User Management in Intellicus

Version: 18.1

intellicus

Dated: September 2018

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

1 User Management

When Intellicus runs in secured mode, it authenticates and authorizes every user trying to access Intellicus.

User belongs to an organization. The functionalities available to a user depend on the organization to which the user belongs, and access rights granted to the user.

Intellicus has a pre-existing organization: Intellica. If Intellicus is deployed as a stand-alone application, you may choose to create more users in Intellica organization instead of creating a new organization. (Users are created on User/Role page).

If Intellicus is integrated with another application, users may access Intellicus functionalities from within the host application. In this case, you need to create an organization in Intellicus (for the users of host application) and create users in it. Users of host application will be mapped with users of Intellicus' organization.

The following topics are discussed under User Management:

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

Organization

You need to have administrator privileges to be able to add, modify or delete organizations in Intellicus. To navigate to the Organization page, click Navigate > Administration > Manage Users > Organization.

Intellicus has an organization already created: Intellica. Use Organization page to create more organizations, which is more likely in case Intellicus will be integrated with another application.

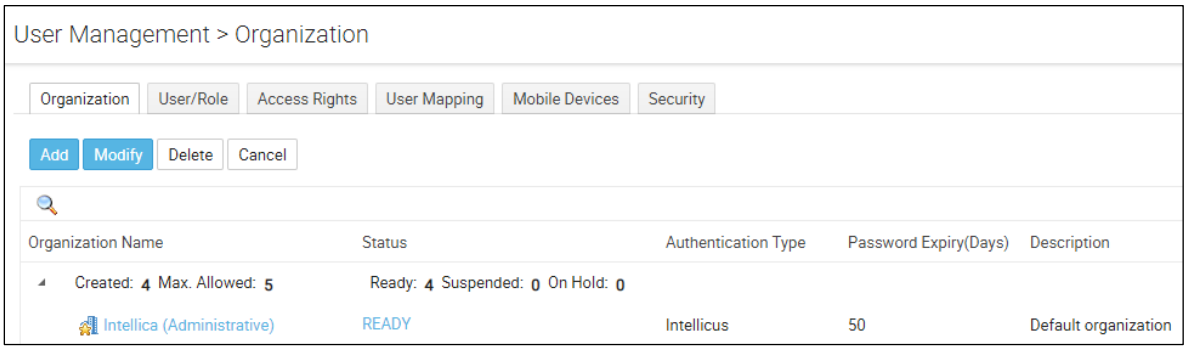

Figure 1: Organization page

Setting up a new organization

To start adding an organization, click **Add** button. The '**New Organization**' screen opens to specify details for the organization being created.

General

Specify a unique **Organization Name**. When user logs in to Intellicus, this name will appear in Organization dropdown box on landing page (login page).

Specify **Description**. This is the field used to specify additional information pertaining to the organization. For example, "This is a default organization."

Check **Is Default** checkbox, if most of the Intellicus users belong to this organization. At the time of login, users will be required to specify Organization along with user name. Default organization's name appears selected on Organization box on landing page. User doesn't have to specifically select the organization.

Check **Suspend** checkbox to temporarily suspend an organization; so users can't use this at the time of login.

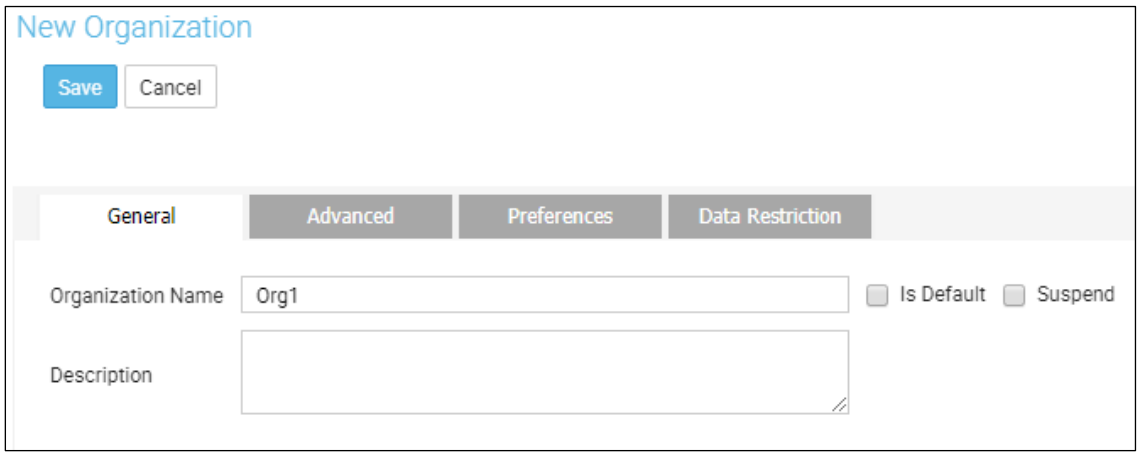

Figure 2: New Organization – General tab

Advanced

Authentication Check is performed by:

Select **Intellicus** if Intellicus should authenticate the user of this organization. User name and password will be stored in Intellicus repository. When a user logs in, Intellicus will verify the credentials before allowing the access. This is selected when Intellicus is deployed as stand-alone.

