How to Enable Low Authority Users[1] to Build Templates

IBM Application Runtime Expert for i

Document version: 1.0

To download the master version of this document, visit product home site:

http://www.ibm.com/systems/power/software/i/are/index.html

Table of content

Preface

In the past, IBM Application Runtime Expert (ARE) for i only allowed user with *ALLOBJ special authority on a system to build templates via the GUI. Since *ALLOBJ special authority is not normally assigned to most system administrators or person who have responsibility to check system health in an organization, due to security considerations, these people really can't use ARE. This problem has now been solved today. You can enable user IDs without *ALLOBJ special authority to use ARE, by using permission management support that is part of theIBM Web Administration for i GUI. Once the low authority user IDs are added to a permission list; that user IDs have the ability to build templates just the same as users with *ALLOBJ special authority. Using the permission management GUI of IBM Web Administration for i to escalate authority of user IDs have the following benefits:

---

[1] Low authority user means user ID which does not have *ALLOBJ special authority on IBM i.

- An Administrator ie a user with *ALLOBJ special authority is required to give the low authority user permission.

- It helps administrators to manage permissions for multiple web applications in a centralized place.

- It provides easy to use permission management panels even if you're just starting.

- Grant ARE permission to user IDs without *ALLOBJ special authority does not have an impact on system security –It is in compliance with security considerations of your organization.

To protect system security, ARE set the following restrictions for user IDs without *ALLOBJ special authority:

- When ARE permission is revoked from a user ID, the user ID still has the permission to rebuild its own templates.

- If your user ID does not have *ALLOBJ special authority, and the permission to use ARE is not granted to it, ARE allows such low authority user ID build new templates with ARE's Deployment Template Editor--- what objects' attributes it could check depends on what actual authorities that   user ID has on those objects. Once the template is successfully built, this low authority user ID becomes template owner. Template owner, user ID with *ALLOBJ authority and escalated user ID have the ability to rebuild, copy, delete, edit, export, import, rename the template. In this document, you will learn how to grant and revoke ARE permission to user ID without *ALLOBJ special authority, with IBM Web Administration for i.

Before you start

Before you start, it is important to ensure HTTP Group PTF has been updated to correct PTF level as below:

IBM i 7.1
HTTP Group PTF SF99368 level 12 or later

IBM i 6.1
HTTP Group PTF SF99115 level 25 or later

The PTF will update ARE GUI version to 2.3

1. Grant a user ID without *ALLOBJ special authority the ARE permission

In this section, you will learn how to grant a user ID without *ALLOBJ the ARE permission by using permission management support in IBM Web Administration for i GUI. When the User ID is escalated (having ARE permission), aforementioned restriction[2] is available.

Step:

1. Access IBM Web Administrator for i by http://*hostname*:2001/HTTPAdmin where *hostname* is your system the IBM Web Administration for i installed.

2. Logon administration GUI with proper user ID that must have *ALLOBJ and *IOSYSCFG special authority on the IBM i system. Only an user with *ALLOBJ can assign a lower authority permission.

Figure 1.1: IBM Web Administration for I GUI

3. Click on Advanced tab to get to manage permission page. By default, the 'By User' tab of permission GUI appears.

---

[2] Having ARE permission only allows user IDs without *ALLOBJ special authority to work on ARE's Deployment Template Editor(ARE GUI), including building, copy, delete, edit, export, import and rename a template. Such escalated user is NOT allowed to test a template.

Figure 1.2, Advanced tab-- Manage Permissions page

Figure 1.3, click on Add button to launch Add permission wizard.

