access Loan** document and then select **Properties**.
- On the **Properties** page, open the **Security** tab.
- Remove the permission for **Loan processors** to read the document by clicking the **X** on the group and then click **Save**.
- Log out of **IBM Content Navigator** and close the browser.

## Verify that access is removed.

User Mary has removed access to the document for Loan processors. You will log in as Peter and verify that he is not able to access the document.

- Log in to **IBM Content Navigator Sample Desktop** as **Peter**:
  - **Sample Desktop** bookmark or URL: <http://vclassbase:9081/navigator>
  - User name: **Peter**
  - Password: **FileNet1**
- From the **LoanProcess** repository, open the **Security Test** folder and then verify that the folder is empty.

This security configuration is an example of an implicit denial. When a user has no permissions (not listed in the ACL), the document is not displayed.
- Log out of IBM Content Navigator **Sample Desktop** and close the browser.

## Change access level.

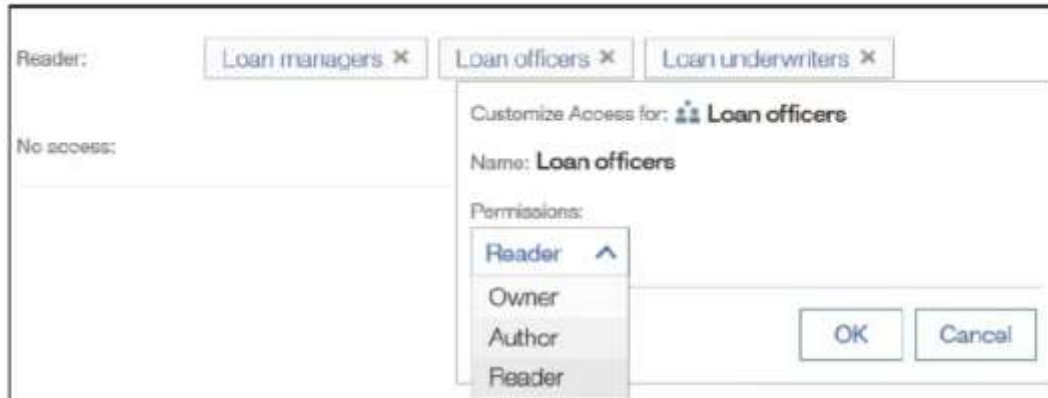
The members of the Loan officers group have Reader access to the document, by default. You want to grant Loan officers with Authors access for this document. As an owner of this document, Mary can change the access levels.

In this task, you will check the Reader access for Olivia who is a member of the Loan officers group. You will grant her group the Author access and then check her access.

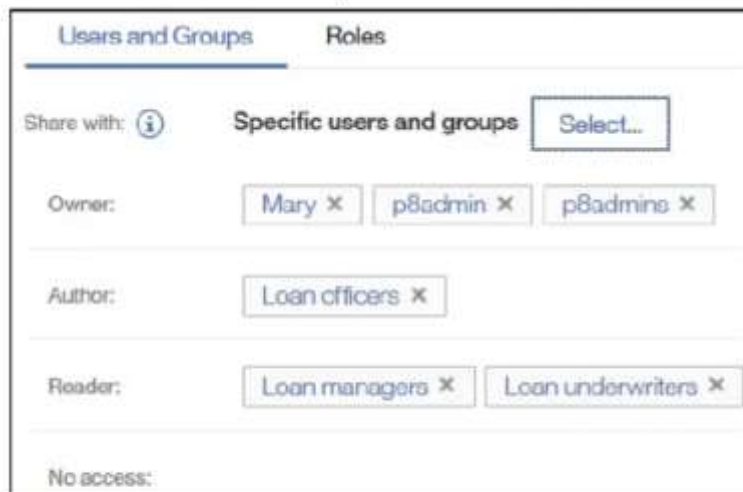
- Log in to **IBM Content Navigator Sample Desktop** as **Olivia**:
  - **Sample Desktop** bookmark or URL: <http://vclassbase:9081/navigator>
  - User name: **Olivia**
  - Password: **FileNet1**
- From the **LoanProcess** repository, open the **Security Test** folder.
- Right-click the **Access Loan** document, and then verify that user Olivia has access to open, preview, properties, and download the document (these actions are enabled) but she cannot check out the document (this action is grayed out) because the Loan officers have only Reader access.
- Log out of **Sample Desktop**, close the browser, and then log in as **Mary** (Password: **FileNet1**).



