

Implementing Security

- Only users with Super Administrator, Administrator, or Full Control privileges can create or modify security permissions.
- For additional information refer to Citadon CW On-Line Help for specific functions categorized by permission level.

This Guide describes security implementation in four areas for Citadon CW, Administration (Organization and Workspace), Document Management (folders, documents and binders), Reports and Business Process (Logs, setup, instances).

Administration Security

When a new organization or workspace is created two groups are automatically created, Super Administrator and Administrator.

The members of the Super Administrator group have full control over all aspects of their organization, OUs and assigned workspaces. They can add or remove members from the Super Administrator and Administrator groups. It is recommended that a select group of individuals be assigned to the Super Administrator Group.

The members of the Administrator group have full control over all administrative objects of the workspace, except that they cannot add or remove members from the Super Administrator or Administrator groups. They also cannot modify user-created groups.

Additional groups can be defined by either the Super Administrator or the Administrator group to provide a subset of the administrative functions. These permissions are categorized as:


View: User can view the object (report, workspace, organization, organizational unit, etc.), view security settings on the object, view some properties of the object, and view some related objects.

Modify: In addition to view permissions, the user can modify some of the properties and perform add / remove functions.

Full Control: In addition to all modify permissions, the user can modify security settings, change the administrator attribute, and delete (some objects). Users with Full Control can also Create, Modify, and apply Custom Attributes

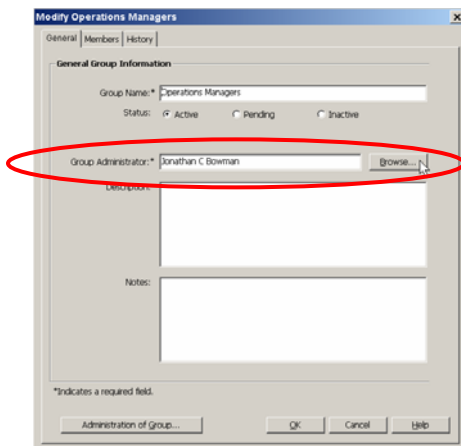
Group Management




Individuals can be selected to be Administrators of any Organization or Workspace groups to allow them to manage adding and deleting members. When the **Create** or **Modify** button is clicked for a specific

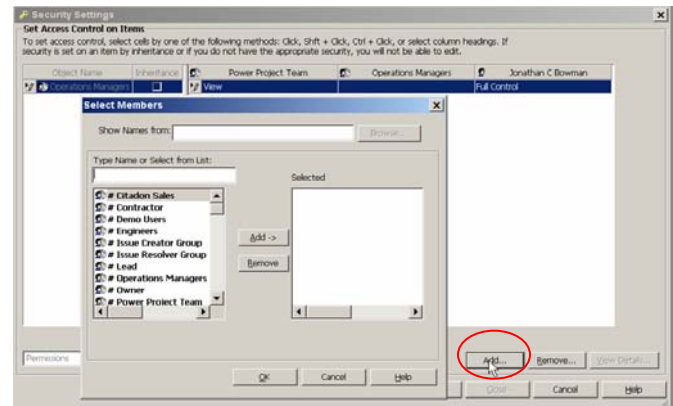
group the following dialog box appears. Click  to select a specific team member.

If additional groups or individuals need to have access to the group to view, modify (add/remove), or change security then they can be added to the Group security definition by clicking on the **Administration of Group** button shown at right.

On the Security Screen, you can add or remove groups or individuals to or from the security definition.

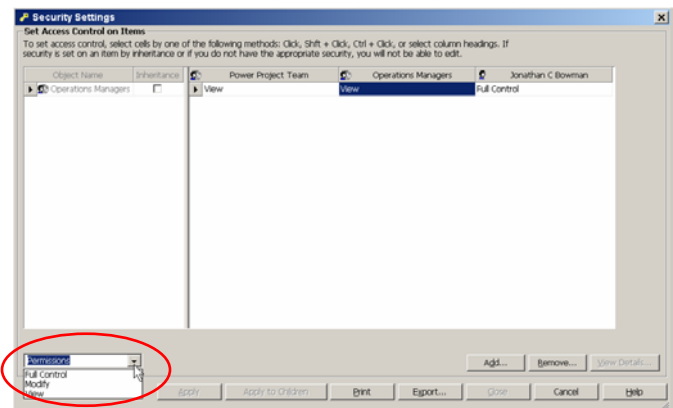


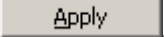

First, if you are in the DMS make sure the Inheritance checkbox is unchecked. Then select the row for the object and click . Select the appropriate group or individual from the Select Members list and click  to add them to the definition. When finished, click . The permission defaults to **View**.



