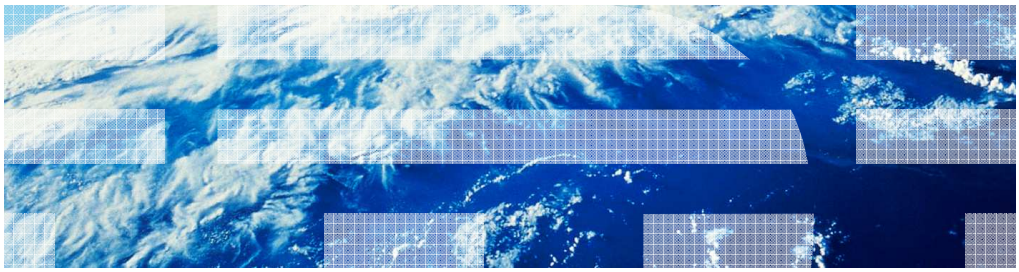
# IBM Tivoli Common Reporting V2.1.1

## Setting up report authorizations





IBM Tivoli® Common Reporting V2.1.1, Setting up report authorizations.

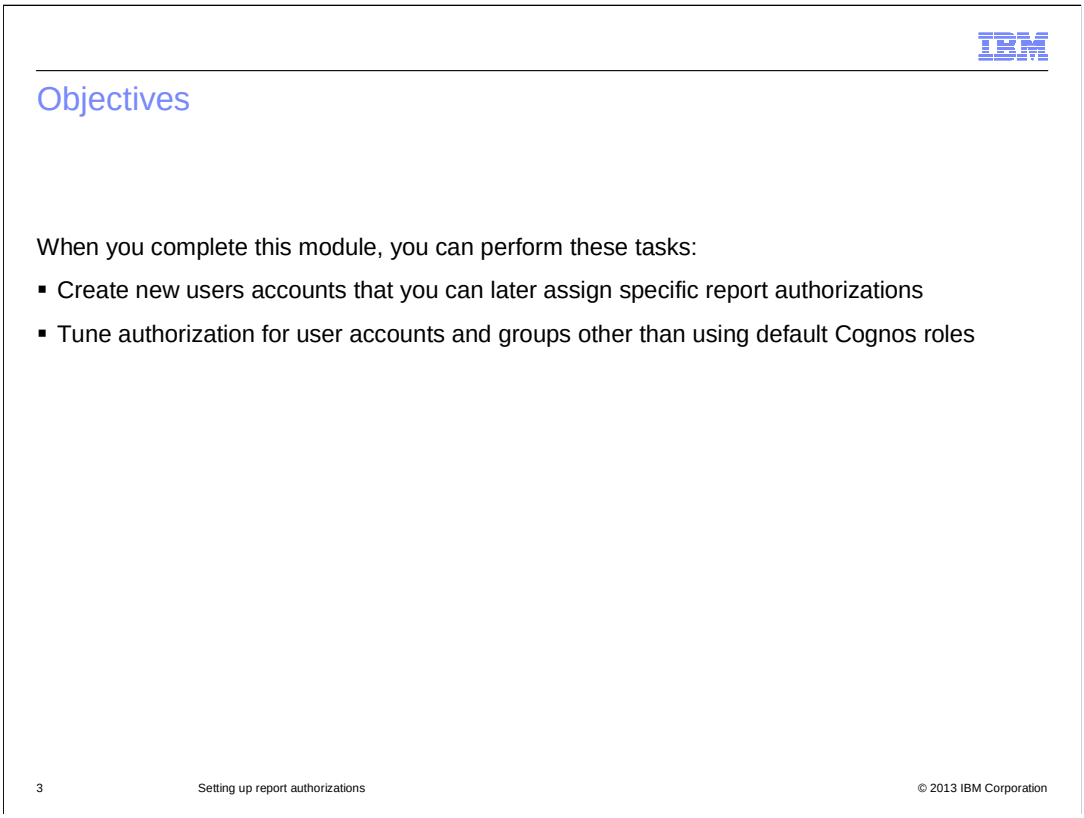
## Assumptions

Before you proceed, the module designer assumes that you have these skills and knowledge:

- Basic knowledge of Tivoli Common Reporting
- Basic knowledge of Cognos® features that are embedded into Tivoli Common Reporting
- Basic knowledge of the Tivoli Integrated Portal authentication and authorization method




The module developer assumes that you understand basic Tivoli Common Reporting concepts and how Cognos Engine and Cognos features fit within Tivoli Common Reporting. It is useful to have a basic knowledge about Tivoli Integrated Portal authentication and authorization. In this module, you create new user accounts and groups to assign them Cognos-specific roles or use them directly with Cognos Report authorization configurations.

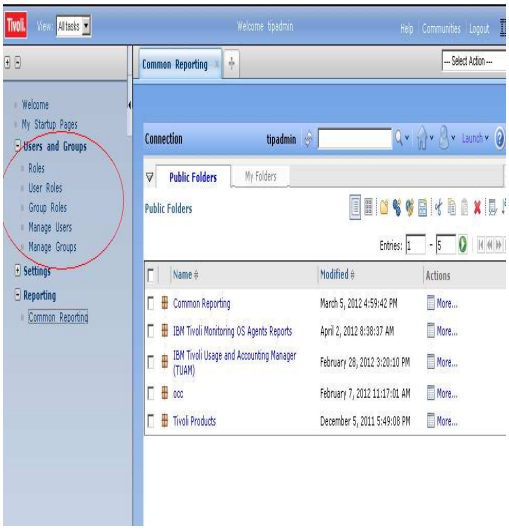



When you complete this module, you can perform these tasks:

- Create new users accounts that you can later assign specific report authorizations
- Tune authorization for user accounts and groups other than using default Cognos roles

## Users and groups

- Tivoli Common Reporting uses a federated repository for user and group authentication
- You can create new users and groups from Manage Users and Manage Groups navigator items
- New users and groups must have the **tcrPortalOperator** role to see Tivoli Common Reporting navigator items.
- The newly added users and groups are then available from Cognos panels to configure report authorization




4 Setting up report authorizations 

For authentication purpose, Tivoli Common Reporting uses a federated repository. By default it uses an internal file repository, but it can be configured to use Lightweight Directory Access Protocol (LDAP) or Active Directory after installation.