4. Click on Add button to launch Add permission wizard.

5. Select one of the user ID without *ALLOBJ special authority from left All User IDs on the
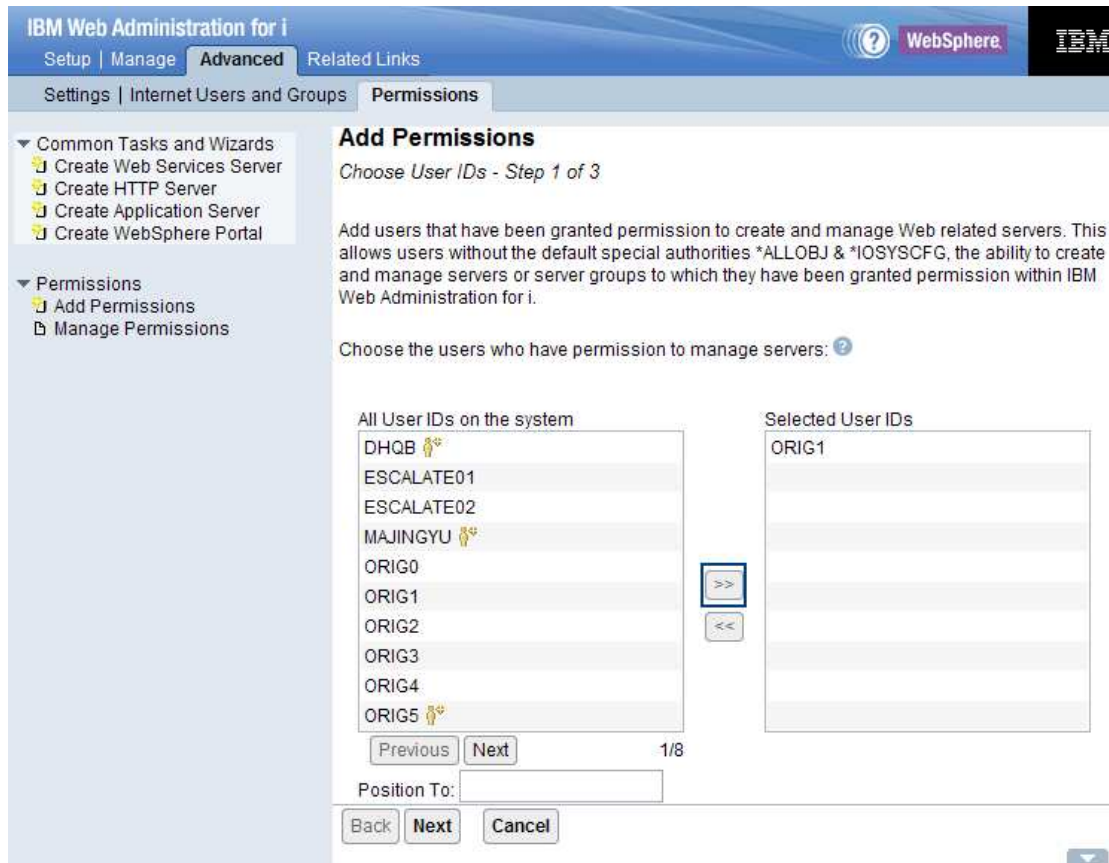   system list.

Figure 1.4, choose a User ID and move it from All user IDs on the system list to Selected User IDs list.

6. Click on ⟦ >> ⟧ button to move specified user ID to Selected User IDs list. (Figure 1.4)

7. Click on Next button to continue the wizard.

8. *Specify Permissions for Servers - Step 2 of 3* page appears.   Ensuring the ARE permission check box is selected (Figure 1.5).
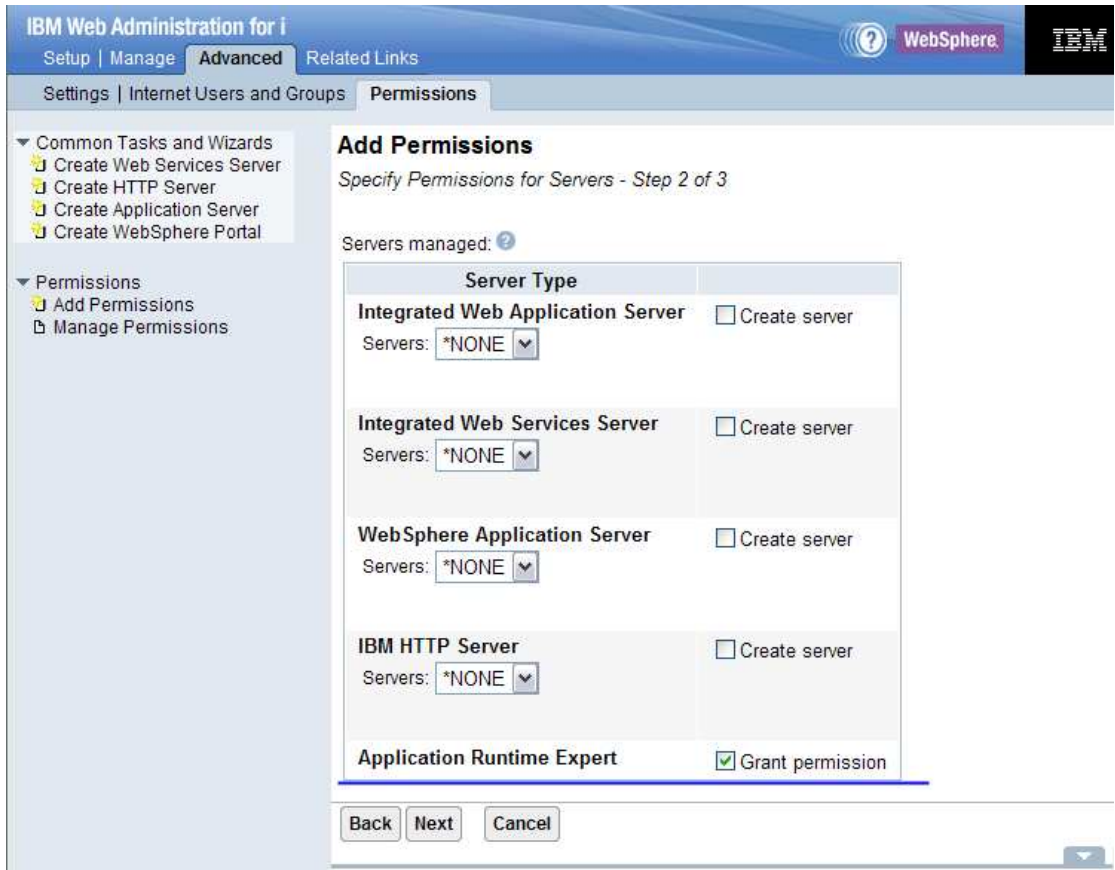
Figure 1.5, ensuring permission for Application Runtime Expert is granted to the user.

