User Management in Intellicus

Intellicus Web-based Reporting Suite **Version 4.5**

Enterprise

Professional

Smart Developer

Smart Viewer

intellicus Enterprise Reporting

info@intellicus.com
www.intellicus.com

Dated: - May 2009.

Acknowledgements

Intellicus acknowledges using of third-party libraries to extend support to the functionalities that they provide.

For details, visit: http://www.intellicus.com/acknowledgements.htm .

Contents

User Management

An Intellicus user belongs to an Organization. Organization logically groups a set of users. For ease of administration, you can create a number of roles, and make users member of respective groups. This chapter covers about:

- Organization
- Users, Roles and access rights
- User Mapping

On Portal, to get user management related pages, click Administration > Manage Users. When installed for the first time, Intellicus has *Intellica* as the default organization.

Organization

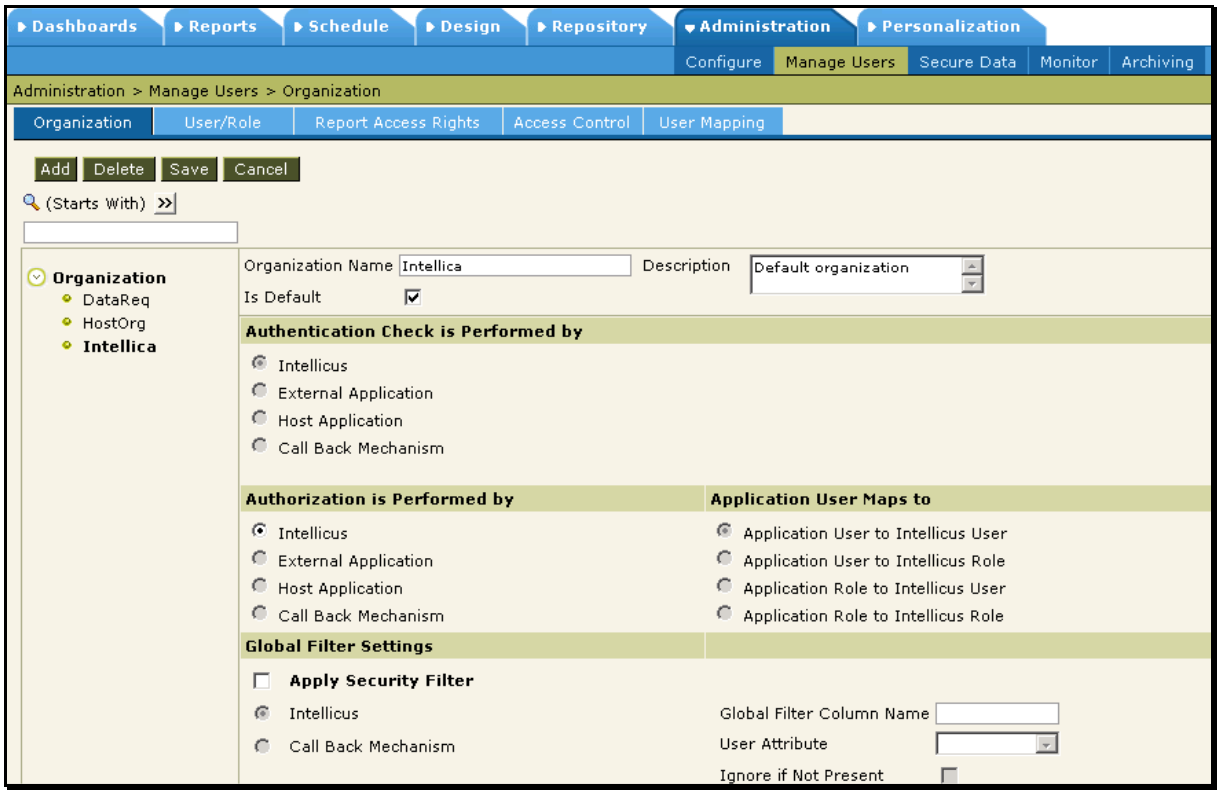

Figure 1: Organization page

Filtering list of organizations

List can be filtered by:

- Starting character (Starts with)
- Characters that appear anywhere in the name (Contains)

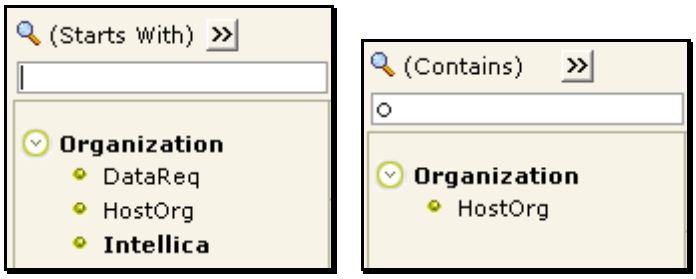

Figure 2: Filtering the list of organizations

1. On **Organizations** page, check the option on right of .
2. To get the right option there, click and select *Start with* or *Contains*.
3. Specify character(s) in the textbox.

The list will be filtered (not case sensitive) as per the criteria.

