Use the Security Script Wizard

If you add new users to an object store that is already in production, the users have permissions only on the objects that are created after the addition of the users. To provide access to the existing objects to the new users, you can use a super group (and add the new users to the super group) as you learned in the previous section.

If you used individual users (instead of groups) in the initial setup, and now if you want to add a new user to provide access to the existing objects, you will use the Security Script Wizard.

How does Security Script Wizard work?

When you run the Security Script Wizard, the wizard assigns security roles to user and group accounts for the objects in an object store through a query to your directory service. The wizard:

- provides an interface to select an object store and a security role
- converts the user inputs into JSON data and appends it to the JSON role definition file
- merges the combined JSON data structure with the JavaScript security script
- submits the populated security script to create the security principals for the object store and the objects

Sample files for the Security Script Wizard

Content Platform Engine provides the following two sample files for use with the Security Script Wizard:

- UpdateOSSecurity.json

  The JSON file defines the security roles to be assigned and the permissions for the roles. The file also establishes communication between the wizard and the SecurityScript.js file.

- SecurityScript.js

When you run the Security Script Wizard the first time on a workstation, you must download the sample files to that workstation. You can customize these files.

Considerations when you use Security Script Wizard

The Security Script Wizard assigns security roles to user and group accounts to create security principals for the objects in an object store, with some exceptions.

The Security Script Wizard:

- sets permissions on the root folder and assigns the security on securable objects
- does not directly modify the security on custom objects, documents, and non-root folders

  Therefore, running the Security Script Wizard alone does not affect permissions on custom objects, documents, and non-root folders in the object store. After running the wizard, you can configure security parentage so that the root folder becomes the security parent of any folders, documents, and custom objects that should inherit the new permissions.
- Does not remove or modify existing permissions

Depending upon the number of objects that must be updated, the changes to the object store can take some time.

Activity: Use the Security Script Wizard

If you need to add a group of users to an object store, and you do not have an established group (like the P8users super group in the previous activity), then you can use the Security Script Wizard. The wizard allows you to assign security roles to user and group accounts to create security principals for the objects in an object store. You must run the Security Script Wizard on each object store to which you are adding the accounts.

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:

- Check a group before running the Security Script Wizard.
- Download the Security Wizard Script files.
- Run the Security Script Wizard.
- Test object store access.

Check a group before running the Security Script Wizard.

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 an IBM Content Navigator (ICN) client.

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.

The student system already has a user called Scott who is a verified member in LDAP but does not have permission to access the Finance object store that is used for authentication. In this task, you will check this status out by logging in as Scott.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **Scott** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that Scott cannot log in and get the following error: *You do not have the appropriate permissions to access the following repository: <repository name>*
- Close the browser.

  In the following tasks, you will run the Security Script Wizard to include the Script testers group (Scott is a member of this group) and repeat checking Scott's access to the ICN desktop.

Download the Security Wizard Script files.

You need the script files to run the wizard. In this activity, you will download the files.

- 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, right-click the **Finance** object store, and then select **Run Security Script Wizard**.
- Click the **SecurityWizardScript.zip** link.

- On the **Opening** … window, select the **Save File** option, click **OK** to close.
- Back in the administration console, cancel the **Security Script Wizard**, log out and close the browser.
- Open the **Downloads** (C:\Users\p8admin\Downloads) folder where the file was downloaded.

  If you cannot download the file for any reason, both the zip file and the extracted files are in the C:\Training\F2810G\SecurityWizardScript folder on your student system.
- To extract the **SecurityWizardScript.zip** file, right-click the file, select **Extract All**, and then click **Extract** on the page.
- In the **C:\Users\p8admin\Downloads\SecurityWizardScript** folder, verify that the following files are listed:

  - SecurityScript.js
  - UpdateOSSecurity.json

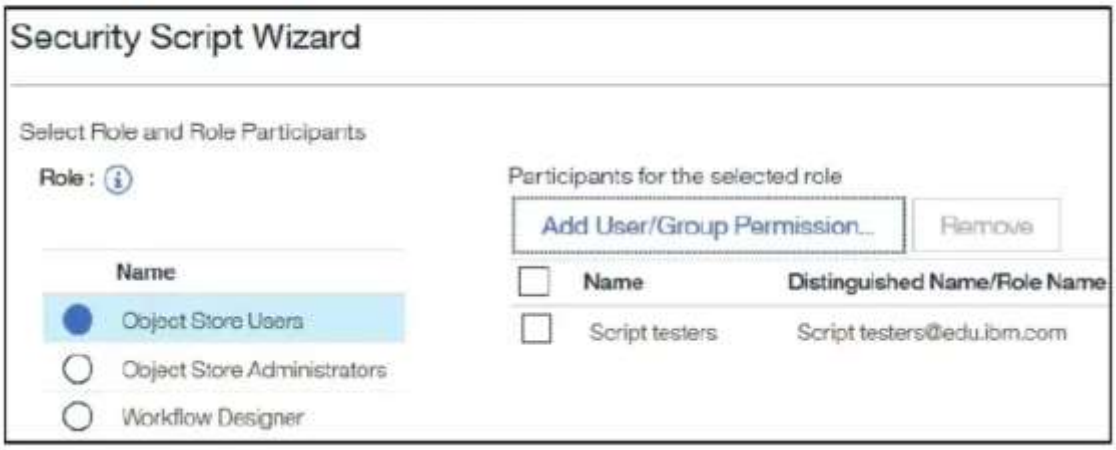
Run the Security Script Wizard.

In this task, you will run the Security Script Wizard again on the object store.