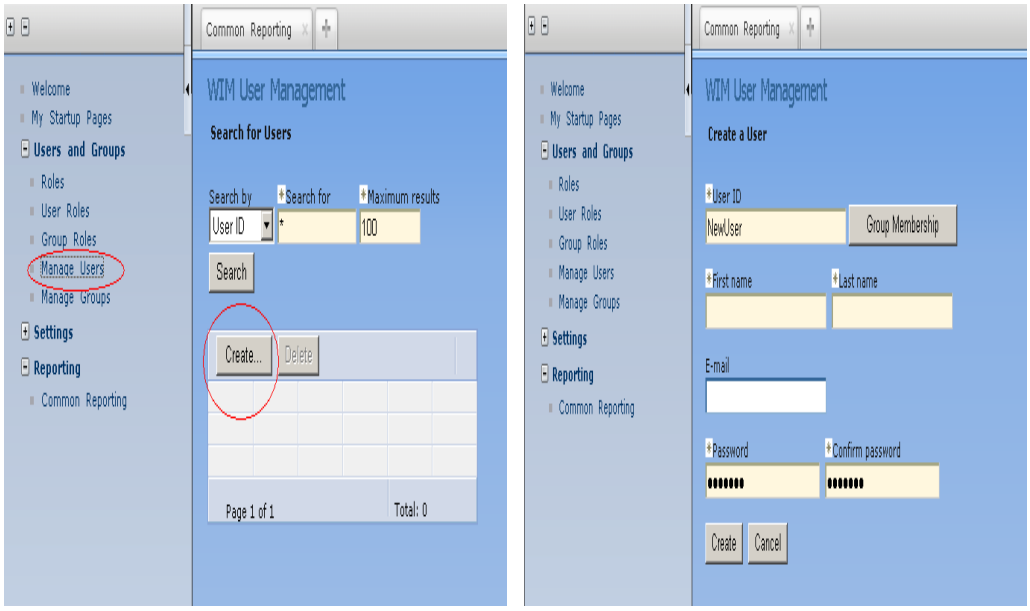
With a file repository, all of the user accounts and groups are contained in this file and they do not need to exist anywhere else.

If you need to define a new user or a new group, click **Manage User and Manage Group**.

The main condition for the new users to see and access Tivoli Common Reporting navigator items is to assign their account the **tcrPortalOperator** role.

To assign a role, click either **Users Roles** and **Group Roles** beneath the **Users and Groups** navigator item and assign the **tcrPortalOperator** role to the user or group.

## Creating new users and groups




5 Setting up report authorizations 

In this example, if you want to create a user account, select **Manage Users** and then click **Create**.

You are prompted to provide the **user ID** and other information, including the **Password**. To complete the user creation, click **Create**.

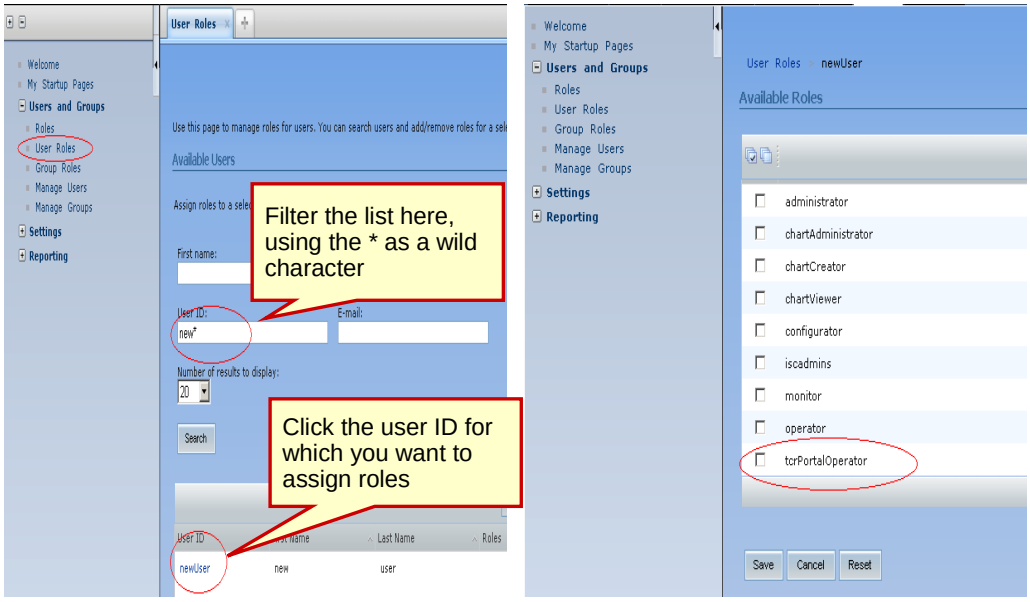
Fields with a yellow background are the mandatory fields and must be filled.

If it is required to assign a group to the new user, click **Group Membership**. Remember that a group must be created before it can be assigned to a user account.

To create a group, from the Manage Groups navigation item, perform similar steps to create a user account.

You can use groups to efficiently perform a report authorization task. If you do not want to use the *predefined Cognos roles*, you can create custom groups and assign the required roles to each group. For example, to assign user accounts that belong to the same department or that require similar roles to a group, you can set authorizations for the group or groups instead of using single user accounts.

## Adding the tcrPortalOperator role




6 Setting up report authorizations 

To add or remove Tivoli Integrated Portal roles to the newly created users, click **User Roles**. These roles have nothing to do with Cognos Report Authorization, they are specific for Tivoli Integrated Portal authorization.

For a user to be able to view the Reporting, Common Reporting navigator item in Tivoli Integrated Portal, you must add the **tcrPortalOperator** role to the user account.

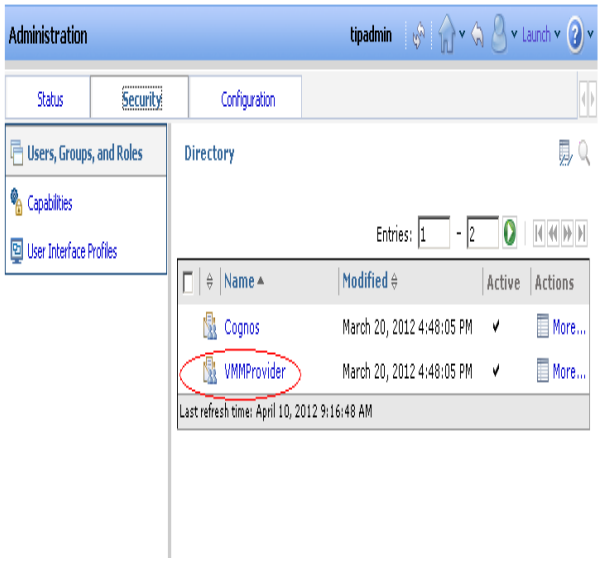
Look at the left screen capture. To assign a role to a specific user, find and click the user ID in the list. You can filter the user ID list by providing a prefix followed by the asterisk (*) character in one of the available fields. In this example, the **User ID** field is set to filter the data for names that begin with **new**.

In the example, the User ID clicked is **newUser**. The screen capture on the right shows the list of available roles. You must select the check box for the **tcrPortalOperator** role. You can select more roles as required. When all required roles are selected, click **Save**.

After the required role is assigned, when someone logs in with the user account, they can see the **Common Reporting** item under **Reporting** in the left navigation panel of Tivoli Integrated Portal.

## Implementing report permissions

- This task can be accomplished in the following ways:
  - Using predefined Cognos roles
  - Assigning permissions directly to users and groups
- The users and groups created in the federated repository are available in the VMMProvider security namespace
- For a distributed Tivoli Common Reporting installation, VMMProvider is not available and you need to use the namespace that is configured during LDAP configuration instead




7 Setting up report authorizations 

Now you define a new user and you can define *Report Permissions* for the account.