Select **External Application** if users trying to access Intellicus will be authenticated by an external application. This is generally the case when Intellicus is integrated in an application that uses another application to authenticate its users. Select **Type** and provide **Server IP and Port** of machine where application responsible for authentication is available. **User DN** of the user is required to authenticate to the external source. In this case, you need to map application users with Intellicus users. The supported types in External Authentication are Windows NT and LDAP.

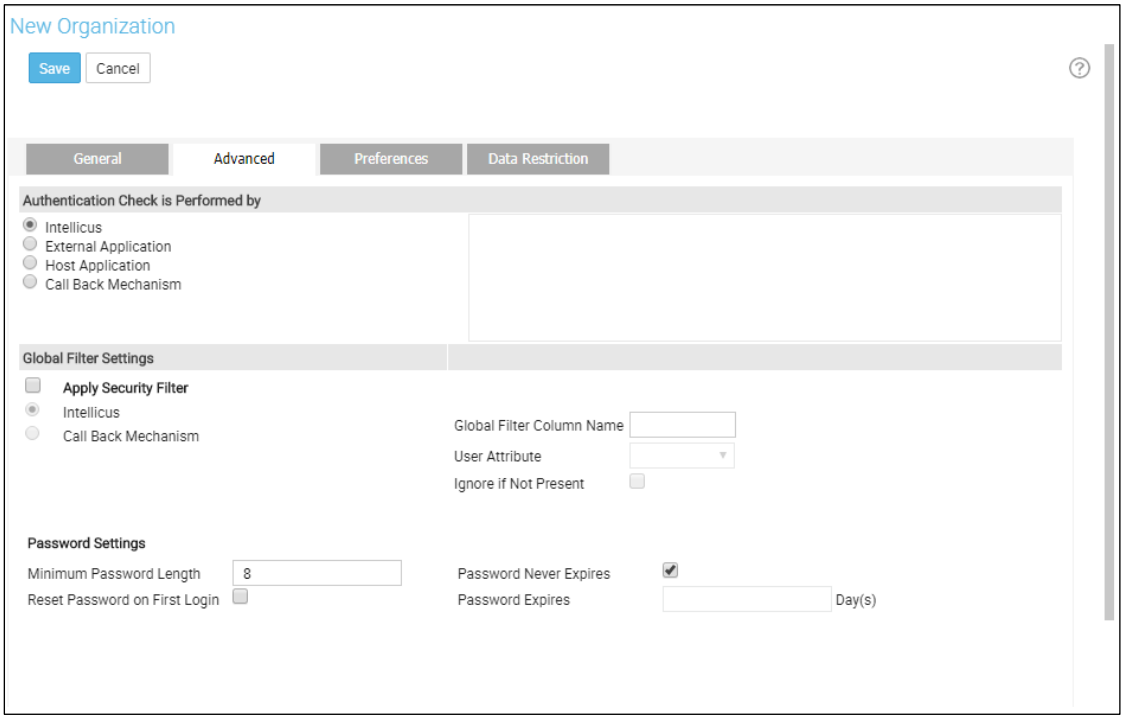

Figure 3: New Organization – Advanced tab

Select **Host Application** if Intellicus is integrated in an application and that will also take care of authenticating the user trying to access Intellicus. In this case, you need to map application users with Intellicus users.

Select **Call Back Mechanism** when Intellicus is integrated in an application and Intellicus should call host application's code to perform the authentication check. In this case, a function is called along with user credentials as arguments. This function carries out authentication and returns the result.

For your authentication code, the selected call method is **Local.** Specify **Server IP** and the **Port** of call back server. Under the **Java Class** Implementer, specify implementer class name that Intellicus should call.

Global Filter Settings

Intellicus' Global Filters feature allows you to set fields based on which you can filter every report related query. This is to make sure that the users have access to desired information only.

To apply security filter, check **Apply Security Filter** checkbox.

If Intellicus should apply the filter, select the **Intellicus** option.

- **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 this box.
- **User Attribute:** Select the user attribute that should be used for matching the secured records for a logged in user.

- **Ignore if Not Present:** Check this checkbox to ignore filtering if the global filter column is not found in the database. When kept unchecked and if global filter column is not found, Intellicus will generate an exception.

If filter will be applied by Call Back Mechanism

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

Password Settings

Make password related settings here.

To set a minimum password length, specify the number of characters that a password must have, in **Minimum Password Length** box.

When user is created in Intellicus, you need to provide a password during user creation. Check **Reset Password on First Login** to force user to change the password on first logon.

It is a good practice to change passwords at regular interval. In **Password Expires,** specify the number of days after which the password should expire. If you don't want to force password change, check **Password Never Expires** checkbox.