Setting up a new organization

To set up a new organization,

1. Click Administration > Manage Users > Organization.
2. Click **Add** button. The page is cleared and name appears in **Organization Name** box.
3. In **Organization Name** box, specify a new organization name to uniquely identify this organization.
4. Select **Default Organization** check box if this is the default organization.
5. Specify other details and click **Save** button to save the work.

Following information is provided as part of Organization setup:

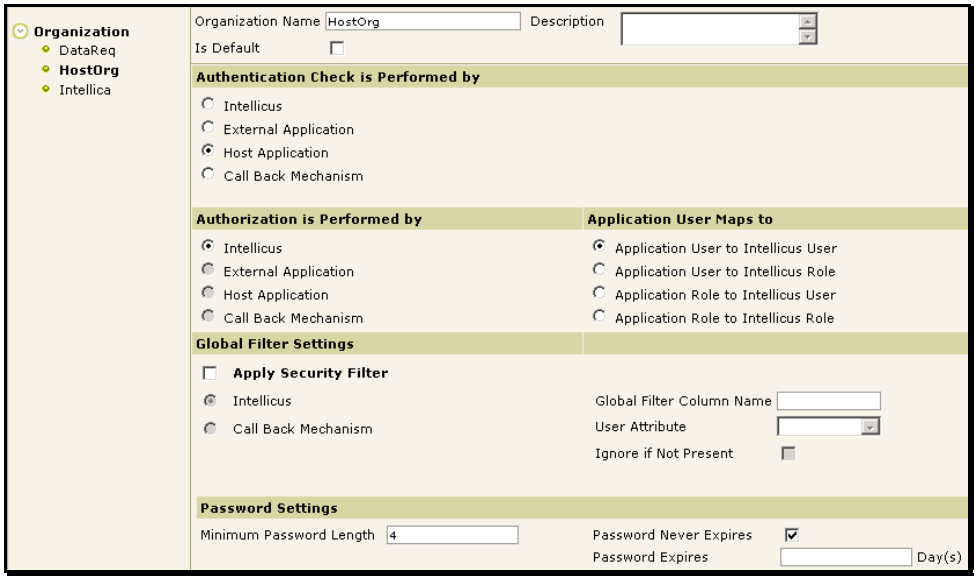

Figure 3: Details about organization

Organization Name: A name to uniquely identify this organization setup. Maximum length of organization name should be 30 characters or less.

Description: A description providing information about the organization.

Is Default: Select this check box, if this organization is the default organization. If this check box is selected, this organization will appear as selected while logging into Intellicus.

Authentication Check is performed by

When Intellicus is deployed as integrated with another application, you need to specify which application will authenticate the users trying to access Intellicus functionalities. Select any of the options based on your integration needs.

- **Intellicus:** Intellicus will take care of user authentication.
- **External Application:** Specify Type, Server and Protocol if the external application will take care of authentication.
- **Host Application:** Select this if the Host Application will take care of authentication.
- **Call Back Mechanism:** Select this if authentication is through Call Back Mechanism. Select the appropriate option among Local, Socket and RMI. Specify Server and Port. Select the appropriate option among Java Class, Native Library and COM DLL. Specify value of Implementer.

Authorization is performed by

When Intellicus is deployed as integrated with another application, you need to specify which application will check whether the user trying to access Intellicus functionalities is authorized to use that functionality. Select any of the options based on your integration needs.

- **Intellicus:** This appears as selected. Select this when Intellicus will perform Authorization. Click **Access Rights** link to open **Report Access Rights** page having a list of users of selected organization.
- **External Application:** Select this when External Application will perform authorization.
- **Host Application:** Select this when host application will perform authorization.
- **Call Back Mechanism:** Select this when call back mechanism will be used for authorization.

Application User Maps to

Select the most appropriate option among following:

- Application user to Intellicus user
- Application user to Intellicus role
- Application role to Intellicus user
- Application role to Intellicus role

Click **Perform Mapping** link to open **User Mapping** page with selected organization.

Global Filter Settings

Feature of globally filtering data is available in Intellicus. To apply security filter, select (check) the check box **Apply Security Filter**.

If Intellicus should apply the filter

Select **Intellicus** option button.

- **Global Filter Column Name:** This is the requirement from database side. All filterable tables must contain a common named column for applying automatic global filtering. Specify that column in "Global filter column name" box.
- **User Attribute:** Select the user info attribute that should be used for matching the secured records for a logged in user.
- **Ignore if Not Present:** The common column used as filter can be optional for master tables that do not require filtering. If this is the case, select (check) the check box.

If filter will be applied by Call back Mechanism

Select **Call Back Mechanism** button. Specify respective values based on requirements of application taking care of call back.

Password Settings

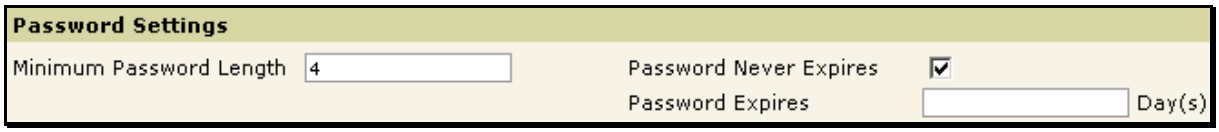

Figure 4: User Password related settings

- **Minimum Password Length:** Specify the minimum number of characters (a-z. A-Z, 1-0) that a password should have. A password specified that is having less number of characters than specified here would not be accepted.
- **Password Never Expires:** Select this check box in case you do not want the password to expire.
- **Password Expires:** Specify the number of days after which the password will expire.

