How to Secure Data 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

How to Secure Data

Data security feature in Intellicus enables users to view only the data which he/she is permitted to view. When you run a report having user parameters, you have to provide parameter value(s) before report can be generated. Using Intellicus' Data Restriction feature, you can restrict users to specific data by being able to select parameter value(s) from a pre-set (restricted) values only.

Data Restrictions can be configured by Intellicus administrators to restrict a user's access to data.

This document covers the functional aspect of how to achieve data restriction for Intellicus users.

Data Security on Query Objects

Let us see the concept of Data Restriction with an example:

Suppose there are two floor managers with respective set of sales representatives reporting to these floor managers. Data Restriction would facilitate each floor manager to view sales data of their respective representatives only. There is also a store manager who can view sales data of all the representatives.

1. As a super administrator, you can configure a set of parameter values for each user. The user can thus select value(s) from the specified set only.
   To apply this data security restriction, you need to specify a parameter as 'Data Restriction' type under Navigate > Repository > Report Objects > Parameter (or under Navigate > Design > Parameter Object).

   Let us first create a secure parameter "prm_REP_name" to fetch the representatives' names. You must check the "Data Restriction" option and save the parameter. (To know more about creating parameters, please refer "WorkingwithParameterObjects.pdf").

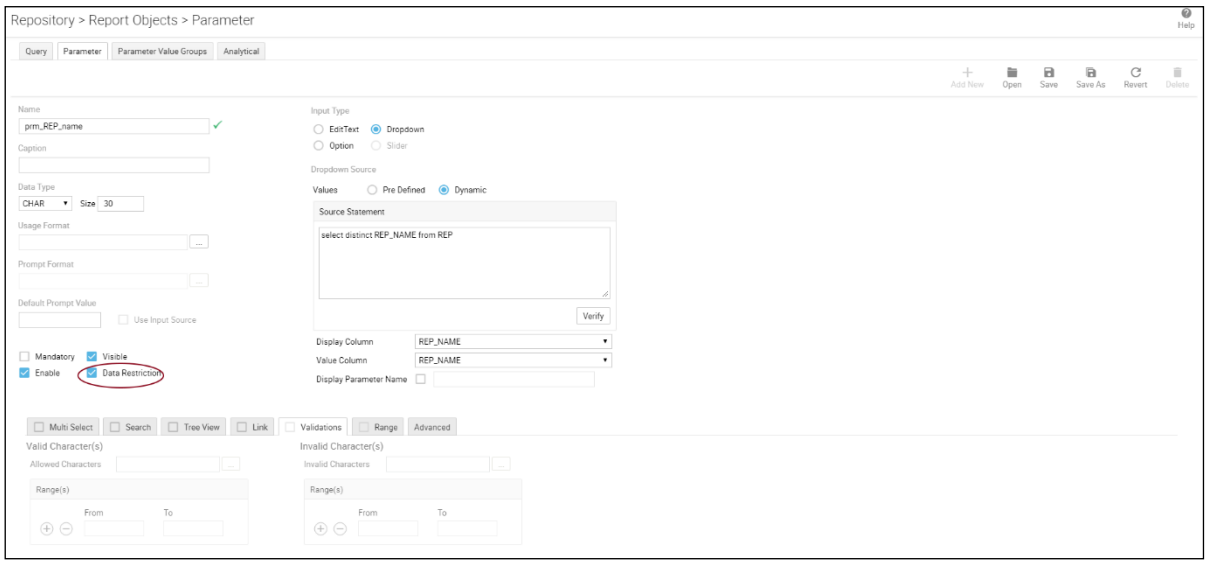

Figure 1: Parameter Object Editor: 'Data Restriction' Parameter

Users will be restricted to view data in reports based on Data Restriction parameter values assigned at the organization and user level (as mentioned in steps 2 and 3).

2. Apply data restriction at the Organization level. Go to Navigate > Administration > Manage Users > Organization to set data security restriction values for the organization. Select organization and click the Modify button. Go to "Data Restriction" tab under Modify Organization dialog box.

   For the parameter created in step 1, you can select 'Restrict To Values' option to specify allowed values from under **Available Groups/ Values**. Apart from these, you can also specify an **Additional Value** for your report parameters. Click Save.