Preferences

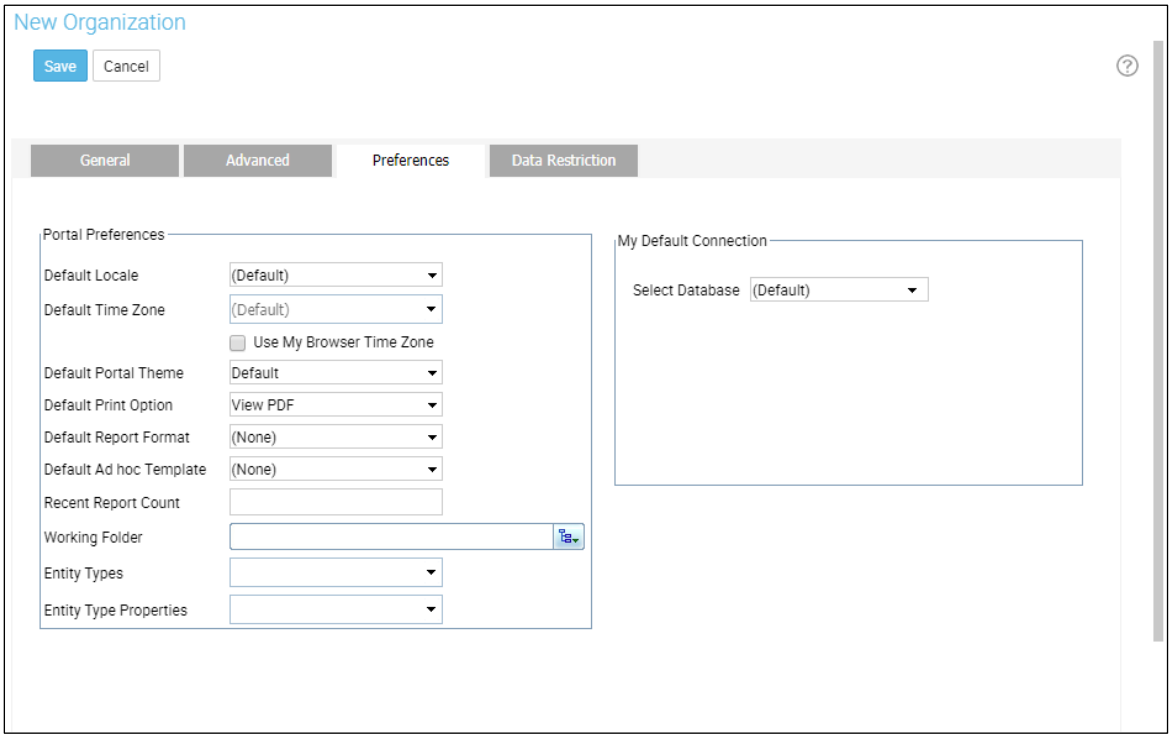

Figure 4: New organization – Preferences tab

You can set following default portal preferences for the users of the selected organization:

Locale governs items like portal language and date format. In **Default Locale**, select the locale that should be applied when users of this organization log into Intellicus.

Time Zone is applicable when application users are spread across multiple time zones and wish to get report output as per their own time zone. In **Default Time Zone**, select the time zone from where your users will access the application. Before starting the report generation, the application will convert date / time field in the time zone selected here. To use the machine's time zone as default time zone, check **Use My Browser Time Zone** checkbox.

Note: In Intellicus, locale and time zone specified in User Preferences takes priority over the ones set at Organization level.

Theme provides look and feel to portal. Select **Default Portal Theme** that will be applied to portal when user logs in.

You can choose to either View or Download PDF under the **Default Print Option**.

Users need to specify report output format on pages like **Ad hoc Wizard** and report deployment page. Select a format in **Default Report Format**, which will be selected by default under Report Format on Ad hoc Wizard. It will also be used as default format during report deployment (**Manage Categories and Reports** page).

Look and feel of ad hoc reports depends on the template you have attached with the report. In **Default Ad hoc template**, select the template that should appear selected on Ad hoc Wizard.

Recently generated reports are listed on **My Reports** page. In **Recent Report Count**, specify the number of newly generated reports that should be listed. Default count is 10.

Application objects are saved in folders. Number of pages in application require user to navigate to the folder in which an object is available. If most of the users of this organization will need to access a specific folder frequently, you can set it as **Working Folder**.

When Working Folder is set on this page, and users of this organization tries to access folders, working folder set here will appear selected. This helps save their time to navigate to the folder every time they wish to access that folder. To set the working folder, (make sure the folder already exists), click  . It will open Object selector where you can navigate to the desired folder and set it as Working Folder.

Select the **Entity Types** like Query Object, Analytical Object, Report, etc. that should get selected by default under the Explorer tab.

Specify the **Entity Type Properties** that should appear for the selected Entity Type under the Explorer tab.

You can specify a default connection under **My Default Connection** for the users of the selected organization.

Data Restriction

When users run a report having user parameters, they must provide parameter value(s) before report can be generated. For example, to get sales detail report, user may have to provide month names. Similarly, to get product details by product line, user may provide product line values. Using Data Restriction feature, you can make sure users provide value(s) from a pre-set value only.

Click **Data Restriction** tab to set the values for the users of the selected organization.

You can select values from under **Available Groups/ Values**. Apart from these, you can also specify an **Additional Value** for your report parameters.