- Open the **Security Test** folder, right-click the **Access Loan** document and then select **Properties** from the list.
- On the **Properties** page, open the **Security** tab.
- Click the **Loan officers** link and then select **Author** from the **Permissions** list.



- Click **OK** and then verify that **Loan officers** are now in the **Authors** group.



- Click **Save**, log out of **Sample Desktop** and then close the browser.
- Log in to **Sample Desktop** as **Olivia** (Password: **FileNet1**).
- Open the **Security Test** folder, right-click the **Access Loan** document, and then verify that Olivia now has access to check out the document.

The Check Out action is enabled. Because the Loan officers have been given Author access and Olivia is a member of this group, she is able to access the action.



- Log out of **Sample Desktop** and close the browser.

## Change ownership.

The user Mary is the owner of the document that you created in the earlier task and this user has full access to the document. Mary will no longer be working on this document and she wants to change the ownership to Matt who is also a member of the Loan managers group. You have already checked that Matt does not have checkout or delete access to this document. In this task, you will make Matt the owner of the document, and then recheck his access.

- Log in to IBM Content Navigator **Sample Desktop** as **Mary** (Password: **FileNet1**).
- Open the **Security Test** folder and then open the **Properties** page for the **Access Loan** document.
- On the document's **Properties** page, click the **Security** tab and then for the **Share with** field, click **Select** next to the **Specific users and groups**.
- On the **Add Permissions** page, for the **Search for** field, verify that **Users** is selected, type **Matt**, and then click the Search  icon.
- Select **Matt** from the **Available** pane and move it to the **Selected** pane by using the forward arrow.
- At the end of the page, make sure **Owner** is selected for the **Permissions** field and then click **Add**.
- Back on the **Properties** page, verify that **Matt** is added to the list of Owners.



Owner:	Mary x	p8admin x	p8admins x	Matt x
--------	--------	-----------	------------	--------

- Click the **X** on **Mary** to remove the user from the **Owners** list, and then click **Save**.
- On the **Browse** page, right-click the **Access Loan** document, and then verify that Mary no longer has Owner access.  
Delete, checkout and a few other actions are now disabled. Since she is part of the Loan managers group, she continues to have Reader access through that membership and can open or download the document.
- Log out of **IBM Content Navigator** and close the browser.

## Verify the change in ownership.

You changed the ownership of the document to Matt. In this task, you will verify that Matt has full access to the document (including delete).

- Log in to IBM Content Navigator (ICN) **Sample Desktop** as **Matt** (Password: **FileNet1**).
- Open the **Security Test** folder, right-click the **Access Loan** document, and then verify that Matt can now check out, delete, and take other actions (these action are enabled now).
- Log out of ICN **Sample Desktop** and close the browser.



## Examine the ownership.

The security that is set on a document in the IBM Content Navigator (ICN) client is executed as configured in ICN. Even though you changed the ownership of the document to Matt, Mary remains the owner when you examine the ownership in Administration Console for Content Platform Engine (ACCE). This is because how ICN maps its security groups (For example, Owner, Author, or Reader). Mary will be able to take owner actions on this document in ACCE even after she is removed as the owner in ICN. An administrator must reset the ownership in ACCE to complete the process. In this task, you will examine this and change the ownership to Matt.

- 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**.
- From the **EDU\_P8** tab, expand the **Object Stores** folder on the left pane and then click the **LoanProcess** object store.
- From the **LoanProcess** tab, expand the **LoanProcess > Browse > Root Folder** node on the left pane and then click **Security Test**.
- From the **Security Test** tab on the right, click the **Access Loan** document link.
- Scroll the tabs to the right and then click the **Security** subtab to open it.
- Scroll down the page to the **Owner/Active Markings** section and then verify that the **Owner** is **Mary** (shown as **mary@edu.ibm.com**).
- Click **Change Owner**.
- On the **Change Owner** page, select the **Change owner to** option, and then click **Find**.
- On the **Add Users and Groups** page, search for **Matt** (by **Short name**).