9. Click on Next button get to the summary page of the wizard.
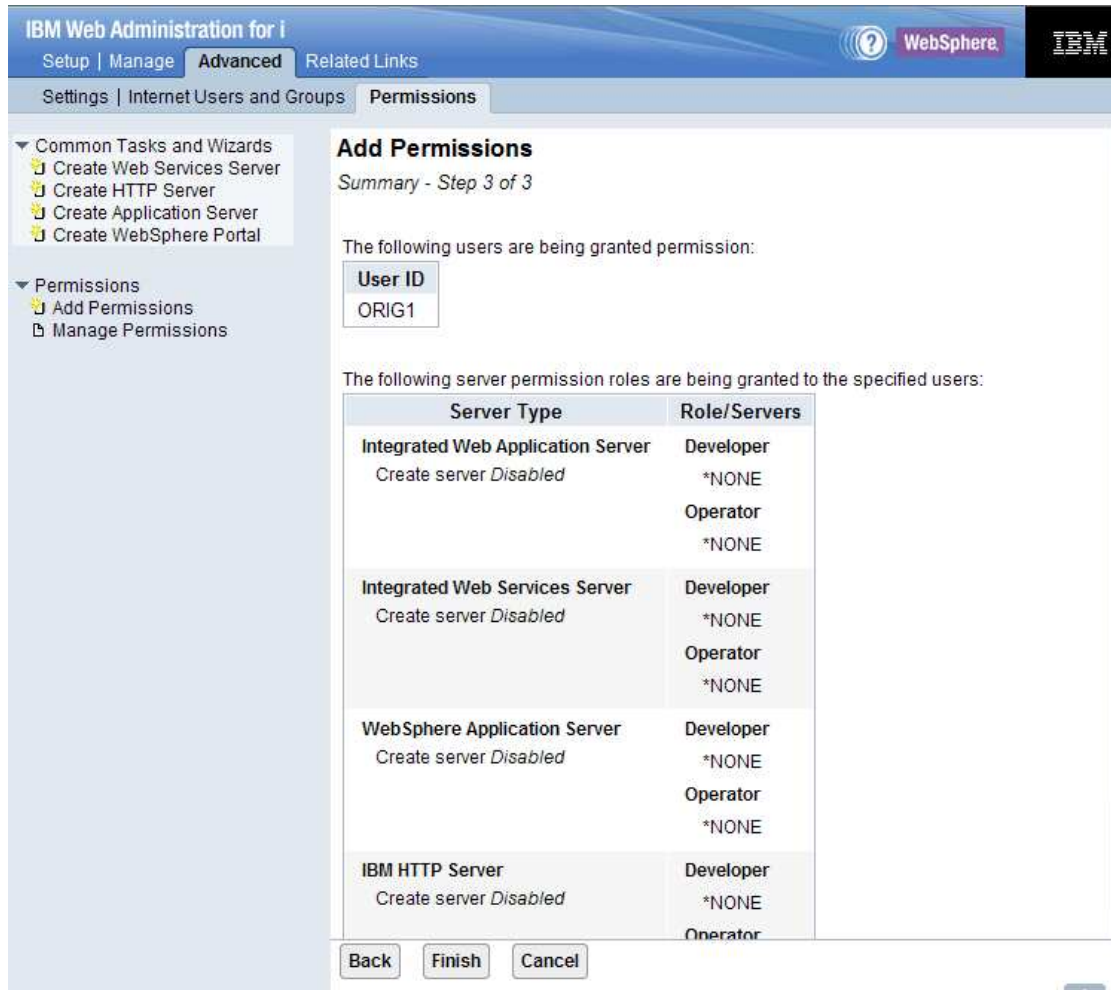
Figure 1.6, Summary page of Add permission wizard.