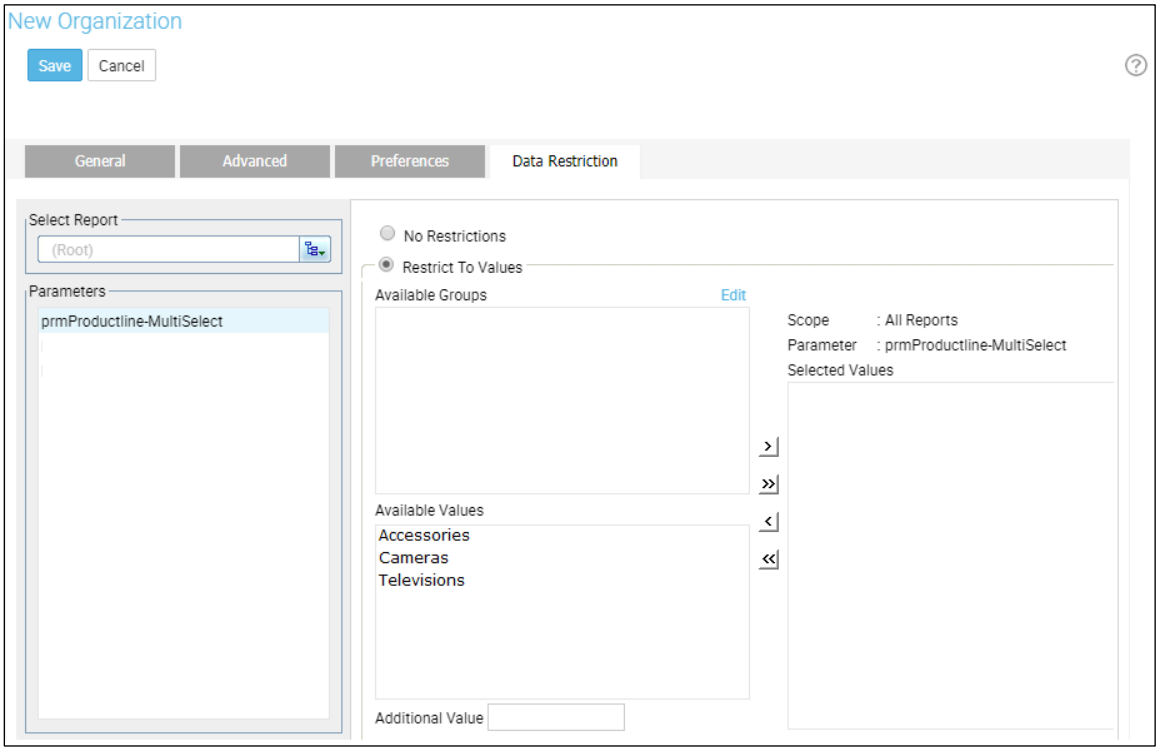

Figure 5: New organization – Data Restriction tab

Managing Users/Roles

When Intellicus runs in secured mode, you need to login into Intellicus to access its functionalities. Functionalities available to a user depend on the system privileges and access rights granted to the user.

On Users/Role page, you can create users and grant them system privileges. You can also change user/role details as well as suspend and delete a user or role.

Click Navigate > Administration > Manage Users > User/Role to open **User/Role** page.

When you have many users who will be granted same type of system privileges, you need not work on each user individually. You may create a role, grant those system privileges to the role and then, assign that role to all the users who need to be granted those system privileges.

User/role belong to an organization. When you open this page, you see a list of organizations on the left of the page. This is an expandable list, having default organization expanded.

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

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 selected organization. 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.

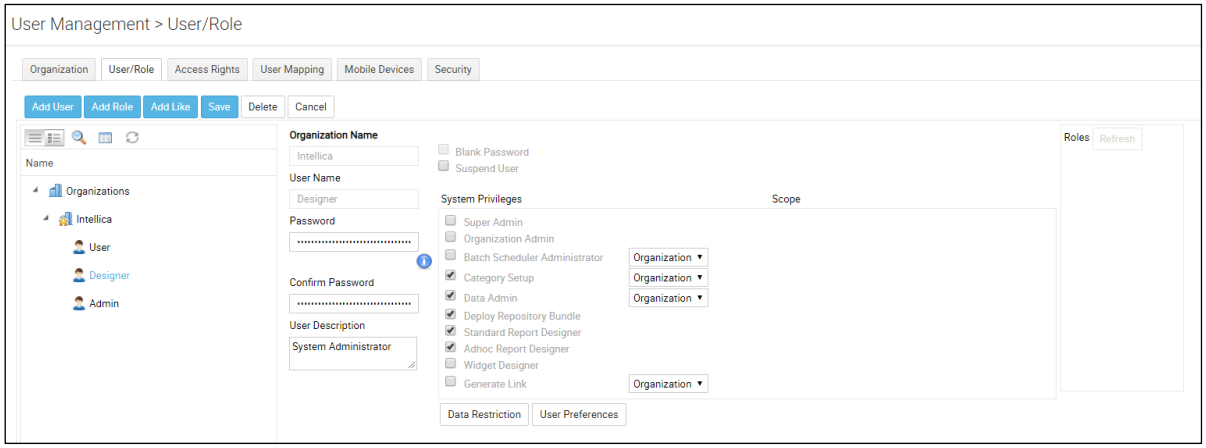

Figure 6: User/Role page

System Privileges

Functionalities available to a user in Intellicus depend on the system privileges and access rights granted to the user. System privileges are granted to a user / role on this page. They are:

- **Super Admin:** (Not applicable to Role) User will be able to carry out all configuration, customization and administrative activities of the application.
- **Organization Admin:** User will be granted all administration rights for the organization to which he/she belongs. For example, creating users and giving them access rights.
- **Batch Scheduler Administrator:** User will be able to view and create jobs, schedules and tasks. If the scope is Organization, user will have access to jobs, schedules and tasks created by users belonging to his/her organization. If the scope is Global, user will have access to jobs, schedules and tasks created by users belonging to any organization.
- **Category Setup:** User will be able to view all public categories and create public categories. If the scope is Organization, user will have access to categories created by users belonging to his/her organization. If the scope is Global, user will have access to categories created by users belonging to any organization.
- **Data Admin:** User will be able to view and create Query objects, Parameter objects and work with Parameter Value Groups page. If the scope is Organization, user will have access to parameter objects and query objects created by users belonging to his/her organization. If the scope is Global, user will have access to parameter objects and query objects created by users belonging to any organization.
- **Deploy Repository Bundle:** User will be able to deploy the repository bundle from Deploy Repository Bundle portal page.
- **Standard Report Designer:** User will be able to design standard reports using Intellicus desktop studio and Intellicus web studio.
- **Ad hoc Report Designer:** User will be able to design ad hoc reports using Ad hoc Wizard.

- **Widget Designer:** User will be able to design dashboard widgets. Widgets are placed on dashboards.
- **Generate Link:** User will be able to generate a link of any published report to be shared with non-Intellicus users.

Creating users/roles

When you have many users who will be granted same type of system privileges, you can create a role, grant those system privileges to the role and then, assign that role to all the users who need to be granted those system privileges.

User

To start creating a user, click **Add User** button. The page will be refreshed having blank entry boxes to fill in the details of new user being created.

Specify a unique **User Name**. You can use alphabets, number, dot, dash, @ and underscore to make a user name. Specify password in **Password** text box and confirm by typing in the same password in **Confirm Password** textbox.

Specify **User Description** to give some details of the user, for example when you create a common user name that will be used by multiple individuals you may add the group detail in this textbox.

Grant system privileges to the user by checking corresponding checkboxes under **System Privileges**. Instead of individually granting system privileges to every user, you can also create a role having those privileges, and add that role to the user being created.

If you want to add a new role or user having most of the system privileges like another user / role, you can reduce your creation efforts using **Add Like**. Select the user / role and then click **Add Like** button. Page will be refreshed having system privileges selected like the selected user / role.

Set **Data Restriction** for the user to provide him/her with a limited set of values to choose from while running a report. Refer “HowtoSecureDatainIntellicus.pdf” for more details.

Click **User Preferences** button to setup user preferences like portal preferences, email ID, user's default data connection. To know more, refer the Preferences under Organization section on page 8.

Role

To start creating a role, click **Add Role** button. The page will be refreshed having blank entry boxes to fill in the details of new role being created.

Specify a unique **Role Name**. You can use alphabets, number, dot, dash, @ and underscore to make a user name. You can also enter the **Role Description** if you wish to.

Grant system privileges to the role by checking corresponding checkboxes under **System Privileges**. When you will select this role for a user, he/she will inherit all the privileges granted to the role and so will be able to access corresponding functionalities.

Working with User/Role

Modifying user/role details

You can modify all user details except user name. To modify the user details, select the user, make changes and save the work.

You can modify all role details except role name. To modify the role details, select the role, make changes and save the work.

Deleting a user/role

To delete a user or role, select corresponding role or user and click Delete button. A confirm delete dialog will appear. Click OK to go ahead with the deletion.

Note: If a role that was assigned to user(s) is deleted, the privileges that the users were enjoying due to that role will be revoked.

Suspending a user/role

When you suspend a user, the user will not be able to login into the application. When you suspend a role, all the system privileges available to the users through this role will not be available.

To suspend a user or role, select the corresponding role or user, click **Suspend User** check box and save the changes.

Managing Access Rights

End-users, by default don't have any system privileges. They specifically need to be granted access rights depending on their application access needs. For example, rights to be able to create and manage Query Object (QO) and Parameter Object (PO); rights to create, run and save ad hoc reports, etc.

This application supports multi-level categories. A category may contain objects like Query Objects, Parameter Objects, dashboards etc.

Use **Access Rights** page to manage end-user access rights on categories, QO, PO, reports, dashboards and dashboard-widgets, analytical objects as well as Connections.

Click Navigate > Administration > Manage Users > Access Rights to open this page.