Search by	Short name	▼	Starts with	▼	Matt	Search
-----------	------------	---	-------------	---	------	--------

- Select **Matt** from the **Available Users and Groups** pane and then move Matt to the **Selected Users and Groups** pane by clicking the forward arrow.
- Scroll down, click **OK**, and then verify that Matt (**matt@edu.ibm.com**) is now the owner on the **Access Loan** tab.
- Click **Save**, click **Refresh**, and then click **Close** to close the **Access Loan** tab.
- Close the **Security Test** tab.
- From the **LoanProcess** tab, click **Refresh**.

This completes the change of ownership at all levels.

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

---

## Activity: Customize security access

---

In Administration Console for Content Platform Engine, you can specify security by using the following predefined Permission groups: Full Control, Minor versioning, Major versioning, Modify properties, View content, View properties, Publish, and Custom.

In this activity, you will use Permission groups for common security scenarios, and specify custom permissions for fine-grained security configurations.

In this activity, you will accomplish the following:

- Add typical document permissions.
- Edit security settings.

### Add typical document permissions.

In this task, you will create a folder and a document. You set security by using the predefined Permission Groups.

- 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**.
- From the **EDU\_P8** tab on the left pane, expand the **Object Stores** folder and click the **LoanProcess** object store.
- From the **LoanProcess** tab, expand the **LoanProcess > Browse** node on the left pane, right-click **Root Folder**, and then select **New Folder**.
- Type **AT Folder** for the **Folder name** field, click **Next** two times, and on the **Summary** page, click **Finish**.
- Click **Close** on the **Success** page.
- Expand the **LoanProcess > Browse > Root Folder** node on the left pane and then click **AT Folder** to open it.
- On the **AT Folder** tab, click **Actions > New Document** from the top toolbar.
- On the **New Document** tab, type **Access Test** for the **Document title** field, verify that the **With content** option is selected and then click **Next**.
- Click **Add** to add a content element, and then click **Browse** to select a document.
- On the **File Upload** page, navigate to the **C:\Training\F2810G\SampleDocs** folder, select a document (For example, **SampleTextDoc1.txt**) and then click **Open**.



- On the **Add Content Element** window, click **Add Content**.
- Back on the **New Document** tab, click **Next** several times, leave the default values, and then click **Finish** on the **Summary** page.
- Click **Close** on the **Success** page.
- On the **AT Folder** tab, click **Refresh**, verify that the new document is listed, and then click the **Access Test** link.
- On the **Access Test** tab, scroll to the **Security** subtab.
- On the **Security** subtab, click **Add Permissions > Add User/Group Permission**.
- On the **Add User and Groups** page, type **Case** on the **Search by** field and then click **Search**.
- Select **Case workers** from the **Available Users and Groups** pane and then move to **Selected Users and groups** by clicking the forward arrow.

- Select **Case workers** from the **Selected Users and groups** pane, scroll down to the **Permissions** section, and then select **Major versioning** from the **Permission group** list.

Verify that the following individual permissions are automatically selected:

View all properties, View content, Change state, Major versioning, Read permissions, Unlink document, Modify all properties, Link a document / Annotate, Create instance, and Minor versioning.


- Click **OK**, back on the **Access Test** tab, verify that **Case workers** is listed and then click **Save**.

### Edit security settings.

For this scenario, the Major versioning Permission group grant access to more actions than what you want to grant to the Case workers group. You can control the security at a more granular level by setting custom permissions. In this task, you will modify the permissions to a custom level.

You are already logged on to Administration Console for Content Platform Engine as p8admin. You are viewing the Access Test document's security tab.

- On the **Access Test** tab > **Security** subtab, select the **Case workers** row under **Access Permissions** section and then click **Edit**.
- On the **Edit Permissions** page, under the **Permission group** section, clear the **Unlink document** permission.
- Confirm that the value for the **Permission group** field changes to **Custom**.