Managing Users / Roles

When security is enabled in Intellicus, you need to log into the system using a user name / password combination.

The activities you can do in Intellicus depends on the access rights given to you.

As an administrator, you have multiple users to whom the same access rights are going to be given, user may prefer to setup role, give the role adequate access rights and add the role to all the users. This way, all the access rights that a role is having are made available to the user too.

User related activities are carried out on **User/Role** tab. Click Administration > Manage Users > User/Role.

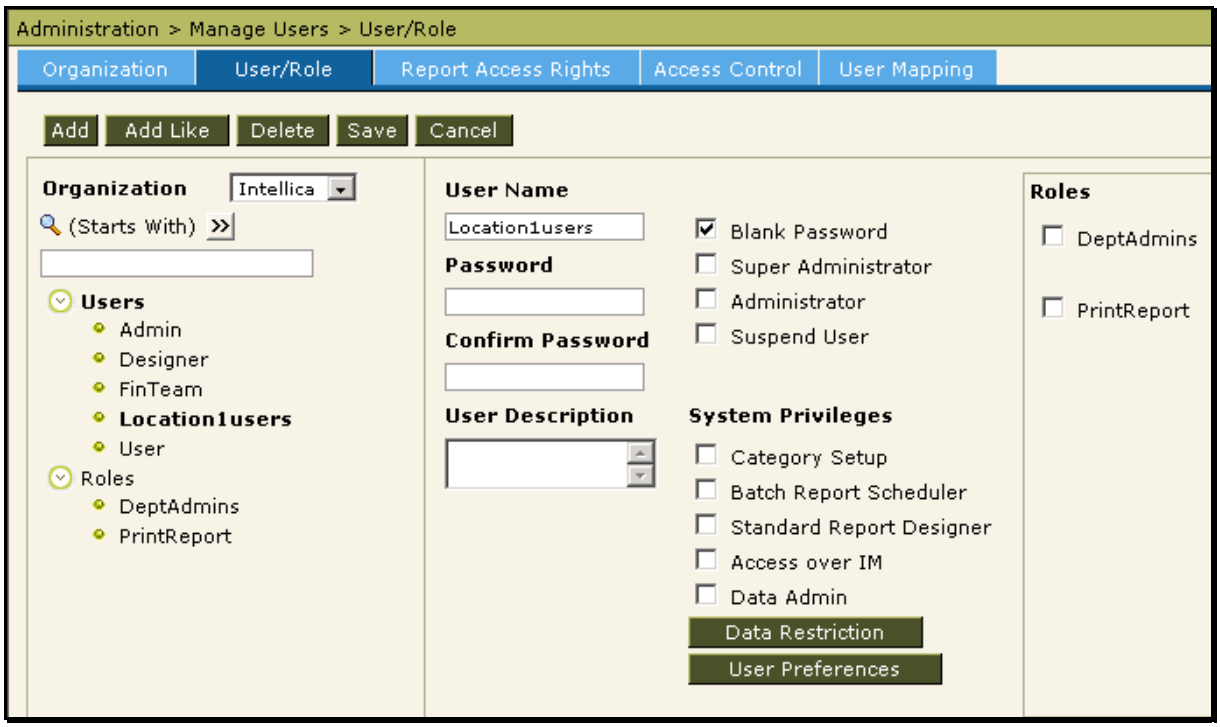

Figure 5: User / Role page of Manage Users tab

Before doing any activity, you need to select the Organization.

The User/Role tab

The User / Role tab, on the left side contains a tree having one branch each for Users and Roles. The branch of User and that of Role has nodes of users and roles setup in Intellicus. Clicking a user node or role node displays related options on the right side of the tree. While a user node or branch is selected, Role box also appears on the right side of the page listing roles setup in Intellicus.

To filter list of Users and Roles

List can be filtered by:

- Starting character (Starts with)
- Characters that appear anywhere in the name (Contains)

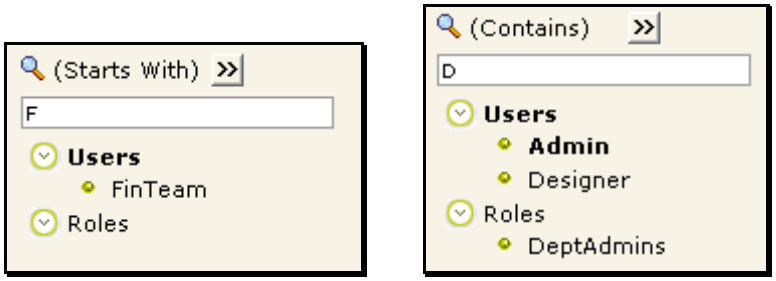

Figure 6: Filtering list of Users and Roles

6. On **User / Role** page, check the option on right of .
7. To get the right option there, click and select *Start with* or *Contains*.
8. Specify character(s) in the textbox.

