Purdue University | Business Intelligence Competency Center
INFORMATION TECHNOLOGY

Departmental Administrator User Guide

Cognos Version 11.2.4

August 2023

General Information

A Departmental Administrator provides support to an assigned area. It is important to understand, the SAP Departmental Administrator role allows access to other departmental content folders outside of your assigned business area.

NOTE: Departmental Administrator should only work within their assigned business area and not administer other departmental folders.

Role of Departmental Administrator

- Create subfolders under the main departmental folder.
- Grant and remove access to the assigned folder for their area – when staff leave – remove access.
- Monitor naming conventions.
- Monitor where content is being saved and delete content no longer needed.
- Contact person for your area.
- Suggest reports for Standard Content
- Maintain appropriate use of departmental Administrator access (do not assign permissions, etc. for other business areas – stay within your folder)
- Have a primary and backup departmental administrator.

Becoming a Departmental Administrator

- **Business side-** you must be granted the 'BI Content Departmental Administrator' role. This can be requested by your supervisor or business office.
    - Directions on how to request access are available on the Boiler Insight Manual.

- **For Student side-** you must be granted "Set Policy" on the departmental folder.
    - Contact the BICC at bicc@purdue.edu to grant access as a departmental administrator.

- If the main departmental folder does not exist for your business area, a request must be submitted to bicc@purdue.edu for a departmental folder to be created.

Departmental Folder Naming Conventions/Recommendations

- By department name within college/school
- By topic or project name (Faculty Concurrent Appointments, PAR Reports, IPEDS….)
- By staff member name
- By Validated v. In Progress

The Shared Content folder is a temporary location to share reports/queries with other departments. Do not use this to permanently store reports/queries. When you or the user are done sharing the report, please delete or move to a departmental folder.

It is suggested users store business reports in the Departmental Content folder rather than My Folders. My Folders is a private storage area and cannot be accessed by any other user. If a report is needed by the business area, it is recommended it be saved in the Departmental Content business folder.

Setting Permissions

This training assumes the bullet points under **Becoming a Departmental Administrator** (Page 2) has been completed; the departmental administrator role has been assigned and a departmental folder created.

As Departmental Administrator, you have the authorization to grant user access to the departmental folder. You have the authorization to grant read, write, execute, traverse or set policy permissions. Based on the type of user needing access to the folder, will determine what permissions you grant.

There are two main "types" of users: Consumers (end users) and Authors.

For **Consumers**, it is advised that they are granted the following permissions **(RUN access)**:

- Read
- Execute
- Traverse

For **Authors**, it is advised that they are granted the following permissions **(WRITE access)**:

- Read
- Write
- Execute
- Traverse

Note: The Set Policy permission provides the ability for a user to administer the folder, so this permission should rarely be granted. Please discuss with the BICC staff prior to usage.

Departmental Administrator

Simple Permission Definitions

The chart below provides a definition of each permission:

Permissions	Permitted Actions
Read	View all the properties of an entry, including the report specification, report output, and so on, which are properties of a report. **Note:** A dashboard requires read permission both on the dashboard itself and on any data sources that it uses.
Write	Modify properties of an entry. Delete an entry. Create entries in a container, such as a package or a folder. Modify the report specification for reports created in Reporting and Query Studio. Create new outputs for a report.
Execute	Process an entry. For entries such as reports, agents, and metrics, the user can run the entry. For data sources, connections, and signons, the entries can be used to retrieve data from a data provider. The user cannot read the database information directly. The report server can access the database information on behalf of the user to process a request. IBM Cognos software verifies whether users have execute permissions for an entry before they can use the entry. For credentials, users can permit someone else to use their credentials. **Note:** Users must have execute permissions for the account they use with the run as the owner report option.
Set policy	Read and modify the security settings for an entry.
Traverse	View the contents of a container entry, such as a package or a folder, and view general properties of the container itself without full access to the content. **Note:** Users can view the general properties of the entries for which they have any type of access. The general properties include name, description, creation date, and so on, which are common to all entries.

Granting Permissions

The steps below walk you through granting a user permission to the departmental folder.

Steps:

1. In the Cognos Analytics **Content** pages, locate the entry for which you want to set access permissions, and select its checkbox.