- 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, right-click the **Finance** object store, and then select **Run Security Script Wizard**.
- On the wizard page, for the **Select a role definition file** field, click **Browse**.
- On the **File Upload** page, navigate to the **C:\Users\Administrator\Downloads\SecurityWizardScript** folder, and select the **UpdateOSSecurity.json** file, and then click **Open**.
- For the **Select a security script file** field, repeat the step to select the **SecurityScript.js** file.

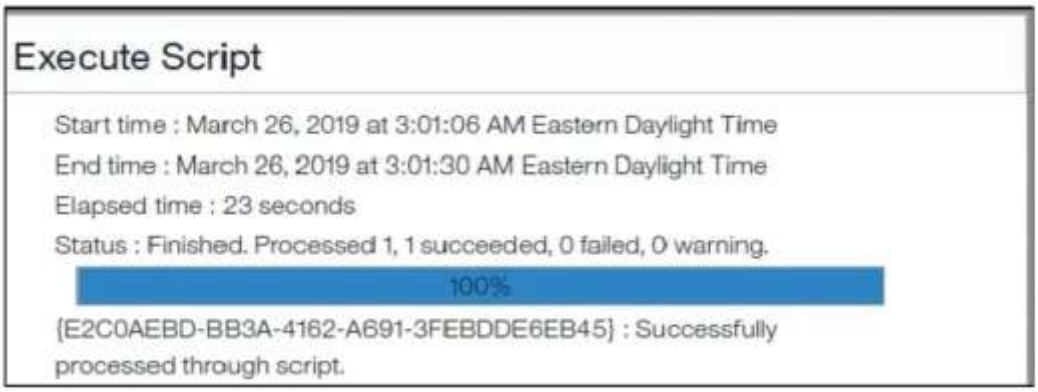
- Click **Next**.
- On the **Select Role** and **Role Participants** page of the wizard, verify that **Object Store Users** option is selected, and then click **Add User/Group Permission.**
- On the **Add Users and Groups** page, search for the **Script testers** group, move it to the **Selected Users and Groups pane** and then click **OK**.

- Back on the wizard page, verify that **Script testers** is listed.



- Click **Next**, click **OK** when you are prompted with the message about unassigned participants, and then click **Finish** to complete the security script wizard.

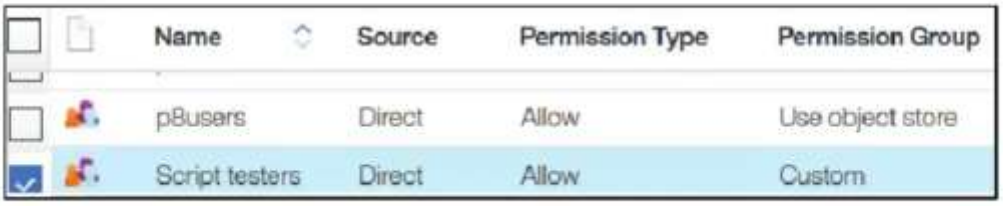
  A window will display the status. Wait for the script to complete.
- When the **Status** shows **Finished**, verify that there are no errors, and then click **Close**.



- Log out of the administration console, restart the browser, and log back in as **p8admin** (Password: **FileNet1**).
- 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, on the right pane, select the **Security** subtab and then verify that **Script testers** is listed under the **Access Permissions** section.

  The group has Custom as the value for the Permission Group column.



- From the **Finance** tab, on the left pane, expand the **Browse** node and then click **Root Folder**.
- From the **Root Folder** tab, on the right pane, select the **Security** subtab and then verify that **Script testers** is listed under the **Access Permissions** section.

  The group has Modify properties as the value for the Permission Group column.

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

Test object store access.

You ran the Security Script Wizard to provide default object store access to the Script testers group. You will now log on to the IBM Content Navigator (ICN) desktop as Scott (a member of the Script testers group) and observe the security access.

- In the **Mozilla Firefox** browser, click the **Finance Desktop** bookmark or type the following URL: **http://vclassbase:9081/navigator/?desktop=FinanceDesktop**
- Type **Scott** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that **Scott** is allowed to log in to the ICN **Finance Desktop** and has access to create a top level folder (the **New Folder** action is enabled).

  Since the Security Script Wizard sets permissions on the root folder, the Script testers group (Scott) has access to the action. However, the wizard does not directly modify the security on documents and non-root folders, Scott cannot view other existing objects.

  After running the wizard, you must configure security parentage so that the root folder becomes the security parent of any folders, documents, and custom objects that should inherit the new permissions. You will learn about setting a security parent in a later activity.

- Click the down arrow next to **Finance** on the upper right and select **Sales** from the list.
- Verify that Scott does not have access to the **Sales** object store and receives an error.

  To provide access to the other object stores, you must run the Security Script Wizard on each one.

Troubleshooting tips:

If the Security Script Wizard changes are not reflected and if you are not able to access ICN desktop, restart the application servers for Content Platform Engine and for ICN to clear the cache and refresh the system.

- On the **Windows** desktop, open the **WebSphere Admin** folder, stop the two application servers and restart them.
  - On the **Windows** desktop, open the **WebSphere Admin** folder.
  - Right-click **_3 Stop ICNserver.bat** and then select **Run as administrator**.
  - Click **Yes** if prompted to allow the program to make changes.

    Wait for the command window to close.
  - Right-click **_4 Stop server1.bat** and then select **Run as administrator**.
  - Click **Yes** if prompted to allow the program to make changes.

    Wait for the command window to close.
  - Right-click **_1 Start server1.bat** and then select **Run as administrator**.
  - Click **Yes** if prompted to allow the program to make changes.

    Wait for the command window to close.
  - Right-click **_2 Start ICNserver.bat** and then select **Run as administrator**.
  - Click **Yes** if prompted to allow the program to make changes.

    Wait for the command window to close.
- Clear the browser cache and repeat the steps to check the access for **Scott**.