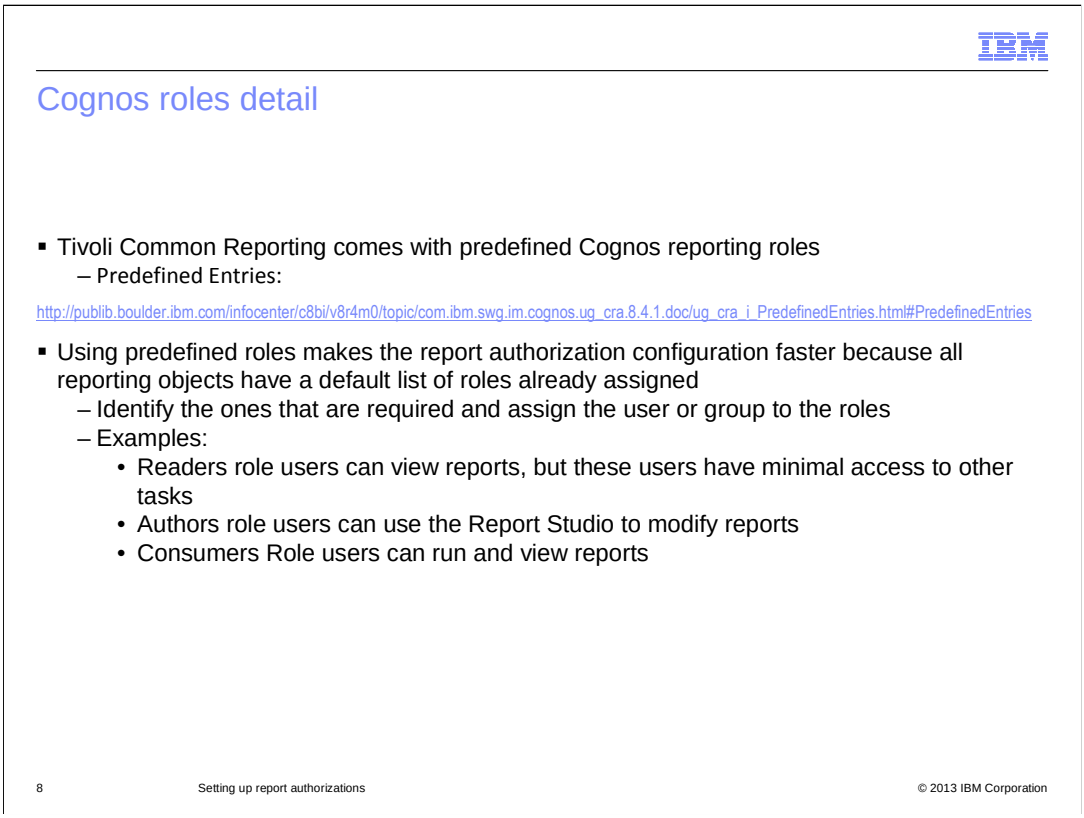
You have two possible options, the first one uses existing Cognos roles. Identify the most suitable role for specific tasks and assign the user account or group to that Cognos role. Because each report or report package is assigned a default set of permission settings for the available Cognos roles, you do not need to alter report permissions settings.

The second option is to assign specific permissions to users and groups directly at report or report package level.

With either option, you can select the new users or groups that are previously defined, because they are available under the VMMProvider security namespace.

If you performed a distributed Tivoli Common Reporting installation, this namespace is not available. Instead, it is replaced by the namespace you provided during LDAP configuration.

The security namespace is the object where users and groups can be retrieved.




The *Cognos Administration and Security Guide* provides a table with all the available Cognos roles and their descriptions. You can use this table to understand the role you need for your newly created user or group. If you use predefined roles, you can complete the job faster because you do not need to access each reporting object, report, or report package to modify authorization settings.

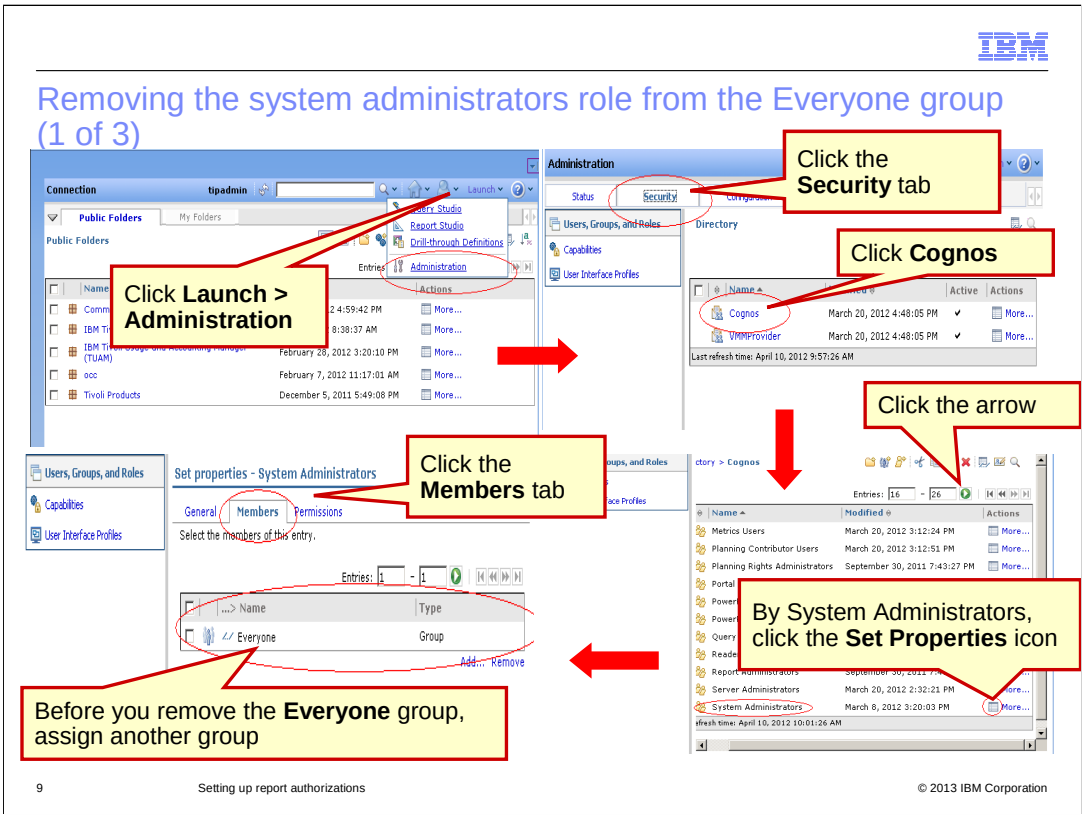
Each reporting object is created with a preconfigured set of Cognos roles and each role has specific permission.

As shown in the example, users that are assigned with the Readers role can view the reports, but these users have minimal access to other types of tasks. Author users can modify or create new reports with the Report Studio or Query Studio tools. Consumer users can instead, run and view report outputs.

If you decide to use the Cognos roles, you need to identify the wanted role and assign the new user or group to it without modifying reporting objects permission settings.

But you might want to use users and groups directly within the Reporting Object permission setting instead without passing through the Cognos roles.

In both cases, before proceeding, you must perform an initial step, which is presented next.




By default, all authenticated users are included in the **Everyone** Cognos group.