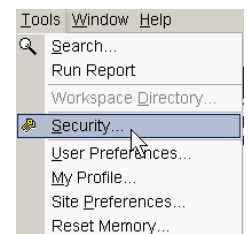
To change the permission, select the cell displaying the **View** permission, then click the **Permission** combo box in the lower left.

You can modify the security permission for several groups or users by selecting cells in combination with the Ctrl or Shift keys. You can also click on the column header displaying the name of a group or user to modify all of the security permissions listed below those groups or users. That is especially helpful when modifying the security of several items as explained in the following sections.



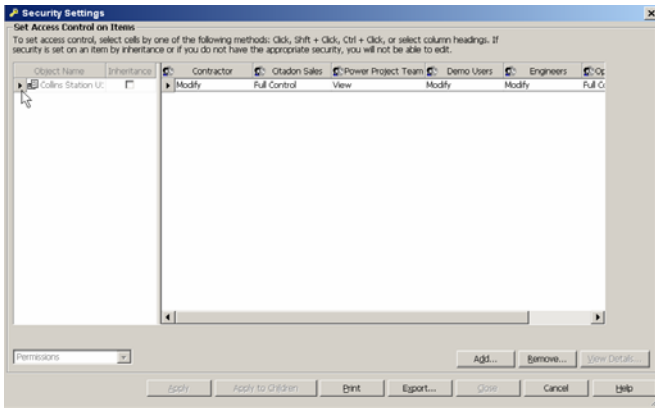
When finished click . After the changes are completed, then click .

As a Super Administrator or Administrator you can also set the default security for all new objects created in the system such as folders, documents, binders, etc. This is done by selecting **Security** from the **Tools** menu when you are on the Organization or Workspace name or from the Summary Page **General Information** screen.





After selecting **Security**, the Security Settings screen appears.

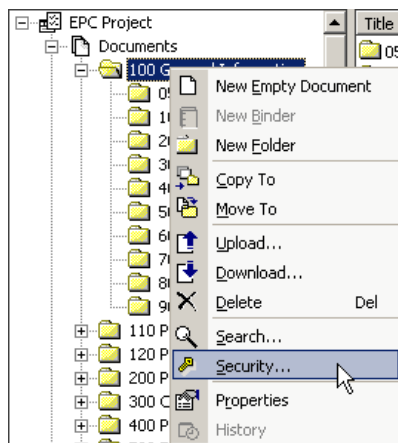


Changes can be made to add, remove, or modify group or individual security settings as described above. These settings will be the default for new objects created or added in Citadon CW.

Document Management System Security

Members of the Super Administrator group by default have full control permission for all objects (folders, documents, binders) in the Document Management System area. As noted above, the default settings can be modified for all newly created objects by modifying the Workspace security settings. This change is applied to existing objects only if the inheritance check box is checked for top level folders and other objects (subfolders, documents, or binders).

With the inheritance check box unchecked, the Super Administrator and those who have full control security permissions may set the security for folders, subfolders, documents and binders by navigating to the desired object and then selecting **Security** from the **Tool** menu bar or right click pop-up menu.



Note:, if you right click on Documents, the menu will not show Security. Security for the DMS as a whole is inherited from the defaults established for the Workspace. See *Administration Security* above.