The list will be filtered (not case sensitive) as per the criteria.

Server Search

If icon appears on right of the text box, it means the organization has large number of user / role entries and some of them are not displayed on this page. To get fewer entries, you need to narrow down the search by providing more characters in search string and click button. You can also press enter key to start the search.

Role related activities

You can carry out following role related activities:

- Create a new role
- Change settings for a role
- Delete a role
- Suspend a role

Setting up a new Role

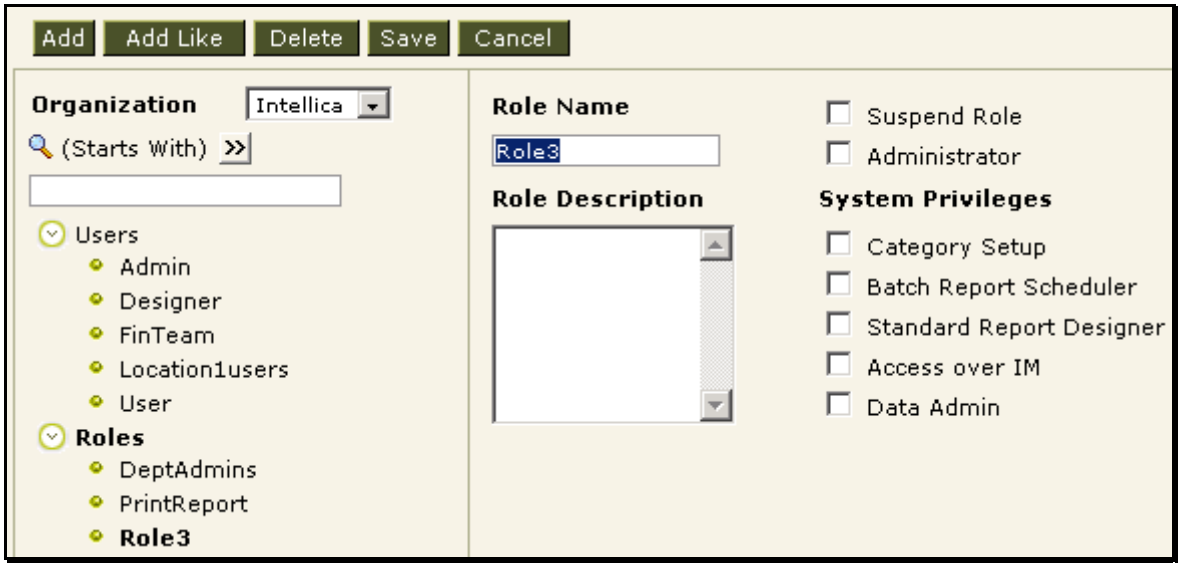

Figure 7: Creating a role

To setup a new role,

1. Click **Roles** Branch. The information on the page changes accordingly.
2. Click **Add** button. A new role name appears in the **Role Name** entry box and check boxes are cleared.
3. In **Role Name** entry box, specify a unique name to identify the role.
4. If the role is to be given Administrator rights, select the check box **Administrator** check box.
5. Select relevant checkboxes under **System Privileges**.
6. Click **Save** button to save the work.

Here is the description of what will happen when check-boxes are selected:

- **Suspend Role:** Privileges that users enjoy through this role will be suspended. However, they will continue to enjoy privileges they have got through other roles.
- **Administrator:** The role will get administrators access privileges on that organization.

- **Category Setup:** The users, for whom this role is added, can create new categories and delete categories for everyone to use (public categories).
- **Batch Report Scheduler:** The users, for whom this role is added, can work with scheduler related activities.

> **Note:** Batch Report Scheduler is not available in Smart Developer and Smart Viewer edition.

- **Standard Report Designer:** The users who are members of this role can design reports using Desktop studio / web studio.
- **Access over IM:** The user can access Intellicus functionalities over the Instant Messenger.
- **Data Admin:** Users who are members of this role will be able to work with **Query** page, **Parameters** page and **Parameter Value Groups** page.

To get the new role to have the settings similar to any of the existing roles,

1. Click the role that you want to continue for the new role being setup.
2. Click **Add Like** button.
3. Click **Save** Button.

Changing settings for a role

Role once setup may require changes over a period of time. It is possible to change all the setting for a role. However, name of a role once setup, can't be changed.

> **Note**: Changes made in a role will affect all the members of the role.

To change settings for a role,

1. Expand the branch and click the role for which you want to change the settings.
2. Make changes in the settings where required.
3. Click **Save** button to make the changes permanent.

Deleting a role

User may wish to remove a role once it is not applicable to any user.

1. Expand the branch and click the role that is to be deleted.
2. Click **Delete** button. A confirm delete dialog box appears.
3. Click **Yes** button to go ahead with the deletion. Click **Save** button to make the changes permanent.

Note: When a role is deleted, the privileges that the users were enjoying due to that role, will be revoked. For example, if a user Villy was a Administrator because of a role assigned to Villy, now, that the role is deleted, Villy will no longer have Administrative access privileges.