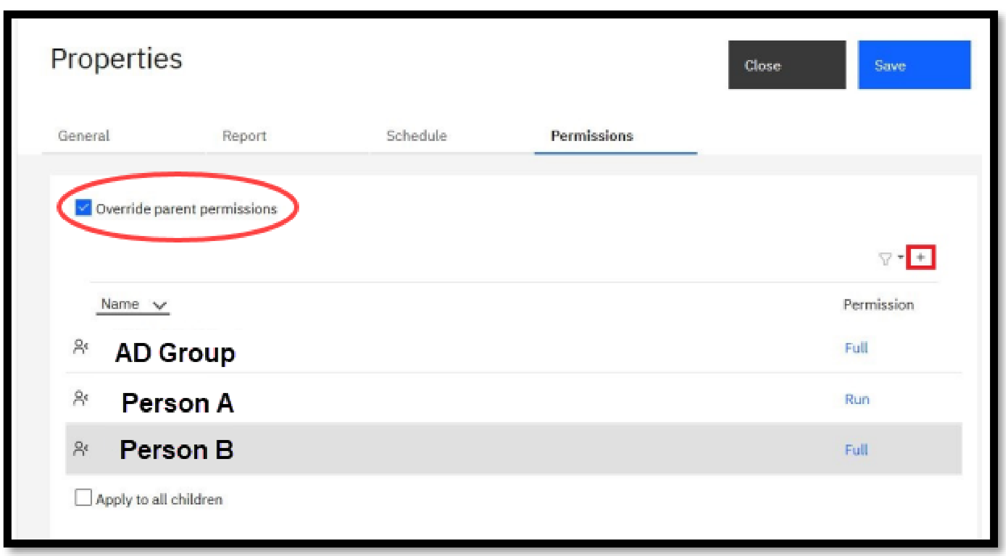
2. Click on the **Ellipsis** button beside the Folder and select **Properties**.

3. In the **Properties** page, click the **Permissions** tab.

4. Select the **Override parent permissions** checkbox.
   a. <u>**NOTE**</u>: When a new folder is created, it will inherit the permissions from the parent folder. Checking the Override checkbox will allow you to change the permissions inherited by the parent folder.

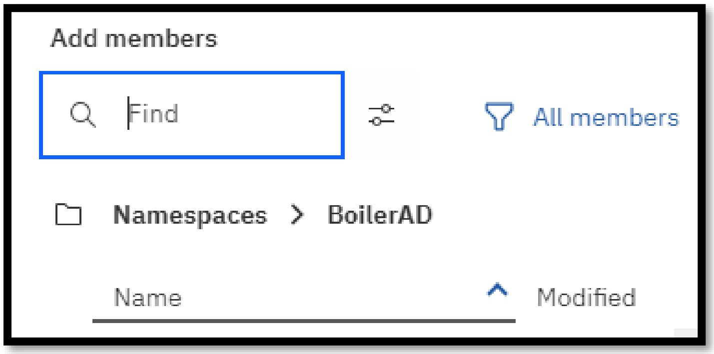
   b. You can now modify permissions for users, groups, or roles that already have access for the entry, or add new users, groups, or roles to the security policy for the entry.

   c. To add new users, groups, or roles, click the **plus icon**, as shown in the following image:



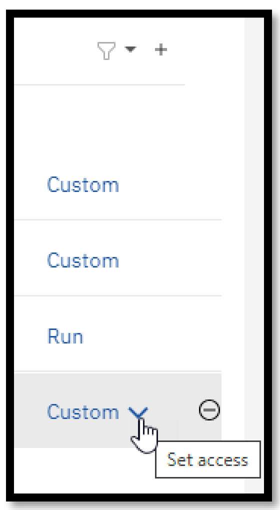
d. Click on the **BoilerAD** link under **Namespaces** section.

e. Type the username or group you want to add in the **Find** textbox and hit the **Enter key**.

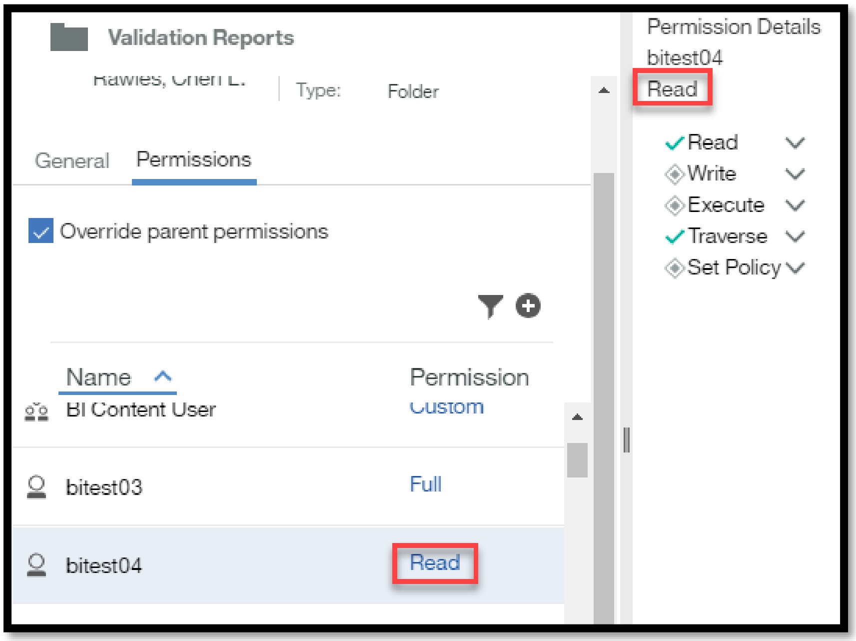


f. The name should appear. **Select** and click **Add**.