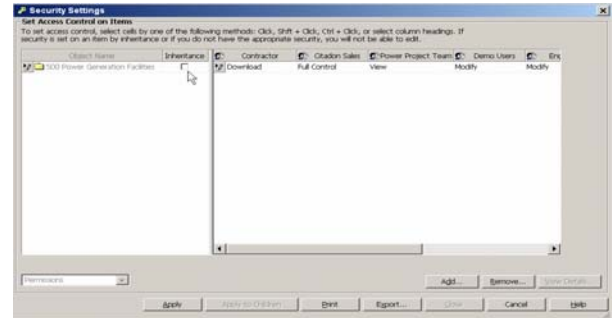
Inheritance

By default the Inheritance checkbox is checked. In this mode, each newly created object will inherit the security settings from its parent. For the top level folders this means the security will be inherited from

the Workspace security. For subfolders, the security is inherited from its parent folder. Documents and binders inherit the security settings of their parent folder or subfolder.

Modify Security

To modify security from the default, click **Security** and the standard Security Settings dialog box appears.



Make sure that the Inheritance box is unchecked, then add, remove or modify the settings as explained in the Administration Security section above.

For the DMS, the security permissions are:

Not Set: Security access permissions are not set

View: The user is allowed to see the object (folder, document, or binder), view its properties, view its security settings and view its contents. A user with view permission is also able to annotate documents using the Citadon CW viewer.

Download: In addition to View permissions, the user is allowed to download or copy the item to another location. Note that Download permission is needed to be able to Open a document in its native application on your desktop.

Publish: For a folder - In addition to Download permissions, the user is allowed to create a binder or empty document, or upload a new document into that folder.

For a document or binder - In addition to Download permissions, the user is allowed to lock or unlock the object or create a new revision of it. The person who publishes the original revision of a document or binder is the owner of that object and therefore has full control rights for that object.

Modify: In addition to Publish permissions, the user is allowed to modify the attributes of the object.

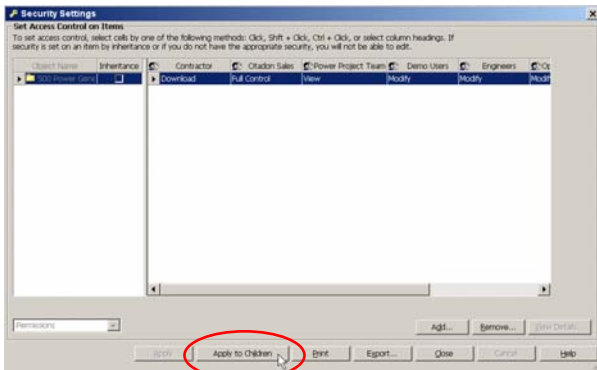
Full Control: In addition to Modify, the user is allowed to move, delete, and modify the security of the object. A user with Full Control can not, however, modify the security to exclude the Owner of the object from having Full Control access to it.

For a more detailed listing of the functions that each security permission is entitled to refer to the matrix included in the Online Help.

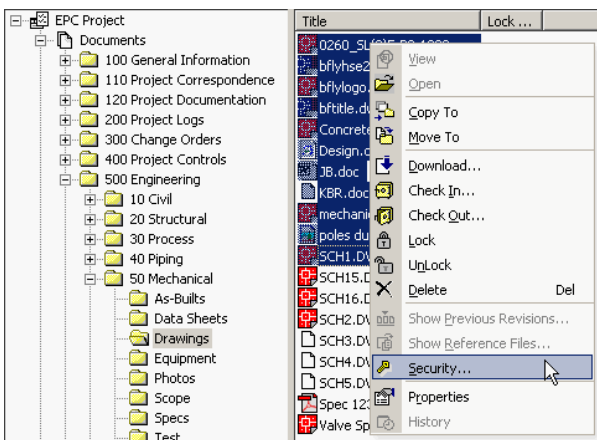
Apply to Children

After a change is made to the security settings for a folder or subfolder any lower level subfolders, documents, or binders which are inheriting from that folder will inherit the new security immediately.

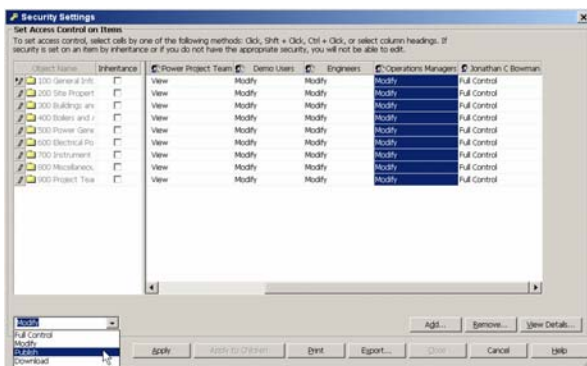
However, if the Inheritance box is **not** checked in some or all of the lower level items, you can still “push” the security changes down. To push the changes down, click on the box to the left of the folder to select the entire row in the security grid. The **Apply to Children** button will then be available. Clicking that button will provide a one-time “push” of the folder security to lower level items within the folder.