10. Click on the Finish button to confirm. As a result, the selected User ID appears on the "By user" list. This user ID can work on ARE deployment template editor as User ID with *ALLOBJ special authority.

Figure 1.7, the ARE permission is enabled to the selected user.

2. Revoke ARE permission for a user ID without *ALLOBJ special authority

For a user ID with ARE permission granted before, if the permission is no longer needed, you can revoke the permission by the following steps.

Step:

1. Access IBM Web Administrator for i by http://*hostname*:2001/HTTPAdmin where *hostname* is your system the Web Administration for i installed.

2. Logon administration GUI with proper user ID that must have *ALLOBJ and *IOSYSCFG special authority on the IBM i system.

3. Click on Advanced tab to get to manage permission page. By default, By User tab of permission GUI appears. You can see all escalated user IDs including the user ID that has ARE permission.

4. Select the user ID that you want to remove its ARE permission (Figure 2.1).
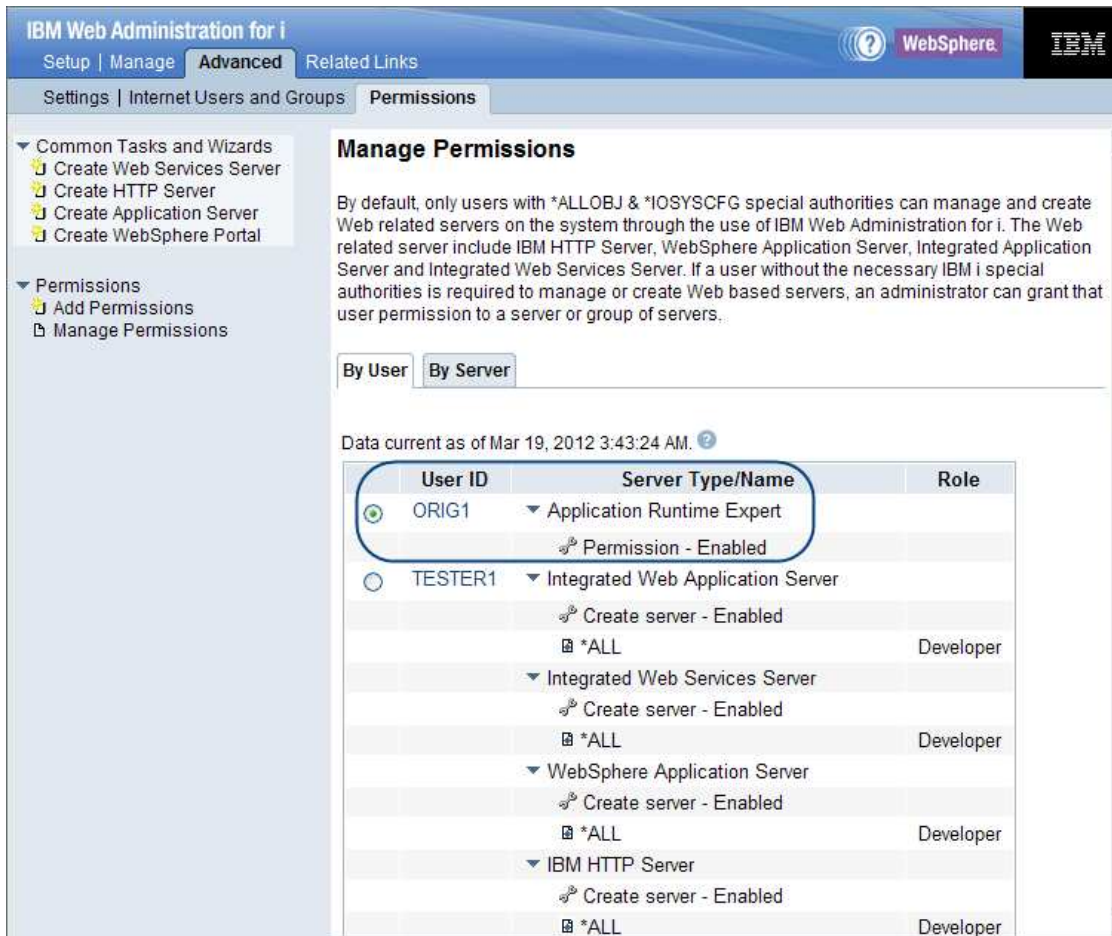
Figure 2.1, select the user ID that you attempt to remove its ARE permission