5. The users, groups, or roles are added with the **Read** access by default.
6. To grant a different permission other than **Read**, click on the down arrow  to the right of the word Read.
   a. The permissions will appear with options such as: **Read, Run, Write**, and **Full**.
   b. Refer to the Permission Definitions section on Pages 4.



7. To view the permission details, click directly on the **blue** permission.



8. Click **Save** to apply the changes.

9. If you are setting permissions for an entry, such as a folder or a package, that contains other entries, and you want the children entries to inherit the same permissions, select the **Apply to all children checkbox**.

    a. The **BI Content Dept Admin** group is granted permission to all departmental folders. Do not remove this group from the folder but be aware other departmental administrators have access to your departmental folder.

    b. The **BI Content User** group grants permission for any Consumer or Author to access your departmental folder. You can remove this group if you only want specific users from your business area to have access. (*Refer to the Remove Permissions section*).

Denying Permissions

In the last section, you learned how to grant access. You also have the functionality to deny a user or group specific access. Denied access has precedence over granted access. When denying permissions, you override the other security policies that grant permissions.

Deny permissions should not be used. It is best practice to grant permissions rather than deny. If you don't want to grant a specific permission to a member, then you will need to add the member to deny the member's permission. The member will not be given that permission. If the deny permissions are in conflict, Cognos will always deny the permission.

For example, if the user, bitest04, belongs to another group assigned to the folder, like the BI Content User, and this group has **Write** permission to the folder, but the individual member is **denied** write permission, Cognos will deny the individual access to the Validation Reports folder.

1. Once in the folder or report you want to deny permissions, click on the **Ellipsis** button beside the folder or report and select **Properties.**

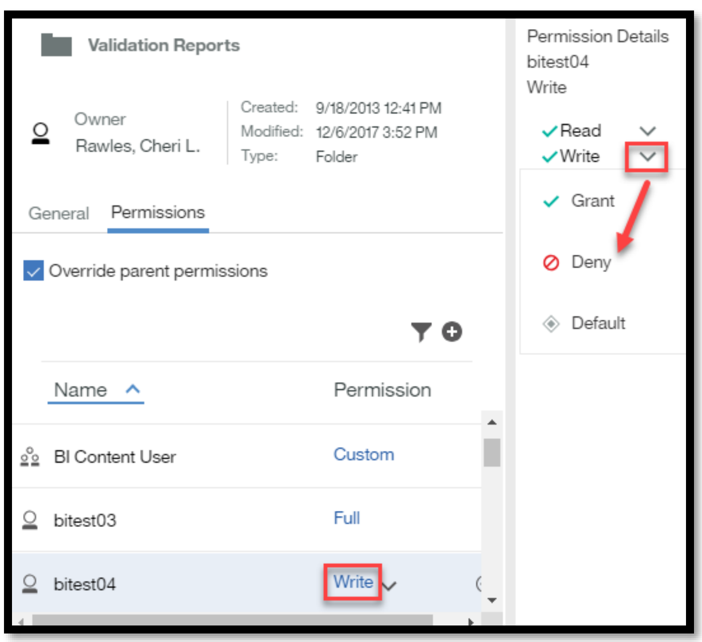
2. Click on the **Permissions** tab. In order to deny permissions, the person will need to be added individually.

3. Click the **Add** button to add new members to the folder. Click on the **BoilerAD** link under **Namespaces** section. Once the new window opens, type in the specific group or user.

4. Click the down arrow and select **Starts with exact string.** Type the last name or user name of the member you want to add in the textbox and hit the **Enter key**.

5. The name should appear below. **Select** and **Add**. The new member is now added to the **Name** section in the **Permissions** tab.