Suspending a role

To suspend a role,

1. Expand the branch and click the role that needs to be suspended.
2. Select the **Suspend Role** check-box.
3. Click **Save** button to make the changes permanent.

User related activities

You can carry out following user related activities:

- Create a user
- Change a user-settings
- Delete a user

Creating a New user

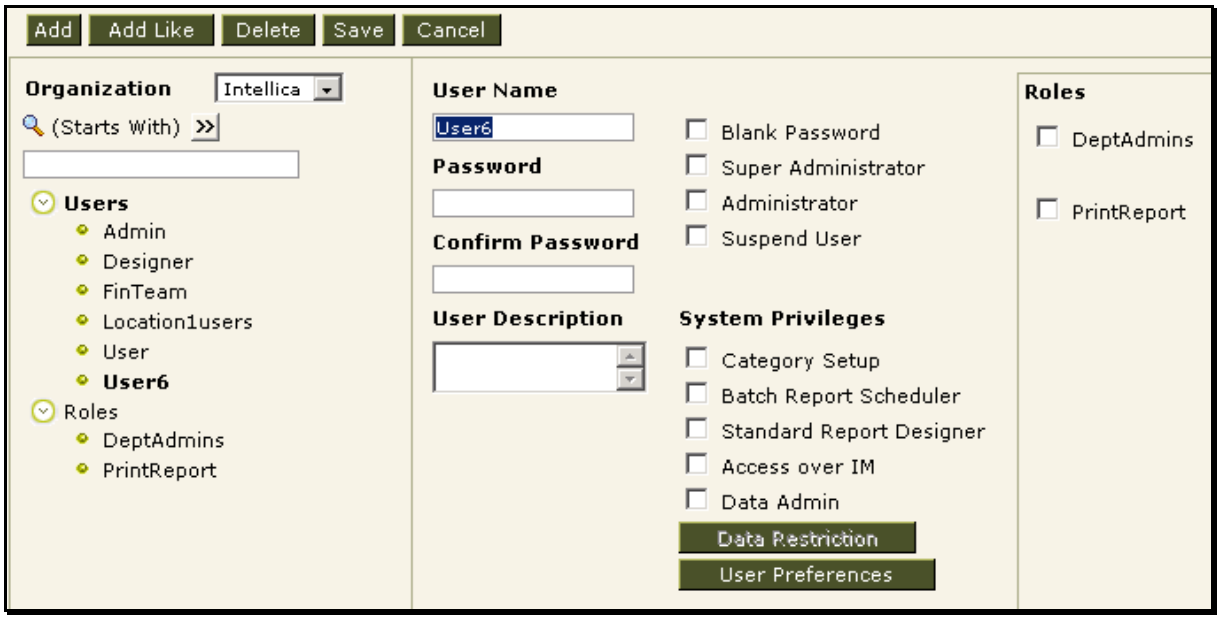

Figure 8: Creating a new user

To create a new user,

1. Click **Users** Branch. Contents on the page changes accordingly.
2. Click **Add** button. A new User name appears in **User Name** entry box. Also, the entry boxes on the right side, gets cleared.
3. In **User Name** entry box, specify a unique user name.
4. If you do not want the user being created to specify password while logging in, select the check box **Blank Password**. If you keep **Blank Password** check-box clear, you need to specify a password in **Password** entry box and then the same password in **Confirm Password** entry box.
5. Select the check boxes as per requirements.
6. In case any of the pre-set roles are to be added for the user, select the check boxes under **Role** accordingly.
7. Click **Save** button to save the work.

The information is saved and a message "Information saved successfully" appears in the header.

If you want the new user to have the settings similar to any of the existing users,

1. Click the user whose settings you want to continue for the new user being setup.
2. Click **Add Like** button.
3. Click **Save** Button.

Here is the description of checkboxes:

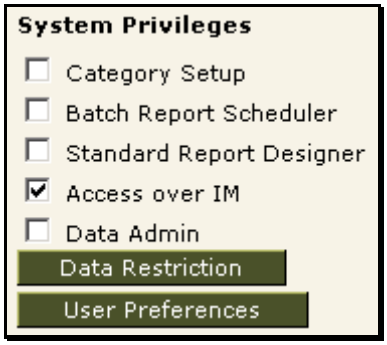

Figure 9: Check boxes to be set while setting up a user

- **Suspend User:** The user will be suspended. User will no longer be able to use Intellicus.
- **Super Administrator:** The user will be given super administrator rights. Super Administrator user gets all the system privileges.
- **Administrator:** The user will be given administrator rights. An Administrator gets all system privileges except *Approve reports* and can work on users of his/her own organization.
- **Category Setup:** The user will be allowed to work with category setup.
- **Batch Report Scheduler:** The user will be allowed to work with scheduler related activities.

> **Note:** Batch Report Scheduler is not available in Smart Developer and Smart Viewer edition.