Users and Groups :	Case workers
<hr/>	
Permission type :	Allow 
Apply to :	This object only 
Permission group :	Custom 
<input checked="" type="checkbox"/> View all properties <input checked="" type="checkbox"/> Modify all properties	

- Click **OK** to close the page.
- On the **Access Test** tab > **Security** subtab, click **Save**.
- Log out of **Administration Console for Content Platform Engine** and close the browser.



---

## Activity: Configure initial object store security

---

In this activity, you will create an object store and specify initial security on the object store so that all P8 users (but not all authenticated users) can access it. P8 users is a security group that is defined in the Microsoft Active Directory (LDAP -authentication provider) on your student system. You will further configure security on objects within this object store in later activities.

In this activity, you will accomplish the following:

- Create an object store and configure initial security.
- Verify the new object store security.
- Configure your repository.
- Edit the desktop to add your repository.

### Create an object store and configure initial security.

You created an object store at the beginning of the course and used it to add other P8 objects. In this task, you will create another object store and use it for the following activities to set various type of security. For more details on this task, refer to the *Create an object store* activity in the beginning of this course.

- 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, click the **Object Stores** node.
- From the **Object Stores** tab on the right pane, click **New**.
- On the **New Object Store** tab, type **Finance** as the value for the **Display name** field and then click **Next**.

- For the **Database connection** field, select **FNOSDS** from the list and then type **Finance** for the **Schema name** field.

Database connection : 	FNOSDS
	<a href="#">New...</a>
Site :	Initial Site
Schema name : 	Finance

Leave the defaults for the other fields.

- Click **Next**, on the **Select the Type of Storage Area for Content** page, click **Next** again.
  - On the **Grant Administrative Access** page, click **Add User/Group Permission**.
  - On the **Add Users and Groups** page, for the **Search for** field, clear the **Users** and **Special accounts** options (checkboxes), and leave **Groups** selected.
  - Type **P8** for the **Search by** field and then click **Search**.
  - From the **Search Results** section, select **p8admins** from the **Available Users and Groups** pane and move it to the **Selected Users and Groups** pane by using the forward arrow.
  - Click **OK** to close this page, verify that the **p8admins** group is listed on the **Grant Administrative Access** page, and then click **Next**.
  - On the **Grant Basic Access** page, click **Add User/Group Permission**, repeat the steps to add the **p8users** group, and then click **Next**.
  - On the **Select Add-ons** page, click **Default Application Configuration** and then verify that the add-ons are selected.
  - Click **Next**, review your selections on the **Summary** page, and then click **Finish** to create the object store.
- Wait for the process to complete. It takes a while.
- On the **Success** page, click **Close**.



## Verify the new object store security.

In this task, you will verify that the object store has correct security settings.

- In the Administrative console, from the **Object Stores** tab, click **Refresh**.
- Click the **Finance** link to open the new object store.
- From the **Finance** tab, click the **Security** subtab and then verify the permission groups for the following security groups and users:
  - P8admins, Full Control
  - P8users, Use object store
  - P8admin, Full Control

	Name	Source		Permission Type	Permission Group
	p8admins	Default		Allow	Full Control
	p8users	Default		Allow	Use object store
	p8admin	Default		Allow	Full Control

The admin users have full control and other P8 users have access to use the object store.

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

## Configure your repository.

Users manage your object store content in the IBM Content Navigator (ICN) client. To be able to access the content, you must first configure ICN to connect to that repository. Then, you must associate this repository with a desktop to enable users to access the content. In this task, you configure the repository that you created in the previous task.

- In the **Mozilla Firefox** browser, click the **ICN Admin** bookmark or enter the following URL: **<http://vclassbase:9081/navigator/?desktop=admin>**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

This account has administrative rights.

- From the ICN administration page, click **Repositories** on the left pane.  
On the Repositories tab, a list of object stores that are already configured is shown.
- To create a connection to your object store, click **New Repository** and then select **FileNet Content Manager** from the list.