To modify the security settings for several objects at one time, such as unchecking the Inheritance check box for all the top level folders, select the folders, subfolders documents or binders in the right hand window and right click to select **Security**.



The Security Settings dialog box lists all the selected objects. You can modify the security permission for several groups or users by selecting cells in combination with the Ctrl or Shift keys. You can also click on the column header displaying the name of a group or user to modify all of the security permissions listed below those groups or users.



Binders

Binders contain links to documents, business process instances, or other binders. Security can be set on binders to control the types of functions that individuals and groups can perform on them. Binders are stored in folders and thus can also be set to inherit the security of its parent.

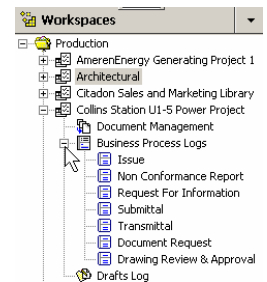
Links within binders are pointers to objects stored elsewhere in the Workspace. The security on those links is the same as the security set on the original source of the link, so links within a binder can be set to have security permissions that are different from the binder itself.

Business Process Security

Security can be established for the Business Process (BP) Log listing in the navigator, on each individual log, on the setups for each BP, and on the individual BP instances.

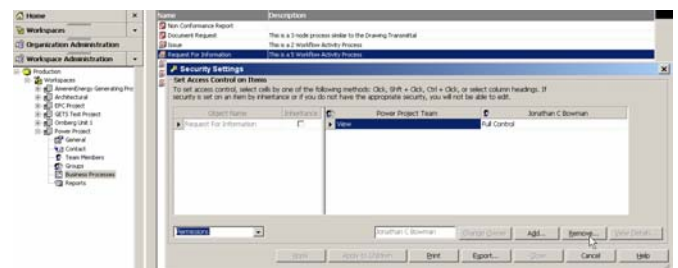
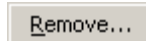
BP Log Listing

In order for the Workspace Team members to be able to see and select the appropriate business process to work on, the first item they need access to is the list of Business Process logs in the navigator. By default, when a new project is created, or a BP is linked or copied to the workspace, the default security shown on Security Settings dialog box is Team = View and Super Administrator group = Full Control.



This is sufficient if you want all the BP logs visible to Team. If not then the security may be modified so the Team does not have access. This is done, as shown below, by selecting the business process in the Workspace Administration area and selecting security from the right click menu.

- Within the Workspace Admin area, double-click on the Business Processes in the Quicklist
- Next select each business process template name individually and select **Security** from the **Tools** menu bar or the right click.
- To Remove the Team, select the Team and click



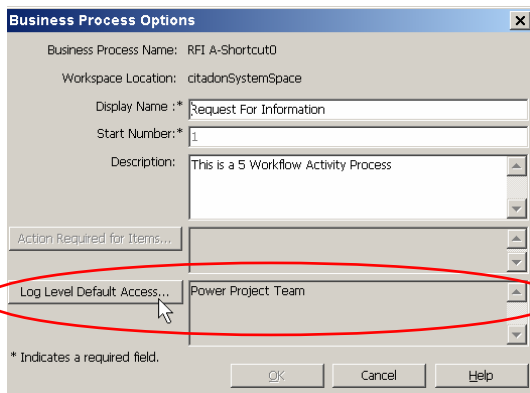
- Click **Add** to add groups or individuals to the right window.
- Next, select the group/individual and then click on the **Permission** combo box and select the appropriate permission, full control, modify or view. Modify allows modification of some of the properties in the business process. Typically either view or full control, allowing others to change security are the options selected.