- **Standard Report Designer:** The user will be allowed to work with designing of reports using Desktop studio / web studio.
- **Access over IM:** The user can access Intellicus functionalities over the Instant Messenger.
- **Data Admin:** The user will be allowed to work with **Query** page, **Parameters** page and **Parameter Value Groups** page.
- **Data Restriction:** Click this button to setup data restriction details and apply it on the user. By doing this, you can provide your users with a limited set of values to choose from while running a report.

Note: When you click **Data Restriction** button, Data Restriction page opens up. Parameter values and parameter value groups are selected on this page. For instructions on how to use this page, refer to **PersonalizingIntellicus.pdf.**

- **User Preferences:** User Preferences: Click this button to setup User Preferences on behalf of the user being created.

Note: When you click **User Preferences** button, **User Preferences** page opens up. Use this page to set **Portal Preferences** and **Default Connection** for the selected user. For instructions on how to use this page, refer to **PersonalizingIntellicus.pdf.**

Changing settings for a user

It is possible to make changes in user privileges and rights.

Note: A user name can't be changed.

To make changes in user settings,

1. If branch of users is not expanded, click to expand it. Click the user for which you want to change the settings.
2. Make changes in the settings where required.
3. Click **Save** button to make the changes permanent.

Note: The changes are made applicable immediately after clicking the **Save** button.

Deleting a user

To delete a user detail from Intellicus,

1. If the branch of Users is not expanded, click to expand it. Click the User that you want to remove.
2. Click **Delete** button. A confirm delete dialog box appears.
3. Click **Yes** button to go ahead with the deletion.
4. Click **Save** button to make the changes permanent.

Suspending a user

To suspend a user,

1. If branch of **Users** is not expanded, click to expand it. Click the user that you want to suspend.
2. Select the **Suspend User** checkbox.

3. Click **Save** button to make the changes permanent.

Managing Report Access Rights

Users need to have appropriate access rights to work with a report (design, view, schedule, etc). Access rights are given to users as well as roles. Access rights, when given to a role, all the users having that role will automatically inherit those access rights.

User related activities are carried out on Report Access Rights tab. Click Administration > Manage Users > Report Access Rights.

Access Rights tab has three sets of information. The left part contains roles and users organized in a tree form. The middle part includes an area to display and select categories (upper part) and reports (lower part). The part on the right side contains options for different level of access privileges. This will appear differently for categories and reports.

If similar access is to be given for all of the reports under a category, we recommend to set access at category level. This way, all the reports under that category will have the same access privileges for that user or role. In other case, setup access at report level.

To filter list of Users and Roles

List can be filtered by:

- Starting character (Starts with)
- Characters that appear anywhere in the name (Contains)

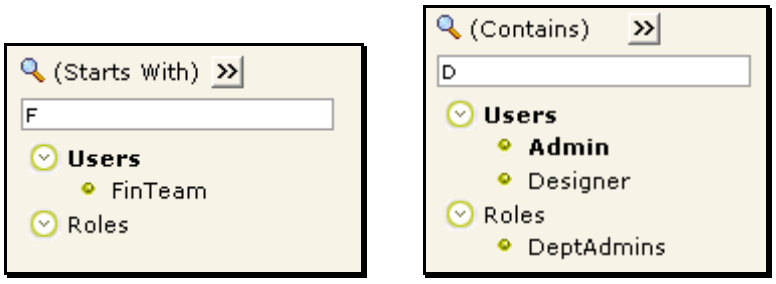

Figure 10: Filtering list of Users and Roles

1. Check the option on right of 🔍 .
2. To get the right option there, click » and select *Start with* or *Contains*.
3. Specify character(s) in the textbox.

The list will be filtered (not case sensitive) as per the criteria.

Server Search

If icon appears on right of the text box, it means the organization has large number of user / role entries and some of them are not displayed on this page. To get fewer entries, you need to narrow down the search by providing more characters in search string and click button. You can also press enter key to start the search.

Setting Report Access Rights at Category level

When you set report access rights at category level, user gets that rights for all the reports within selected category.

The sequence of the steps is the same for a user as well as a role.