- On the **New Repository** tab, enter the following values:
  - Display Name: **Finance**  
The ID field is automatically populated.
  - Server URL: **iiop://vclassbase:2809/FileNet/Engine**
  - Object store symbolic name: **Finance**
  - Object store display name: **Finance**
- Scroll down and then click **Connect** to test the connection to the repository.
- On the **Log In** page, type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Click **Save and Close** to save the configuration settings for the new repository.
- On the **Repositories** tab, click **Refresh**, and then verify that **Finance** is listed.

Display Name	ID	Server Type	Server Name
 Finance	Finance	FileNet Content Manager	iiop://vclassbase:2809/FileNet/Engine

This repository is now available to be used for the ICN desktops.

- Close the **Repositories** tab.

## Edit the desktop to add your repository.

In this task, you associate your repository with an ICN desktop. A desktop called Finance Desktop is already created for your student system.

- From the **Desktops** tab, select **Finance Desktop** and then click **Edit**.  
You can also double-click the desktop to open it.
- On the **Finance Desktop** tab > **General** subtab, select the **Finance** repository for the **Authentication** section.

General	Repositories	Layout	Appearance
<div> <div>▼ Authentication</div> <div>           * Repository: <span>Finance</span> </div> </div>			



When users log in to this desktop, ICN authenticates the users of Finance object store. If the user does not have access to this object store, the access is denied.

This step is very important for all the following activities to work correctly.

- From the **Finance Desktop** tab, select the **Repositories** subtab and verify that the **Finance** and **Sales** repositories are listed for this desktop in the **Selected Repositories** pane.
- If the **Finance** repository is not listed, select **Finance** repository from the **Available Repositories** pane and then click the forward arrow (Add) to move it to the **Selected Repositories** pane.
- On the **Finance Desktop** tab, click **Save** and then select the **Layout** subtab.
- Under the **Displayed features** section, select **Browse**, and then select **Finance** for the **Default repository** field on the right pane.

The screenshot displays the 'Feature configuration' window. On the left, under 'Displayed features', there is a table with three rows: 'Home', 'Browse', and 'Search'. Each row has a checked checkbox. The 'Browse' row is highlighted in light blue. Above this table are 'Move Up' and 'Move Down' buttons. On the right, under 'Feature configuration', the 'Default repository' is set to 'Finance'. Below this is a table for 'Repository Name' with two rows: 'Sales' and 'Finance'. The 'Finance' row has an orange star icon next to its checked checkbox, indicating it is the default repository.

Feature configuration	
* Default repository:	Finance
Repository:	
Repository Name	
<input checked="" type="checkbox"/>	Sales
<input checked="" type="checkbox"/>	Finance

The default repository (listed under Repository Name) is indicated by an orange star.

- Repeat the steps to define **Finance** as the **Default repository** for the **Search** feature.
- Click **Save and Close** and then click **Close** if you are prompted with the message to refresh your browser.
- In a separate browser tab, click the **Finance Desktop** bookmark or enter the following URL: **<http://vclassbase:9081/navigator/?desktop=FinanceDesktop>**
- If you are prompted, type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that the desktop opens with the **Browse** page and **Finance** repository is listed.
- There are no folders or documents at this time. You will be adding the objects and testing the security in the following activities.
- Log out of the ICN desktops and close the browser.

---

## Activity: Modify root folder security

---

The security on the Root Folder of an object store determines who can add folders to the top level. Access to the Root Folder is typically restricted. You must restrict Root folder security if you want to maintain control over the top-level directory structure.

The initial security on the object store (that you created in the previous activity) allows all P8users (which includes many Finance security groups that are created for this course) to use the object store. They can currently add documents and top level folders to the root folder. You plan to restrict who can add folders (top folders) at the root level. In this activity, you will grant this permission only to Finance administrators. You will also create top folders for the Finance users to use.

Important: This activity builds on the previous activity, and so ensure that the previous activity is completed.

In this activity, you will accomplish the following:

- Edit Root Folder security.
- Add a folder to your repository for Finance group.
- Verify folder access.
- Examine the security settings.

### Edit Root Folder security.

In this task, you will restrict the root folder access for the P8 users to only view properties and then grant create folder access to Finance Administrators.