BP Log Level Access

By default, when a user creates a new BP instance, the log access for viewing and checking on the status of the new BP instances is

restricted to only the participants of the specific instance. If you want the log and all of the contents (except as noted below) visible to the Team or specific groups then you need to:

- ✎ Click to select the BP in the list in Workspace Administration.
- ✎ Right click on the BP name and select **Options** (see below).
- ✎ Click **Log Level Default Access...**
- ✎ Next, select the group and individuals from the User Selection dialog box.

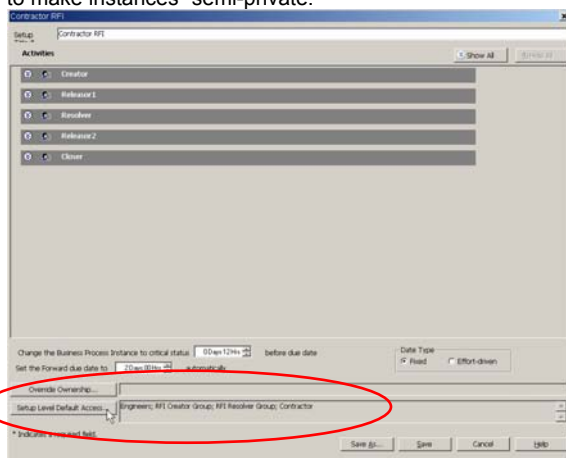


With the settings as shown above the Project Team has access to the Request for Information log. Any team member will be able to view all the instances created, unless they are restricted by the Setup Level security as explained next.

As a minimum, the BP Log Level Access and the BP Log Listing, described in the previous section, should be reviewed and set for each business process.

BP Setup Level Access

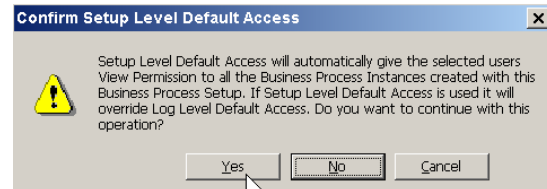
BP Set-ups describe the possible participants and the rules for each step of the business process workflow. Access to specific instances, created by a set-up can be restricted even though an individual has view access to the log. Set-up level access is controlled from the Workspace Administration area on the BP Set-up dialog. When a setup level access is defined it will override the access granted at the log level described in the preceding section. This method can be used to make instances “semi-private.”



The above shows that although the Team has access to the log, they will not be able to view any of the instances created using this BP setup. The example shows that for this Contractor RFI set-up, the Contractor, Engineers, RFI Creator, and RFI Resolver groups only

have access to these instances as well as any others specifically involved in the instance.

Before the access is revised a reminder dialog box is displayed as shown below to ask you to confirm your intent and reminds you that this will override the log level access.



Reports

Report security can be set on a Report Type in the administrative area of the Workspace or Organization, or on a Report Instance in the Report Log. Security permission set on a Report Type in the administrative area controls which users can administer or run a specific type of report within that Workspace or Organization. Security permissions on a Report Instance in the Report Log controls which users can view or administer a report instance which has been run and saved.

Administrators navigate to the Reports window of the Workspace or Organization Administration area. In the Organization Administration area, users who are members of the Super Administration or Administration group for the Organization have permission to modify the administrative security of reports. In the Workspace Administration area, users who are members of the Super Administration group for the Organization or Workspace and users who are members of the Administration group for the Workspace have permission to modify the administrative security of reports.

Selecting one or more reports and choosing Security from the menu displays the standard security window described in sections above. Users and Groups can be added or removed from the window and permission can be set to either Full Control or Run. A user with Full Control permission can generate the report and modify the security to allow others to run it. A user with Run permission can generate a report within that Organization or Workspace.

Reports Instances which have been run and saved are stored in the Report Log. The user who generated the report has Full Control to that instance by default and is the only user who can see it. That user can select the instance in the log and choose Security from the menu to modify the security permission to it. To change the security, select one or more instances from the Report Log and choose Security from the menu. The standard security window described in sections above is displayed. Users and Groups can be added or removed from the window and permission can be set to either Full Control or View. A user with Full Control permission can view the report instance, modify the security on the instance, or delete it. A user with View permission can view report instance only.

For more information about Reports, see the *Standard Reports Quick Reference Guide*.