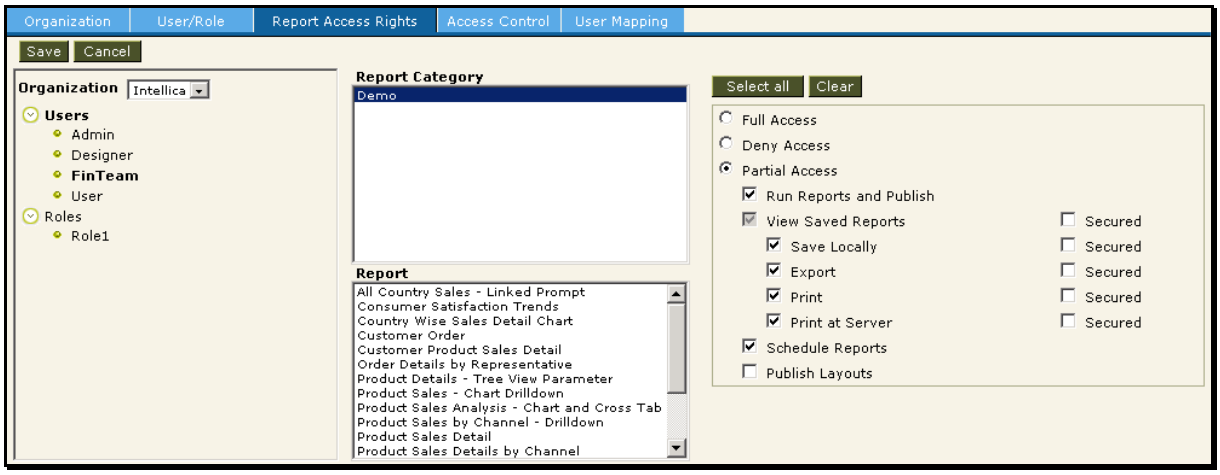

Figure 11: Setting report access rights for category

To set access rights for a category,

1. Click **Role** or **User** branch name and select a user / role respectively.
2. Select the category from **Report Category** List. To do this, click the category name for which report access rights are being set.
3. From the options available on the right part of the page, select appropriate options. The detail of options is given after this sequence of steps.
4. Click **Save** button to save the changes made.

The Detail of Options

- **Full Access:** All access rights on all the reports placed under the selected category.
- **Deny Access:** No access right on any of the reports under the selected category.

- **Partial Access:** Selective access rights for all the reports under the selected category. The detail is given below:

The Detail of Check box Options

- **Run Reports and Publish:** To run and publish reports. When a report is published, it is saved and can be viewed afterwards.
- **View Saved Reports:** To run (view) the published reports.
  - **Save Locally:** To view a published report and save output of the report locally.
  - **Export:** To view a published report and can export the report to available export options.
  - **Print:** To view a published report and can print the output of the report.
  - **Print at Server:** To view a published report and can print the report on the machine running report server.
  - **Secured:** To carryout view operation in Jvista Viewer.
- **Schedule Report:** To schedule a report.
- **Publish Layouts:** To deploy report (publish layout) through **Deploy Repository Bundle** and **Manage Folders and Reports** pages.

Setting Report Access Rights at Reports level

The sequence of steps is the same for a user as well as a role.

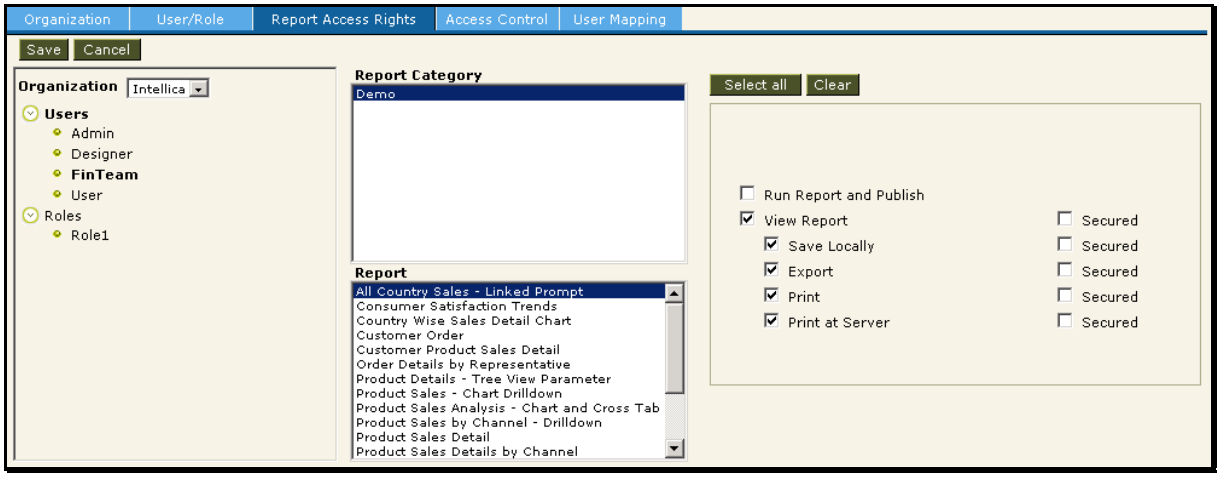

Figure 12: Access rights for reports

To set access rights for a report under selected category,

1. Click **Role** or **User** branch name and select a user / role respectively.
2. From **Report Category** List, select the category under which the report is deployed. To do this, click the category users are looking for. All the reports under that category are listed in **Report** List.
3. From the **Report** List, click the report for which access rights are being setup.
4. From the options available on the right part of the page, select appropriate options.
5. Click **Save** button to save the changes.

<u>Use of **Select All** and **Clear** button</u>

- Click **Select All** button to select all the check boxes.
- Click **Clear** button to clear all the check boxes.

The Detail of Check box Options

- **Run Reports and Publish:** To run and publish reports. When a report is published, it is saved and can be viewed afterwards.
- **View Reports:** To run (view) the published reports.
  - **Save Locally:** To view a published report and save output of the report locally.

- **Export:** To view a published report and can export the report to available export options.
- **Print:** To view a published report and can print the output of the report.
- **Print at Server:** To view a published report and can print the report on the machine running report server.
- **Secured:** To view operation in Jvista Viewer.