- 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** node and then click the **Finance** object store.
- From the **Finance** tab, expand the **Browse** node on the left pane and then click **Root Folder**.
- From the **Root Folder** tab, click **Refresh** and then open the **Security** subtab.
- Under the **Access Permissions** section, select the **P8users** row by selecting the box, and then click **Edit**.



- On the **Edit Permissions** page, notice that the **Permission group** field has **Modify properties** as the value.  
The permission allows them to create subfolders.
- Change the value by selecting **View Properties <Default>**.



**Edit Permissions**

Users and Groups : p8users

Permission type : Allow

Apply to : This object only

Permission group : View properties <Default>

☒ View all properties ☐ Modify all properties

Verify that the permission change removed the create subfolders permission.

- Click **OK** to close the page and then click **Save** on the **Root Folder** tab.

Verify that the p8users row now has View properties as its permission group.

- Click **Add Permissions**, and then select **Add User/Group Permission**.
- On the **Add Users and Groups** page, for the **Search for** field, clear the **Users** and **Special accounts** options (checkboxes), and leave **Groups** selected.
- Type **Finance** for the **Search by** field and then click **Search**.
- In the **Search Results** section, select **Finance admins** from the **Available Users and Groups** pane and move it to the **Selected Users and Groups** pane.  
Use the forward arrow.
- Select **Finance admins** on the **Selected Users and Groups** pane, scroll down, and then verify that **Allow** is selected for the **Permission type** field.
- For the **Apply To** field, select **This object only** from the list.
- For the **Permission group** field, select the **View Properties <Default>**, and then select **Create subfolder** to add a custom permission.

- Verify that the **Permission group** field now has **Custom** as the value.

Add Users and Groups

Permission type :

Allow

Apply to :

This object only

Permission group :

Custom

☒ View all properties

☐ Reserved12 (Deploy is deprecated)

☐ File in folder / Annotate

☐ Create instance

☐ Delete

☐ Modify permissions

☐ Modify all properties

☐ Reserved13 (Archive is deprecated)

☐ Unfile from folder

☒ Create subfolder

☒ Read permissions

☐ Modify owner

- Click **OK** to close the page and then click **Save** on the **Root Folder** tab.
- Verify that the **Finance admins** row is added and has **Custom** as its permission group.

Finance admins are now allowed to add subfolders to the Root Folder and they can then specify security on the folders that they create.

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

### Add a folder to your repository for Finance group.

In the previous task, you granted access to the Finance admin group to add subfolders to the Root Folder. In this task, as a Finance admin (Adam), you will create top folders and configure access to users in the various Finance groups. So that the users can add subfolders and documents in the designated folders.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or enter 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**.
- Create a new folder:
  - In the **Finance** repository, click **New Folder** from the toolbar.
  - On the **New Folder** page, type **Invoices** for the **Folder Name** field and click **Add** on the lower right to create the folder.
  - Back on the **Browse** page, verify that your new folder is listed.

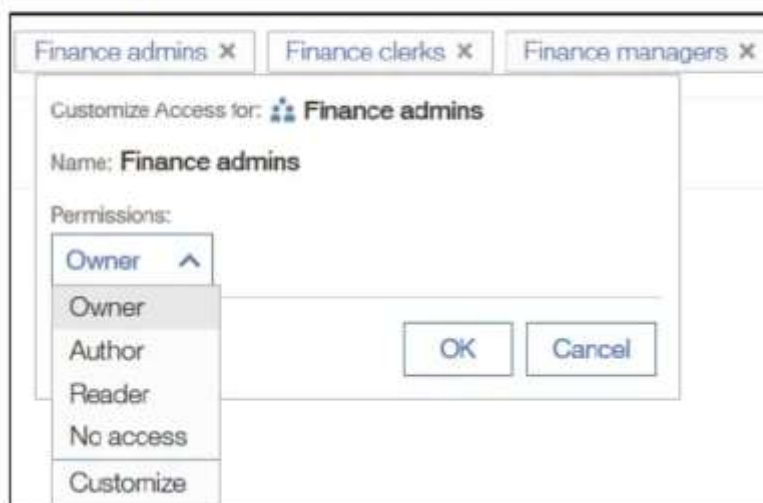


- Add **Finance** groups to the folder permissions:
  - Right-click the **Invoices** folder and then select **Properties**.
  - Open the **Security** tab, check the security details, and then click **Select** under the **Users and Groups** subtab.
  - For **Search for** field, select **Groups** from the list and then search for **Finance** groups.  
Verify that the search returns the following four groups: Finance admins, Finance clerks, Finance managers, and Finance reviewers
  - From the **Available** pane, select all **Finance** groups by holding the shift key and selecting the first and last groups.
  - Click the forward arrow to move the groups to the **Selected** pane.
  - For the **Permissions** field at the end of the page, select **Reader** from the list and then click **Add**.