The predefined Cognos System Administrators role includes the **Everyone** group. To avoid having all users be considered System Administrators, you must remove the ***System Administrators*** role from the **Everyone** group.

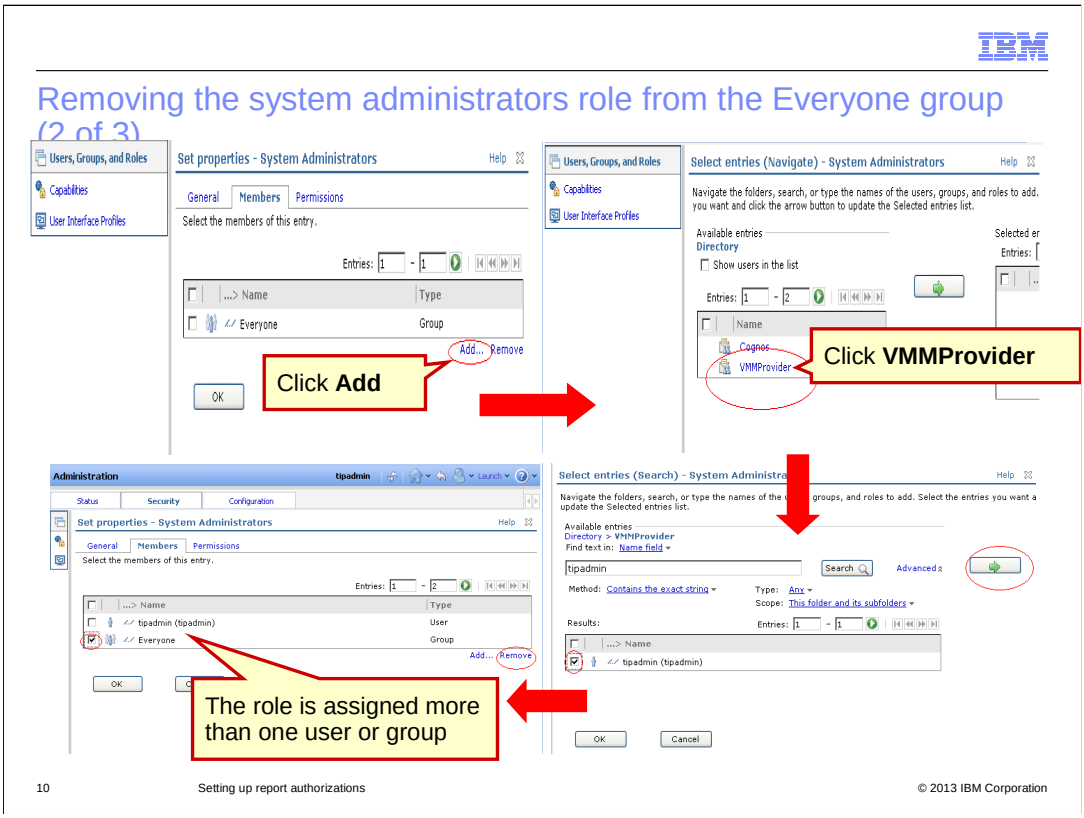
To open the Cognos Administration panel from the menu, click **Launch > Administration**.

From the Administration panel, click the **Security** tab and then the Cognos namespace to be displayed with the list of available Cognos roles.

Because the System Administrators role is the last of the 26 entries, click the arrow to move on to the second page. By the System Administrator entry, click the **Set Properties** icon.

On the Set Properties panel, click the **Members** tab to see the members assigned with the System Administrators role.

As you can see, you have the **Everyone** group assigned with the ***System Administrators*** role. Before you can remove the **Everyone** group, you must assign at least one other user or group to the same role.




In this example, you can assign the user account **tipadmin** the ***System Administrators*** role and then remove the **Everyone** group.

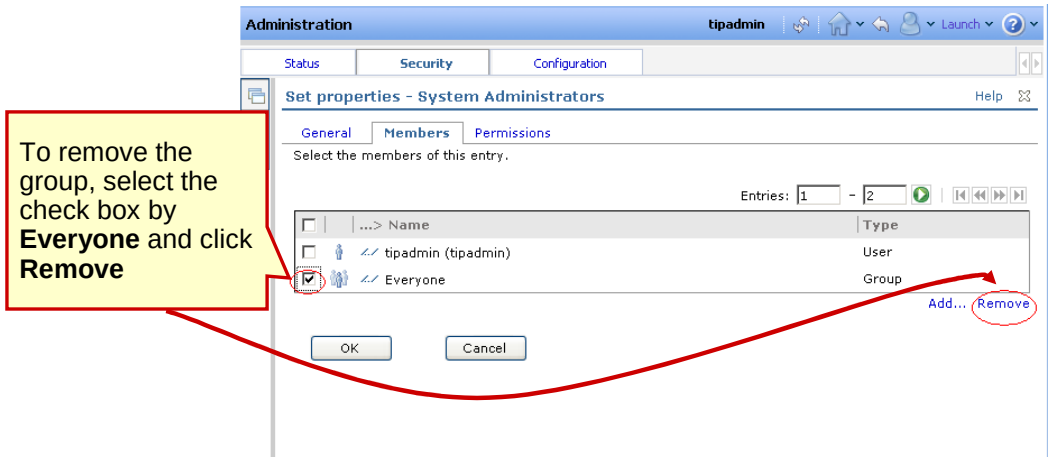
To give the tipadmin user the ***System Administrators*** role, you need to click **Add** and then click the **VMMProvider** security namespace, which is the container for all the users and groups as previously explained.

In the Select Entries panel, to search for the available user ID, click the **Search** link. Select type **Any** to include both users and groups. In the **Find Text** field enter the criteria; in this example, **tipadmin**.

The Search function returns a list of available users. Select the check box for **tipadmin**, click the Green arrow to add the user ID to the **Include** list, and click **OK**.

After you assign the **tipadmin** user ID to the ***System Administrators*** role, it has more than one group or user assigned so you can remove the **Everyone** group.

## Removing the system administrators role from the Everyone group (3 of 3)





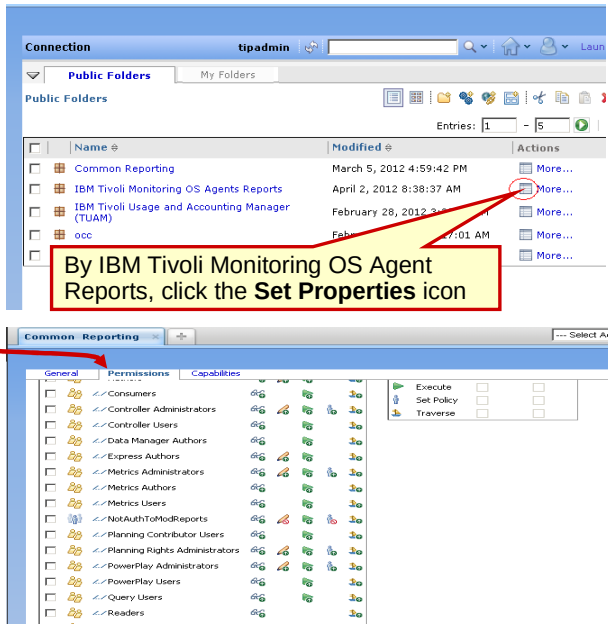


To remove the **Everyone** group, select the check box and click **Remove**.