Access Control

Various objects within Intellicus are available only to the users who are granted access rights to respective object. Users are able to view only the objects for which they were granted the rights.

To get Access Rights tab, click Administration > Manage Users > Access Control tab.

Use this page to manage access rights to users on any of the following:

- Dashboard
- Query Objects
- Parameter Objects
- Database connections

Only public items are listed here.

If you are an administrator, you will be able to set access rights of users of your organization. You will be able to give access rights of the items that users of your organization have created.

If you are a super administrator, you will be able to set access rights of all the users. You will be able to give access rights of the items created by users of any organization.

Server Search

If icon appears on right of the text box, it means the organization has large number of user / role entries and some of them are not displayed on this page. To get fewer entries, you need to narrow down the search by providing more characters in search string and click button. You can also press enter key to start the search.

To grant rights

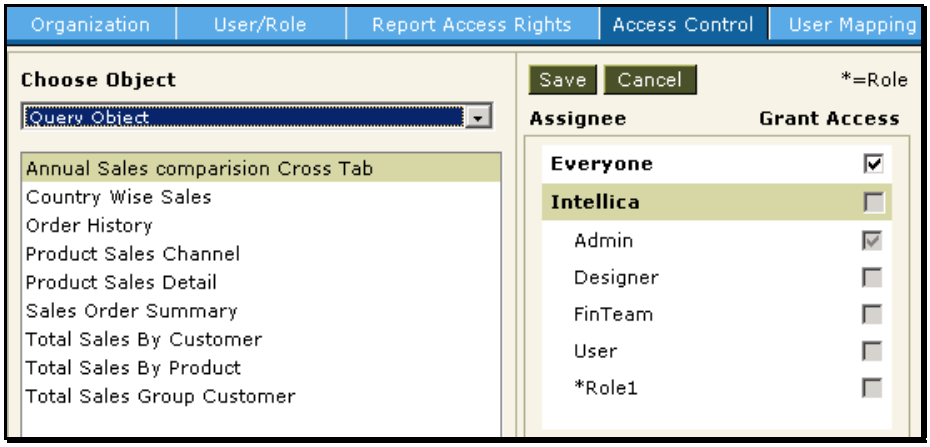

Figure 13: Providing access on objects

1. Select an object type from **Choose Object** list. List of objects will appear in the box below.
2. Select an object type. From **Choose Assignee**, check the checkboxes for the users / roles / organization(s) to whom access is to be granted.
3. Click **Save** button to save the work.

To withdraw rights

1. Select an object type from **Choose Object** list. List of objects will appear in the box below.
2. Select an object. From **Choose Assignee**, clear the checkboxes for the users / roles / organization(s) from whom access is to be withdrawn.
3. Click **Save** button to save the work.

Note: User needs to save the changes made for the selected object before switching over to another object or another object type.

User Mappings

When the external application takes care of authentication, users of the external application are mapped with roles/users setup in Intellicus. This way, the users of external applications are able to enjoy the privileges given to the Intellicus-roles / users they are mapped to.

User Mappings related activities are carried out on **User Mappings** tab. Click Administration > Manage Users > User Mapping.

To work with mappings setup for an organization, you need to select that organization from **Organization** selection box.

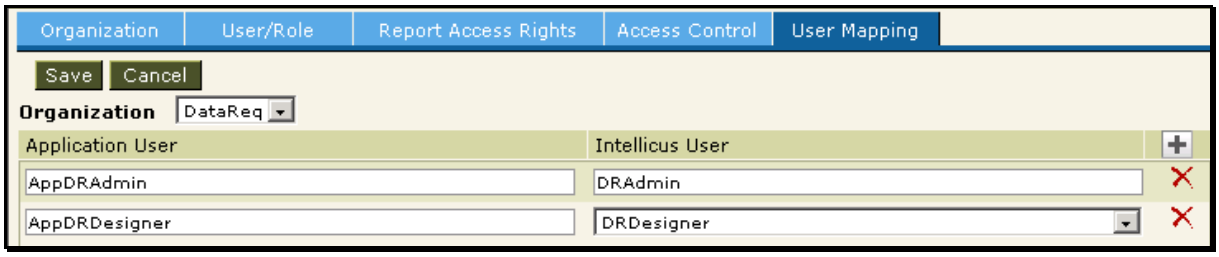

Figure 14: Mapping of organizational users with organization set in Intellicus

To add a mapping

1. Click button. A row for mapping appears.
2. In **Application User** or (or Application Role) entry box, specify the user-name used by the host application.
3. From **Intellicus User** (or Intellicus Role) selection box in that row, select the role that you want to map to the selected user.
4. Click **Save** button.

Note: If you are mapping Application user with Intellicus user, a drop down box having all the users setup for that organization in Intellicus will appear for you to select from.

The mapping information is saved.

To modify a mapping

Edit the entry of Application User / Role, Intellicus User / Role depending

To modify a mapping

- Edit the entry of Application User / Role.
- Click and select Intellicus User / Role from the drop down.

Click **Save** button to save the changes.

To delete a mapping

1. Click ✕ button of respective row. A confirm dialog box appears.
2. Click **OK** to go ahead with deletion.