The list of available security settings is different in IBM Content Navigator (ICN) as compared to Administration Console for Content Platform Engine (ACCE). ICN presents some aggregations of security settings to give end users a more intuitive set of options, whereas ACCE provides a much more granular set of options.

In the following steps, you will edit the permissions for each group.

- Click the **Finance admins** link, select **Owner** from the list for the **Permissions** field, and then click **OK**.



- Click **Finance clerks**, select **Customize** from the **Permissions** list, and then click **Advanced**.
- Select **Create subfolders** and then clear the **Add to folders** permission.

<input checked="" type="checkbox"/>	Create subfolders	<input type="checkbox"/>
<input type="checkbox"/>	Add to folders	<input type="checkbox"/>
<input checked="" type="checkbox"/>	View properties	<input type="checkbox"/>

- Review the **Finance clerks** permissions and then click **OK**.  
The Finance clerks group has a diamond icon to indicate that it has custom permissions.
- Use the following data to configure permissions for the remaining Finance groups:
  - Finance managers: **Customize - Create Subfolders, Add to folder**
  - Finance reviewers: **Author**

Properties

Security

Users and Groups

Roles

Share with: ⓘ

Specific users and groups [Select...](#)

Owner:

Adam × Finance admins × p8admin × p8admins ×

• Finance clerks × • Finance managers ×

Author:

Finance reviewers ×

Reader:

p8users ×

No access:

- Verify the completed folder permissions and then click **Save**.
- Log out of ICN **Finance Desktop** and then close the browser.



## Verify folder access.

In the previous task, you created a top-level folder called Invoices and granted access to the members of the Finance clerks group to create subfolders under the Invoices folder. In this task, you will log in as a member of Finance clerks (Carol) and create a subfolder under the Invoices folder to verify the access.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or enter 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**.
- Expand the **Finance** repository on the left pane, click **Invoices**, and then click **New Folder** from the toolbar.
- On the **New Folder** page, type **Carol** for the **Folder Name** field and click **Add** in the lower right to create the folder.
- Back on the **Browse** page, verify that your new folder is listed.  
Finance clerks group, to which Carol is part of, has permission to add subfolders.
- Log out of ICN **Finance Desktop** and then close the browser.

## Examine the security settings.

As an administrator, you can check the folder security settings in the Administration Console.

- 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 **EDU\_P8 > Object Stores** node and then click the **Finance** object store.
- From the **Finance** tab, expand **Browse > Root Folder** on the left pane and then click the **Invoices** folder.
- From the **Invoices** tab on the right pane, click **Refresh** and then open the **Security** subtab.

If the Security tab is not shown, scroll to the side to find the Security tab.

- Scroll down and then under the **Owner/Active Markings** section, observe that the user Adam (adam@edu.ibm.com) is the owner.

- Scroll up, under the **Access Permissions** section, select **Finance admins** by selecting the checkbox and then click **Edit**.

- In the **Edit Permissions** page, inspect the permissions.

The Owner permissions that you assigned in IBM Content Navigator for the Finance admins group is considered as custom access when we view it in ACCE because some of the inherited permissions were not be assigned to the Finance admins group.

If you check the permissions for P8admins group (or for Adam who created this folder and is a member of the Finance admins security admin group), they have complete permissions including the inherited ones. This is because the P8admins group was assigned to the Object store where this folder is created and the user Adam is the owner of this folder.

- Click **Cancel**.

Optionally, you can inspect the permissions for the other Finance groups in ACCE and compare them with the ones that you assigned in ICN.

- Log out of administration console and close the browser.