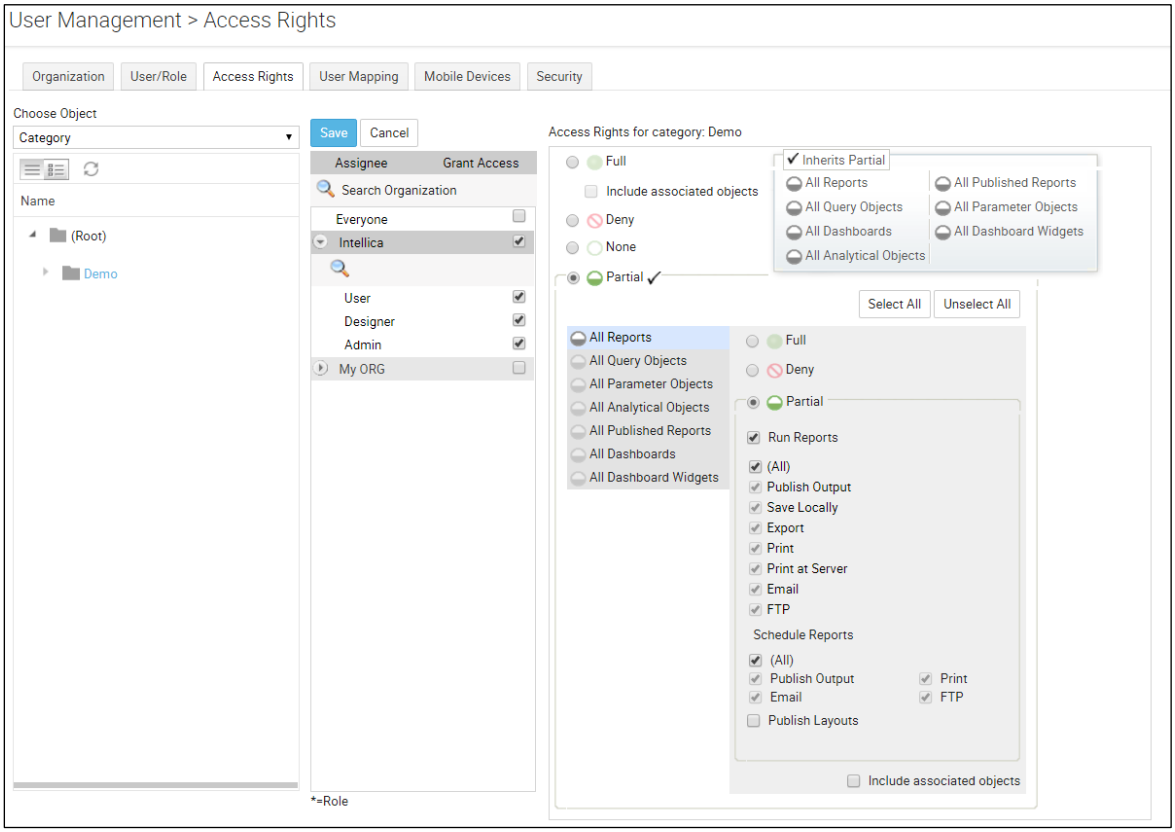

Figure 7: Entity Access Rights page

From **Choose Object** dropdown available on the top left of the page, select the object you want to work on. List of the items will be available below.

Checkboxes to select assignees are in the center and access rights details appear on the right side of the page.

At a time, you can select an object and grant access right on the selected object to:

- All users of all organization(s)
- All users of the selected organization(s)
- All users who are assigned the selected role(s)
- Selected user(s)

Access rights are: Full, Deny, None and Partial.

General steps

To grant rights on category, select category in **Choose Object** dropdown, navigate to respective category and select the category.

To grant rights to an object, select respective object type in **Choose Object** dropdown, navigate to the category where the object is and select the object.

Now, select assignee(s), select access rights and click **Save** button.

Application will display an alert if you navigate away to another category, object or select another assignee without saving the changes.

Access rights for category

Objects like Reports, Parameter Objects (POs), Query Objects (QOs) etc. are saved in categories. Access rights for category are:

- **Full:** Selected category and all its child categories will be listed to the user. User will be able to open any of the categories and carry out any operations on any of the objects in the categories and its child categories.
- **Deny:** Selected category and any of its child categories (as well as objects in it) will not be listed to the user. As a result, user will not be able to access any of the categories (as well as objects in those categories).
- **None:** Selected category and all objects in the selected category will not be listed to the user (hidden), but will be available for access to the user.
- **Partial:** User can access selected category and all objects on which access is provided. For example, you may grant the user access to all reports, all QOs but not POs.

Access rights on Reports

These are the rights to carry out report operations on selected report (direct run and scheduled run).

- **Full:** User will be able to carry out all the report operations on the selected report.
- **Deny:** Selected report will not be listed to the user. User will not be able to carry out any operation on selected report.
- **Partial:** User will be able to carry out report operations as per following on the selected report.
- **Include associated objects** when checked under Reports, enables execute right for all objects associated with that report.

Schedule Reports

Select **(All)** to allow user to create private schedule of report delivery as well as run report in background for all delivery types. Uncheck **(All)** and select the delivery types to allow scheduled delivery and run in background operations in corresponding selected delivery option.

Delivery of scheduled reports can be made via publish, print, email or FTP.

Access rights on Query Object (QO) / Parameter Object (PO) / Analytical Object (AO)

- **Full:** User will be able to carry out all operations on the QO / PO / AO.
- **Deny:** User will not be able to carry out any operation on the QO / PO / AO.
- **Partial:** Partial rights for QO / AO are: Read, Write and Execute. Partial rights for PO are: Read, Write and Prompt.
    - **Read rights on QO / PO / AO:** Object will be listed to the user. User will be able to open, view and save as a PO / QO / AO. To carry out these operations on a category, user should have Read rights granted at category level (all POs / QOs / AOs).

- **Write rights on QO / PO / AO:** User will be granted all the rights that are granted through Write rights. Also, user will be able to update an object (modify it and save with the same name). To carry out this operation on a category, user should have Write rights given at category level (all POs / QOs / AOs).
- **QO / AO Execute:** QO / AO will be listed to the user. User will be able to view the QO / AO details. User will be able to use it at all the places where that QO / AO needs to be executed / built, like during report execution.
- **PO Prompt:** PO will be listed to the user. User will be able to view the PO details. User will be able to use it at all the places where that object's execution is required, like Input Parameter Form.