You can proceed with authorizing the new user or group to the required roles or directly change the permissions of a specific Reporting object.

## Reporting objects permissions (1 of 2)

- Tivoli Common Reporting Reporting Objects are
  - Single reports
  - Report packages
  - Other objects
- The Set Properties panel shows you the object permission settings, under the **Permissions** tab





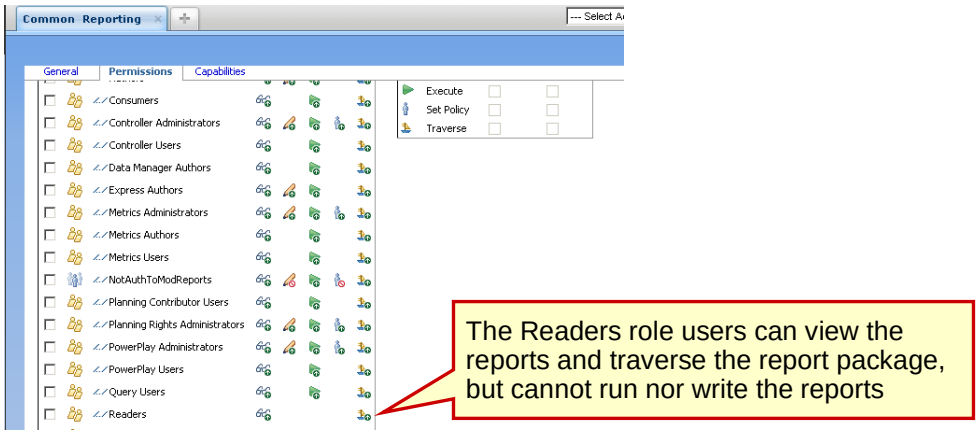


You can change authorizations and permissions on report packages, like the one listed in the top picture, or directly to specific reports.

In this example to see the Permissions settings for report package that is called **IBM Tivoli Monitoring OS Agents Reports**, first click the **Set Properties** icon and then click the **Permissions** tab.

## Reporting objects permissions (2 of 2)

- You can alter the permissions settings that are assigned to specific Cognos roles (not suggested)
- You can add newly added users or groups here and then provide the wanted permissions



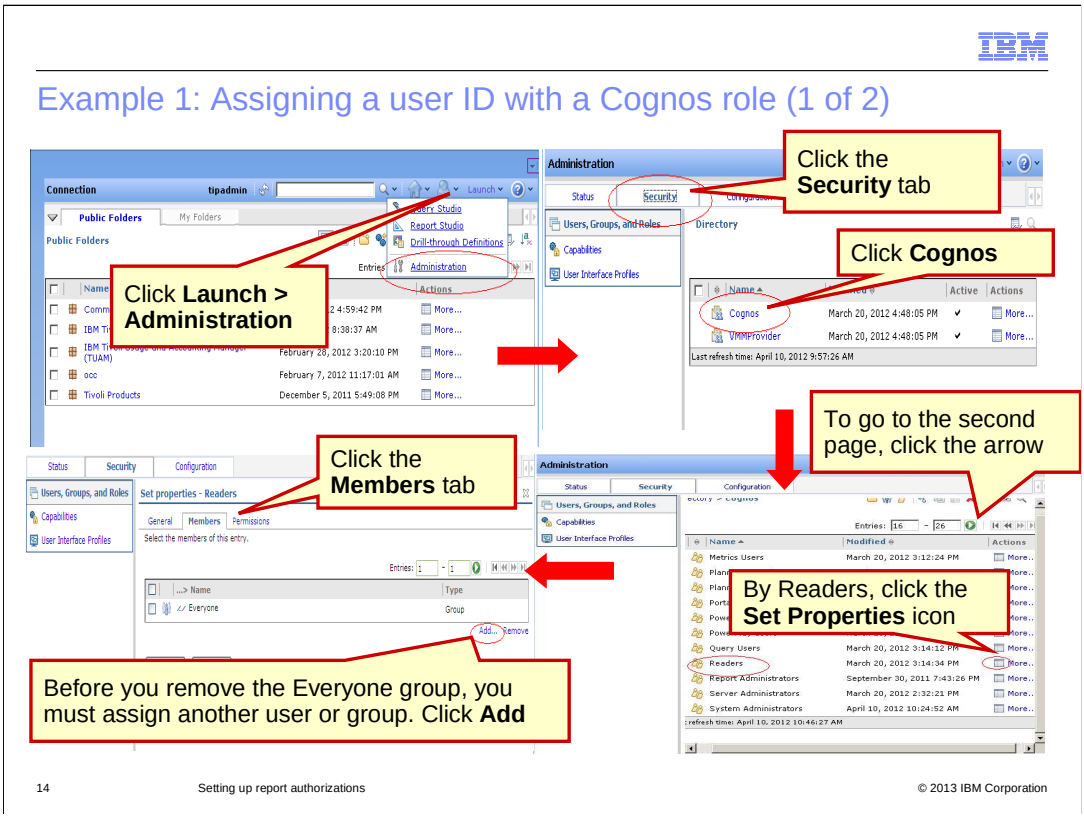

13 Setting up report authorizations 

All of the default Cognos roles are listed with the predefined settings. In the example, the Readers role users can view the reports and traverse the report package, but cannot run nor write the reports.

If you want to, you can change the Permission setting for the Cognos roles by adding or removing permissions. It is not a good idea for you to change them because the roles are supposed to serve specific tasks and are well suited for them.

It is better, in this example, to add the user ID or group ID and provide the needed permissions.

This lesson shows two examples. The first example uses a predefined Cognos Role. The second example, adds user IDs directly within the Reporting Objects Permissions definition.




Example 1: Assigning a user ID with a Cognos role.

Suppose that you identified the Readers role as the one you need for your newly added user ID or Group ID.

Similar to other Cognos roles, like System Administrators, the Readers role is assigned to the Everyone group by default.

To prevent all the authenticated users from access to the Readers role, you need to remove it. You must add the required users or groups to the Readers role before you can remove the Everyone group.