5. Click the Remove button on the By user tab (Figure 2.2) to launch the Remove Permission wizard.

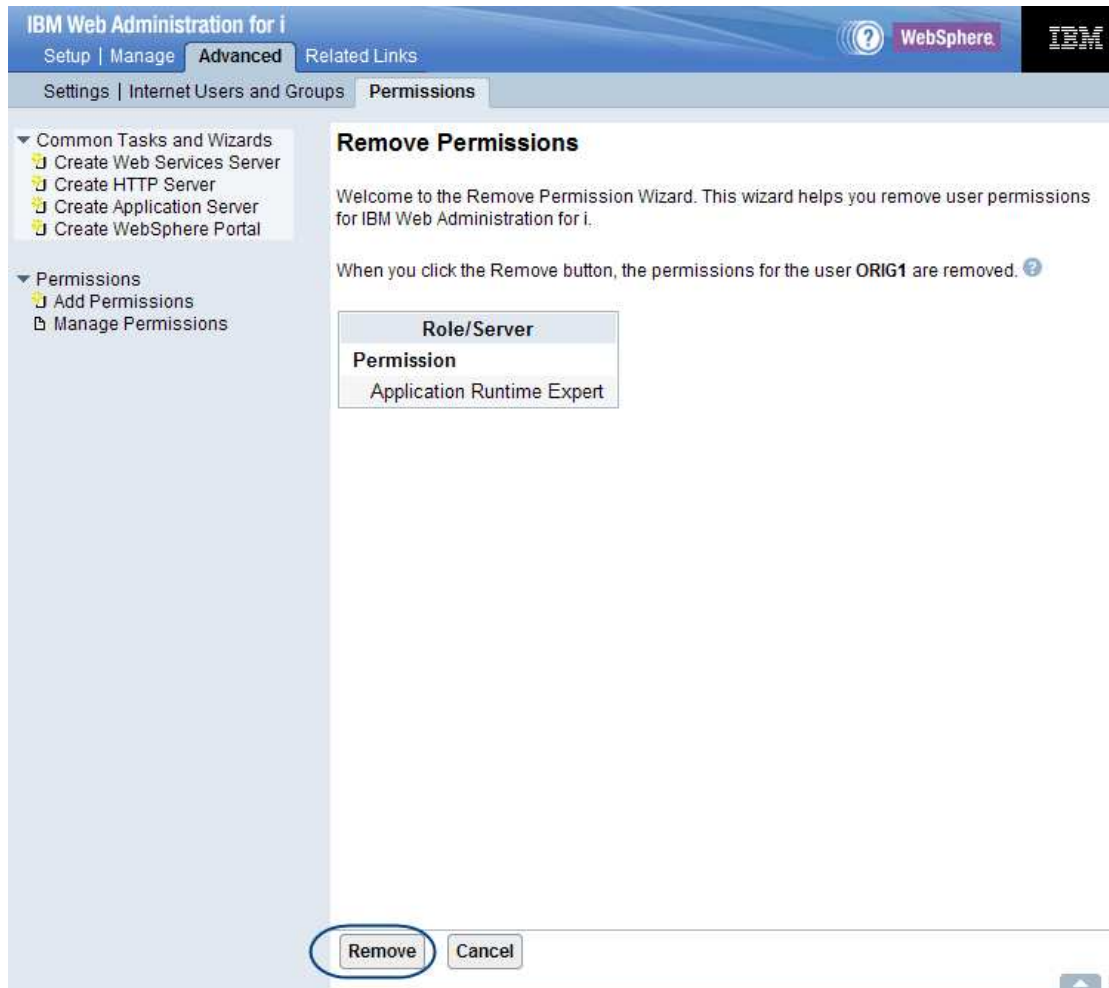Figure 2.2, click the Remove button to launch Remove permission wizard.

Figure 2.3, the summary page of remove permission wizard

6. From summary page of the Remove Permission wizard, you can see all selected User ID(s). (Figure 2.3)

7. Click on the Remove button to confirm your operation (Figure 2.3).

8. After that, GUI returns to the "By user" tab. The selected user ID is removed (Figure 2.4). As a result, aforementioned restriction[3] is available to this user ID.

---

[3] When ARE permission is revoked from a user ID, the user ID still has permission to rebuild their own templates.

Figure 2.4, after clicked Remove button on the summary page of remove wizard, the GUI return to "By User" tab.