Access rights on Dashboards / Dashboard Widgets

- **Full:** User will be able to carry out all operations on the dashboard / dashboard widget.
- **Deny:** User will not be able to carry out any operation on the dashboard / dashboard widget.
- **Partial:** Partial rights for dashboard / dashboard widget are: Read, Write and Execute. If none of these rights are granted, it will not be listed and so user will not be able to execute or update it.
    - **Read Rights:** The dashboard / dashboard widget will be listed to user. User will be able to view the dashboard / dashboard widget. User will however be able to copy definition from one category to another.
    - **Write Rights:** User will be granted all the rights that are granted through Write rights. User will be able to update the definition (modify it and save with the same name) and delete the dashboard / dashboard widget. To carry out this operation, user should have Write rights at category level.
    - **Execute Rights:** Dashboard / dashboard widget will be listed to the user. User will be able to view its details, and execute the objects on dashboard / dashboard widgets.
    - **Include associated objects** when checked under Dashboards, enables execute right for all objects associated with that dashboard.

Access Rights on Connections

- **Full:** User will be able to run reports on the selected connection.
- **Deny:** User will not be able to run reports on the selected connection.

User Mapping

When Intellicus is integrated with another application, an organization needs to be created in Intellicus, users need to be created in that organization with desired privileges and access rights. Host application users are then mapped with these users.

User Mapping is set on **User Mapping** tab. Click Navigate > Administration > Manage Users > User Mapping.

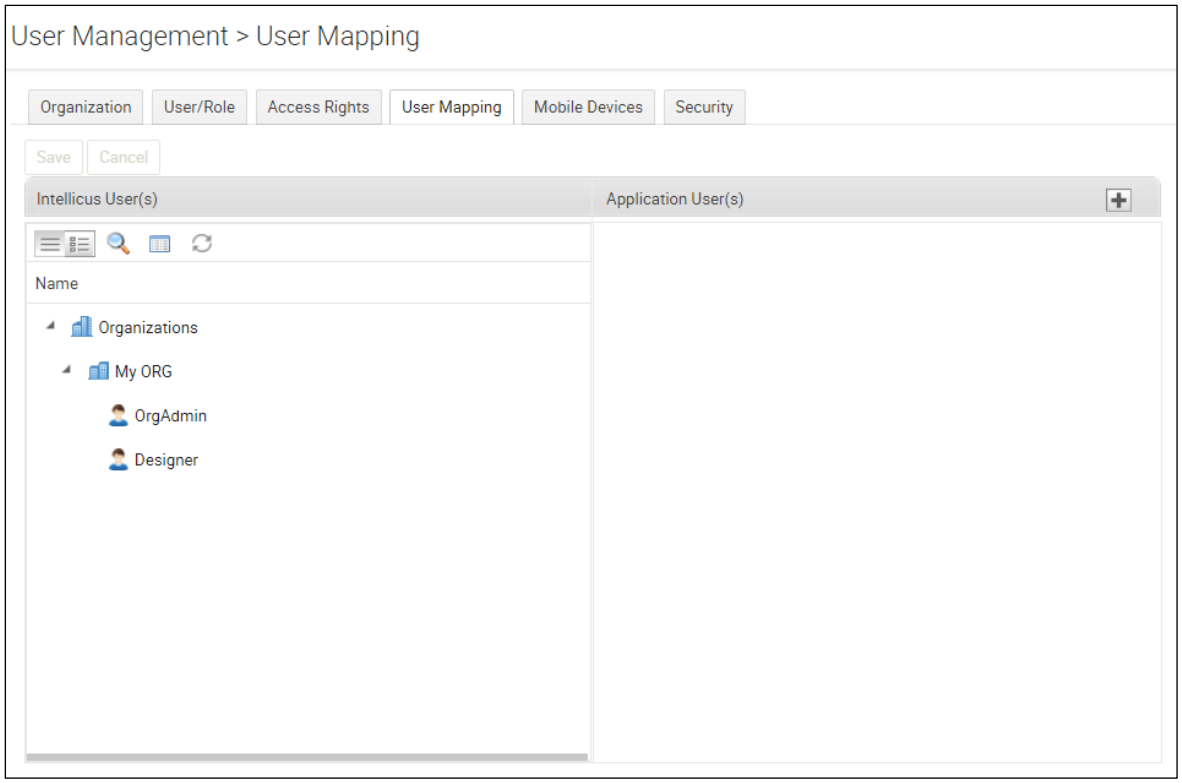

Figure 8: User Mapping page

When a request will come from host application users they will be able to carry out tasks based on the Intellicus users / roles they are mapped with.

User / role belong to an organization. When you open this page, you see a list of host organizations under **Intellicus User(s)** list. This is an expandable list.

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

To add a mapping

1. From **Intellicus User(s)** list, select the user that you want to map to the application user.
2. Click  button on top-right corner of the User Mapping screen. A row for mapping appears.
3. In **Application User(s)** entry box, specify the user-name used by the application.
4. Click **Save** button.