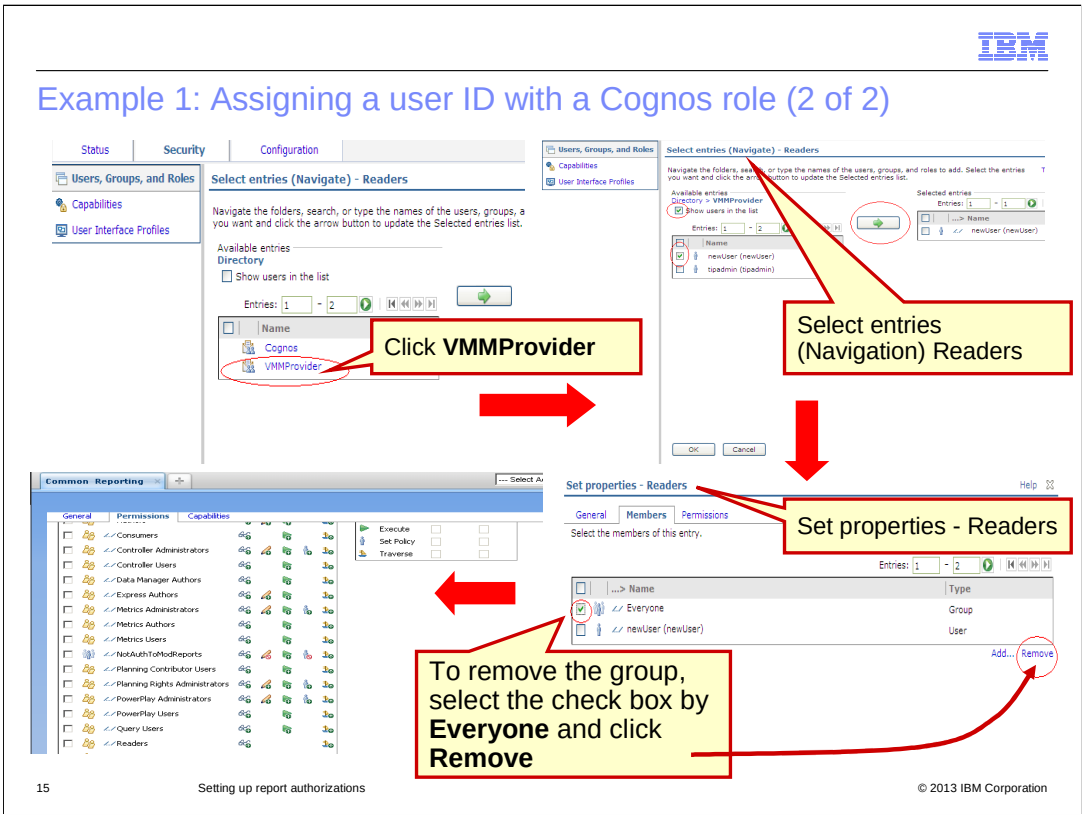
Start from the **Launch** menu, click **Administrations**. The Administration window displays. On the **Security** tab, click **Cognos**. The list of available Cognos roles displays.

The Readers role is on the second page; click the arrow. When you locate the role, click the **Set Properties** icon.

On the **Members** tab, you can see users or groups assigned the Readers role. Remember that by default, the Everyone group is assigned the Readers role.

Before you can remove it, you must add a user or group. For this example, you can add the newUser ID previously created in the federated repository.

Click **Add**.




In the Select Entries panel, click **VMMProvider** security namespace. The list of available entries displays.

On the Select entries (Navigation) Readers window, you can either use the search option or select the check box for **Show Users in the List** to display the list of the user ID available in the repository. The list is displayed in the example.

In this example, select the check box for **newUser** and click the green arrow to add it to the include list. To complete the operation, click **OK**.

You assigned the ***Readers*** role to the user ID newUser. With similar steps, you can assign Cognos roles directly to groups.

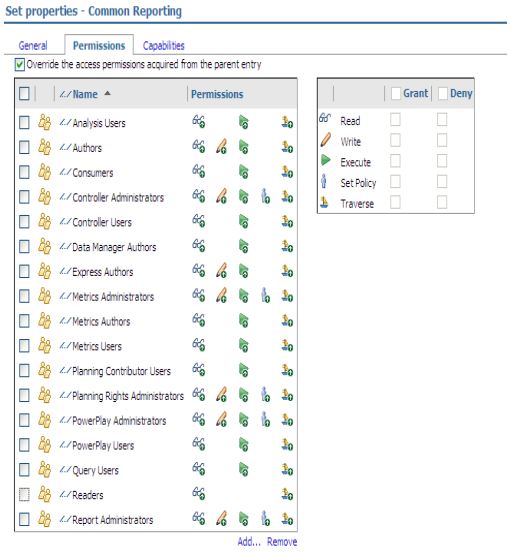
In the lower right image, **Set properties - Readers**, you can see both a user and a group are assigned to the Readers role.

To remove ***Readers*** role for **Everyone** group, select the check box for the **Everyone** group and click **Remove**. Because you removed the **Everyone** group, only the user ID called newUser is assigned the ***Readers*** role and can perform the tasks that are permitted to this Cognos role. You can assign other user accounts or groups to the ***Readers*** role.

When you log in as newUser, you are allowed to view reports for any report packages that are defined in Tivoli Common Reporting. You are not authorized to run reports nor to create or modify new reports for these report packages.

## Example 2: Assigning permissions to users or groups (1 of 2)

- In the Set Properties panel, **Permissions** tab of the Reporting Object, you can alter authorizations
  - Add the required user or group to the list of the authorized or available entities
  - Assign required permissions to the user or group
- If the Everyone group is not removed from Cognos roles, then you must perform either of these tasks:
  - Remove the permissions (select **Deny**) for all the Cognos roles that are not of your interest (keep the default permission settings for the System Administrators role)
  - Remove the unwanted Cognos roles from the list







Using user and group permission directly on Reporting Objects instead of using Cognos roles allows you to have a closer control over report package or report tasks, but of course using this approach can introduce maintenance complexity.

First of all, because the Everyone group has been assigned to a lot of Cognos roles and all the authenticated users belong to this group.

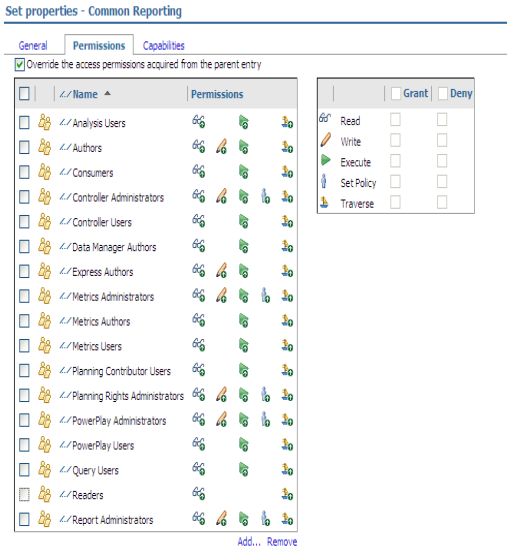
In order to avoid unwanted authorizations, you should remove the Everyone group from all the Cognos roles. Alternatively, you can keep it only for roles that are not used in the Reporting Objects that you want to use to authorize configuration for users or groups.

Suppose that you want only a specific user ID or group ID to view and run the reports included in a specific report package.

In this example, unless you are sure that Everyone group has been removed from the predefined Cognos roles, you should remove the permissions for all the predefined Cognos roles, in order to be sure that unwanted user accounts do not get authorization from being assigned to one of the existing Cognos roles.

## Example 2: Assigning permissions to users or groups (2 of 2)

- In the Set Properties panel, **Permissions** tab of the Reporting Object, you can alter authorizations
  - Add the required user or group to the list of the authorized or available entities
  - Assign required permissions to the user or group
- If the Everyone group is not removed from Cognos roles, then you must perform either of these tasks:
  - Remove the permissions (select **Deny**) for all the Cognos roles that are not of your interest (keep the default permission settings for the System Administrators role)
  - Remove the unwanted Cognos roles from the list







Alternatively, you can select and remove unwanted Cognos Roles from the list to obtain the same behavior.