6. When denying permissions, click directly on the blue permission to display the permission details. Click on the down arrow to the right side of the permissions title you are wanting to deny. Click **Deny.**



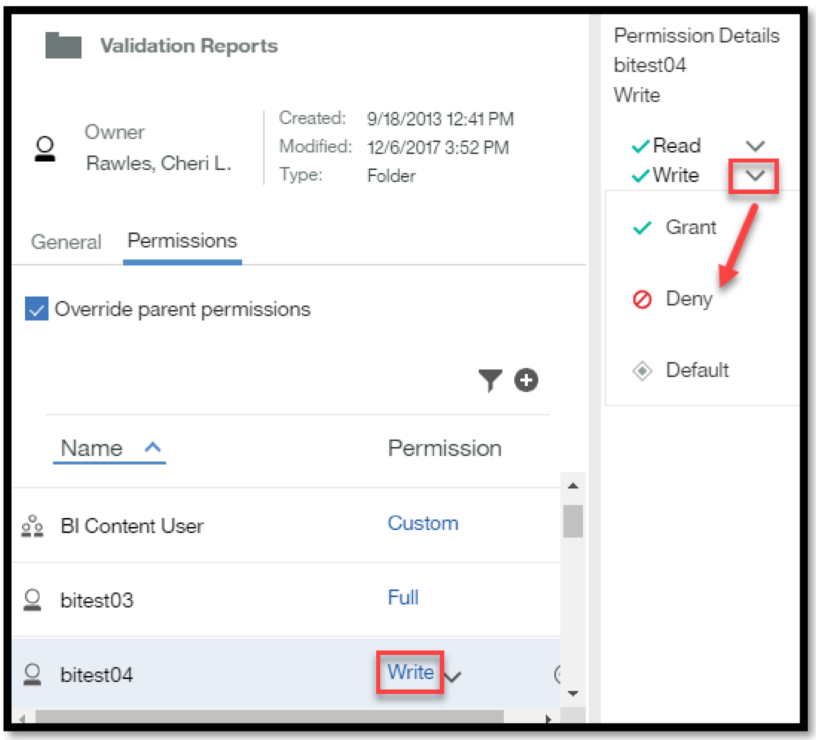
Removing Specific Permissions

The steps below walk you through removing a specific permission for a user to the departmental folder.

Steps:

1. Once in the folder or report you want to deny permissions, go to the **Ellipsis** on the folder or report. Click on **Properties** and the **Permissions** tab. To edit a specific permission

2. When denying permissions, click directly on the blue permission to display the permission details. Click on the down arrow to the right side of the permissions title.



3. Click **Deny** then click **Apply.** The permission will change to **Custom.**

Removing Users/Groups

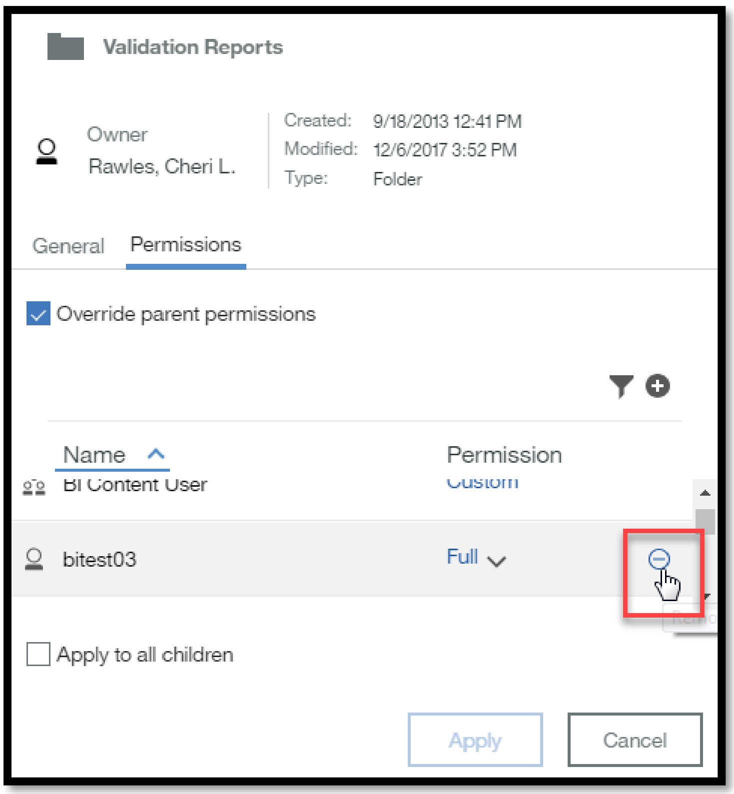
The steps below walk you through removing a user/group completely from the departmental folder.

Steps:

1. Login to Cognos and navigate to the Departmental Folder created for your area.

2. Click on the go to the **Ellipsis** on the folder or report. Click on **Properties** and the **Permissions** tab and view the list of users with permissions to this folder.

3. Check the **checkbox** next to the user you wish to remove folder access. In this example, we will remove bitest03.



4. Click on the **Remove** button**.**

5. The member will be removed. Click **Save** and close the Set Properties window.

Troubleshooting

Please contact the BICC at bicc@purdue.edu with questions specific to this manual or for any Cognos questions or issues.