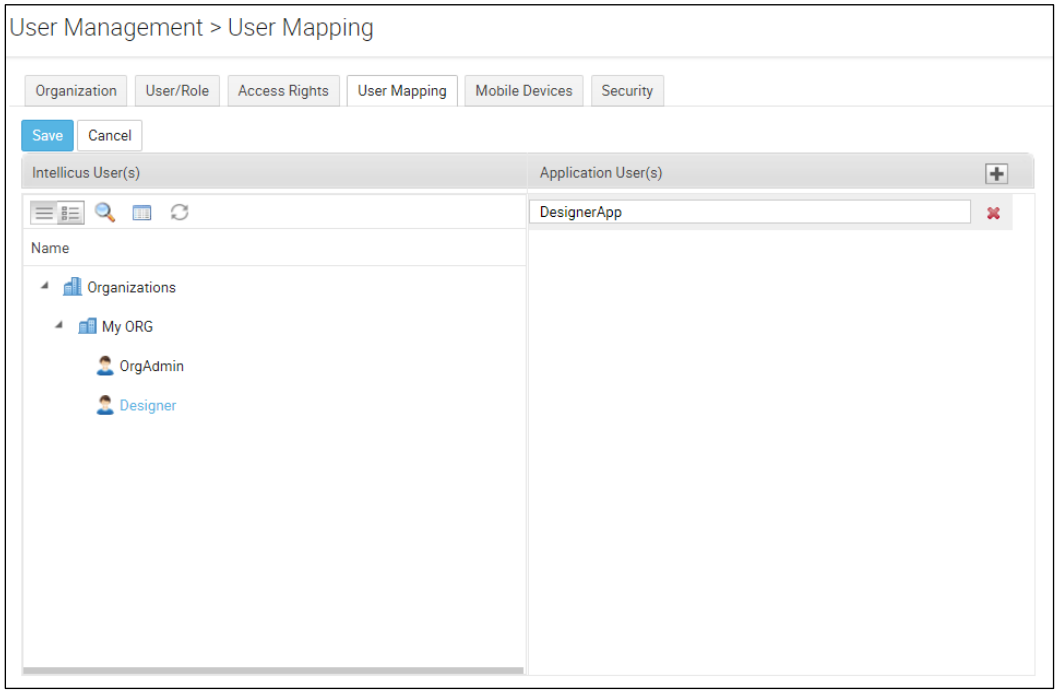

Figure 9: Adding a user mapping

Now on, when a host application user tries to access Intellicus, he/she will be able to access the functionalities available to Intellicus user mapped with that application user.

The mapping information is saved.

To edit the entry of Application User, click and select Intellicus User from the drop down.

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

Click button of respective row to delete a mapping.

Note: The entry box Application User(s) and Intellicus User(s) may be replaced by Application Role and Intellicus Role based on settings done on Organization page.

Mobile Devices

This tab is used to register/ administer mobile devices to be able to connect to Intellicus Report Server. This is discussed under section “Installing and Configuring Intellicus Mobile” in the document titled InstallingIntellicusOnWindows.pdf

Note: This is a license-controlled feature. You need to have a compatible license to view this tab.

Security

Under this tab, you can set the complexity level for user's password once the **Enforce Policy on Login** is checked.

You can enforce restrictions on the **Minimum Password Length**, **Contains Number**, **Contains Mix Case Character** or **Contains Special Character**. You can also provide a check that the specified password **Should Not Resemble Or Contain User Name**.

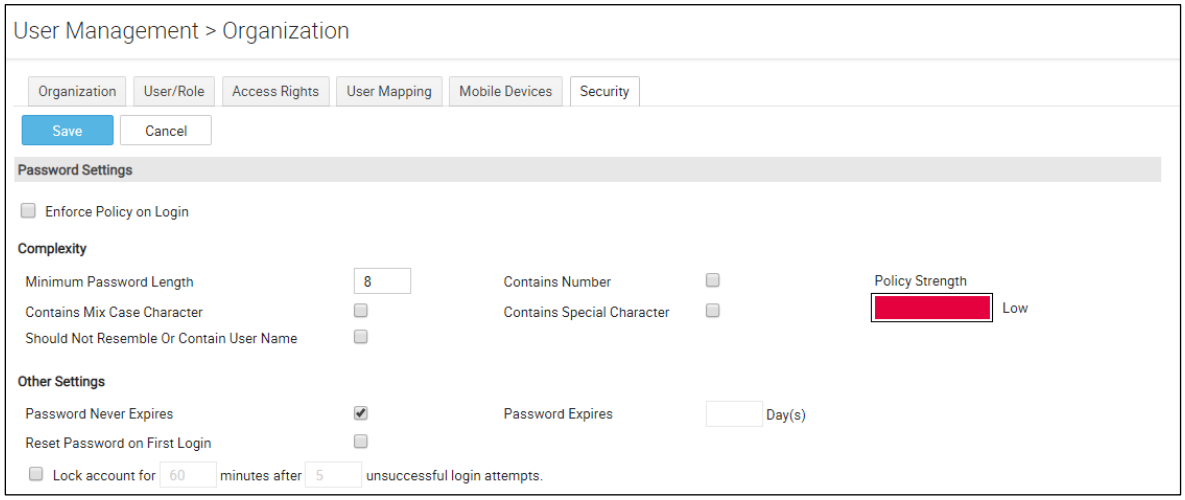

Figure 10: Security page

You can check **Password Never Expires** if you wish the login password should not expire. Specify the number of days of expiration under **Password Expires**. **Reset Password on First Login**, when checked, prompts to reset the password after first login attempt. You can also **Lock account for x minutes after n unsuccessful login attempts**.