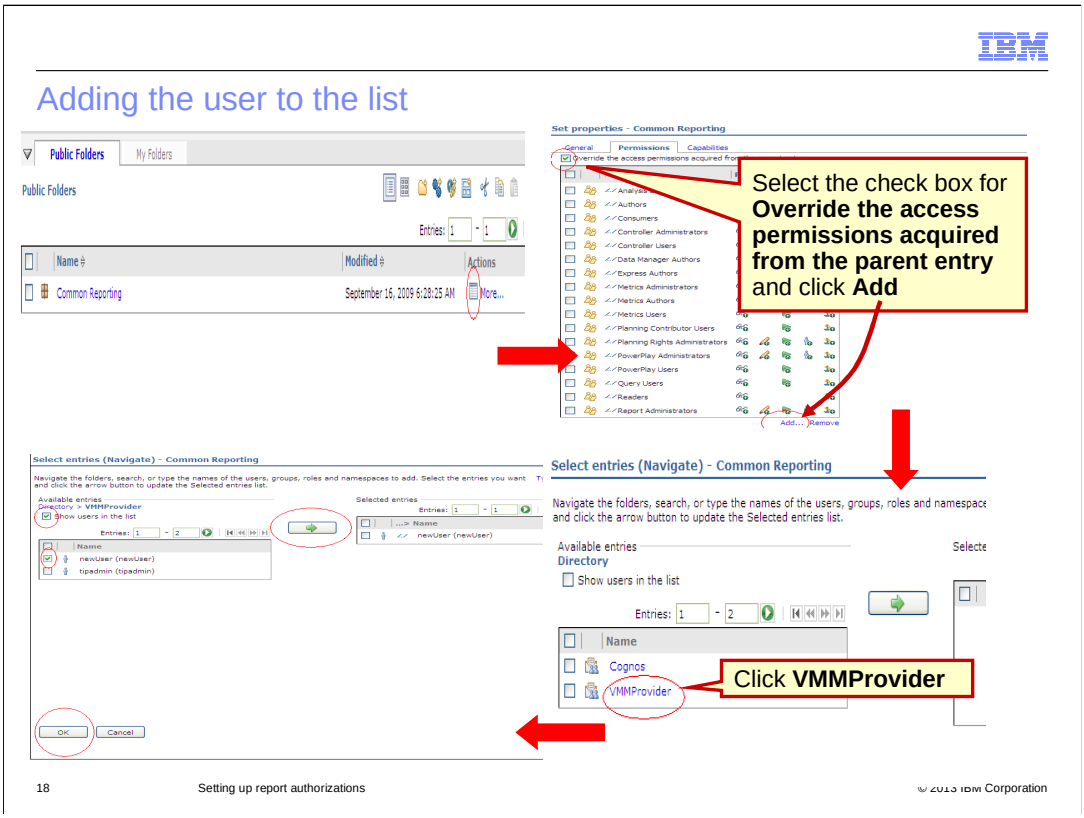
Then, you can add the user or group ID directly to the Reporting Object and assign it the wanted permissions.

The necessary tasks are listed:

Add the user ID to the list of available entities and assign to them the needed permissions. So in the example, if you have a group that is called reportUsers, you can assign it the View, Traverse, and Execute permissions.

For another group called reportEditors, you can instead add to the permissions the write permission. The write permission adds some capabilities to open and work with report editors like *Report Studio* or *Query Studio*.

After you add the required user or groups ID and assign the required permissions, you can deny the permissions for all of the Cognos Roles that you are not interested in. Those roles might be all except for the System Administrators role. To deny permissions, remove the role from the list.




These steps show how to authorize only a specific user to view and run reports in a report package.

See the upper left image. Select the check box for **Common Reporting package** and click the **Set Properties** icon.

When the Set Properties window opens, as shown in the upper right image, click the **Permissions** tab to list all of the Cognos roles and related permissions.

To change these settings, you need to enable the check box **Override the access permissions acquired from the parent entry**. To add new users or groups to the list, click **Add**.

See the lower right image. Like the previous example where you selected the user for a specific Cognos role, select the **VMMProvider security** namespace to display the list of available users and groups.

See the lower left image. Select the check box for **Show users in the list**.

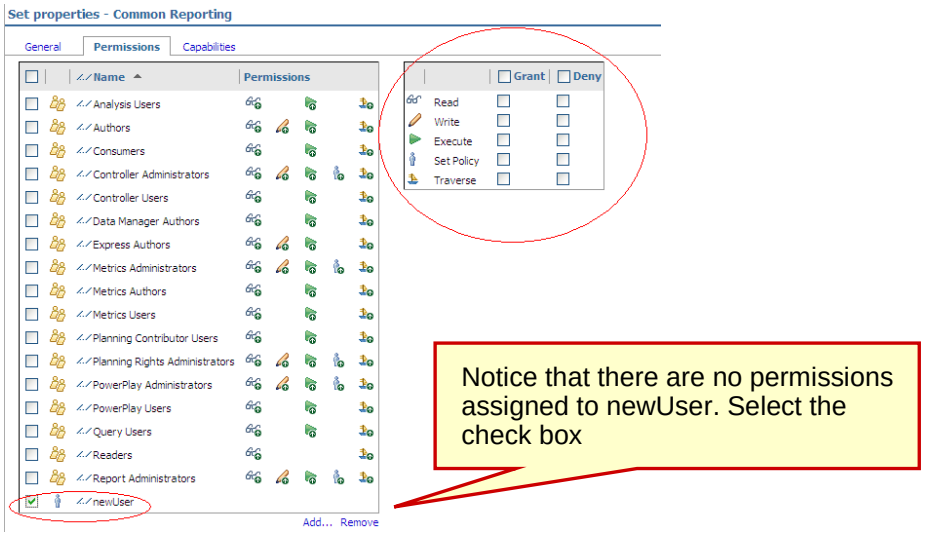
From the list, select the check box for any user ID you want to add.

Click the green arrow button to activate the selection.

To complete the operation, click **OK**.

The user ID displays in the list of entities so you can assign permissions.

## Granting permissions to the user (1 of 4)



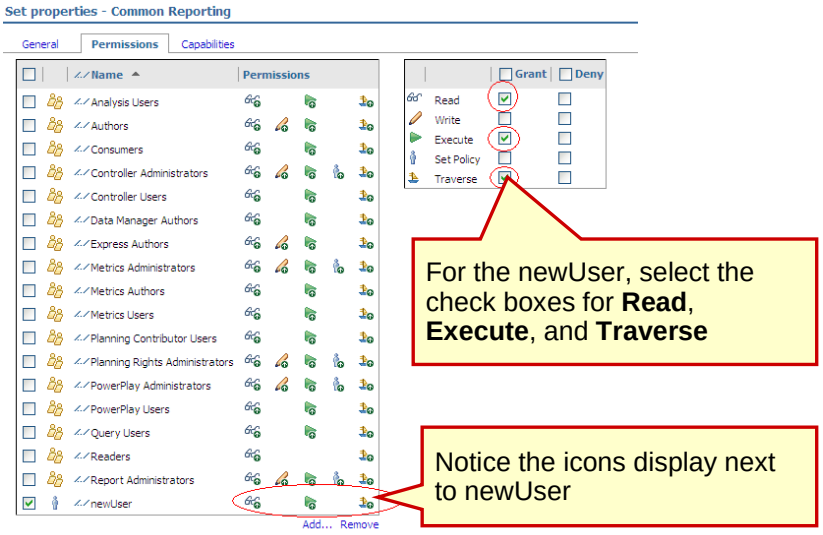




As you can see, the user ID is listed with Cognos roles and other predefined entities, but it has no permissions granted.

Select the user ID and then work on the Permission panel to grant the permissions you need for the user account.

## Granting permissions to the user (2 of 4)

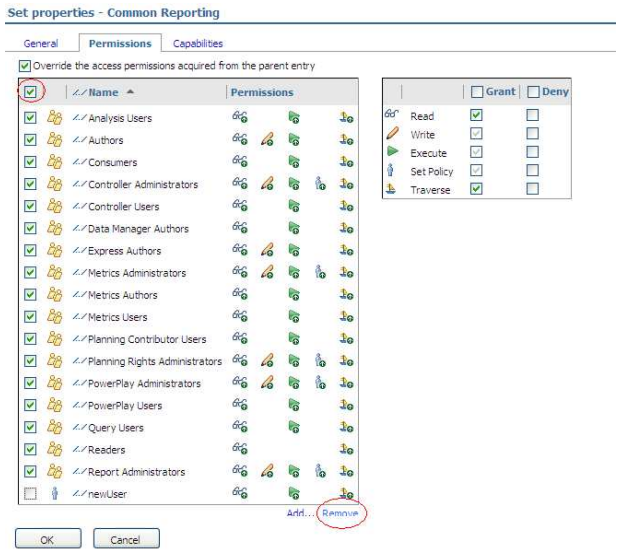






In this example select **Read**, **Execute**, and **Traverse** to enable the user to access the report package, read, and run the reports. As you make the selections, notice the icons display next to the user ID newUser.

## Granting permissions to the user (3 of 4)

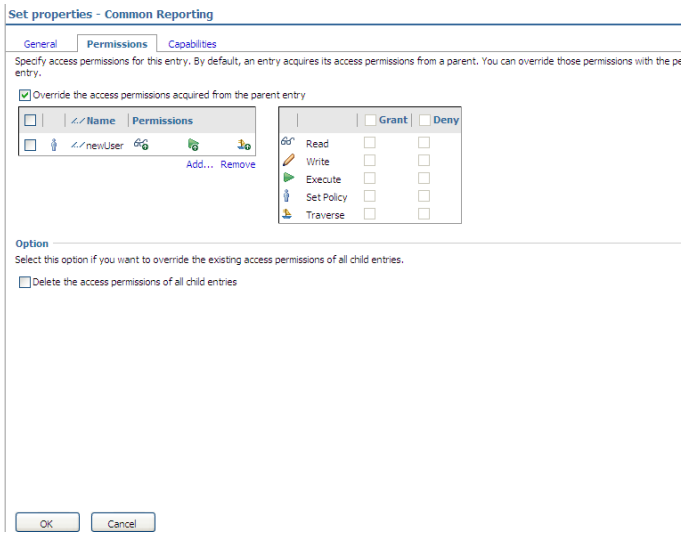






Now, if you want to deny all the other Cognos roles from accessing this reporting object, in your case the report package, you need to select all the Cognos roles and click **Remove**.

## Granting permissions to the user (4 of 4)



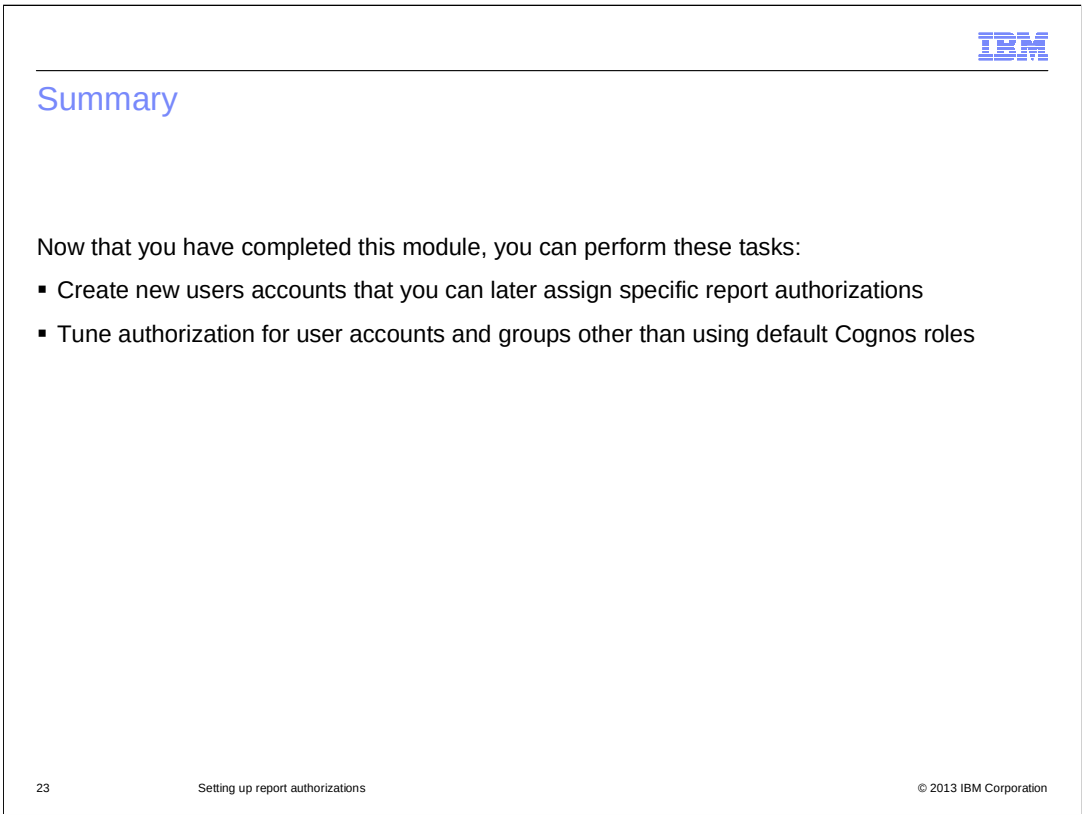




You can add another user that also has Write permissions.

In a real context, it is easier to use groups instead of users to assign permissions.

Depending on their specific tasks, you can select which user accounts must be included in which groups and grant the group permissions instead of the users. You use similar steps to the ones already described.




Now that you completed this module, you can perform two tasks.

1. You can create new users accounts that you can later assign specific report authorizations. You also can create a group with similar steps.

2. You can tune authorization for user accounts and groups other than using default Cognos roles.

## Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_setting_up_report_authorizations_in_tcr211.ppt

This module is also available in PDF format at: ../setting_up_report_authorizations_in_tcr211.pdf




You can help improve the quality of IBM Education Assistant content by providing feedback.

## Trademarks, disclaimer, and copyright information