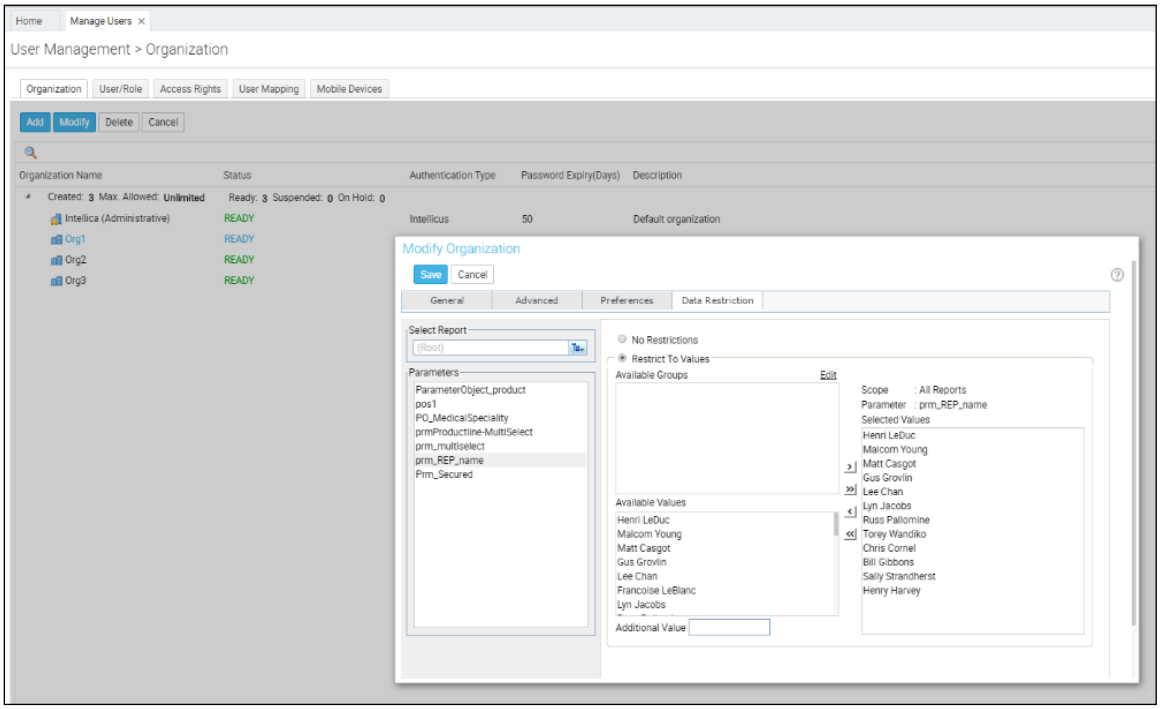

Figure 2: Data Restriction on Organization

3. Apply data restriction for the "Floor Manager1" user as shown in Figure 3. Go to Navigate > Administration > Manage Users > User/Role. Expand the organization (as selected in step 1) from the left side of the screen to select the user. Next, click the **Data Restriction** button (that appears below the System Privileges section on Figure 3) to set the values for Floor Manager1. Once you click Data Restriction button, it opens a new dialog box. In this dialog box, select the parameter with "Data Restriction" checked as created in step 1. You can select parameter values from under **Available Groups/ Values** when 'Restrict To Values' option is chosen. Click Save.

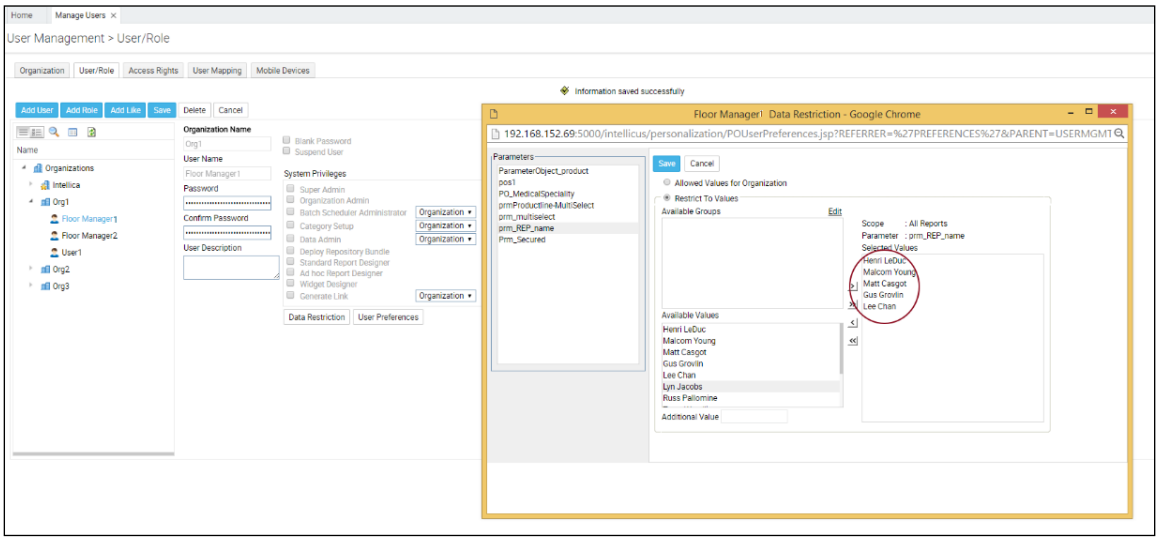

Figure 3: Data Restriction for 'Floor Manager1'

Similarly, apply data restriction for the “Floor Manager2” user as shown in Figure 4:

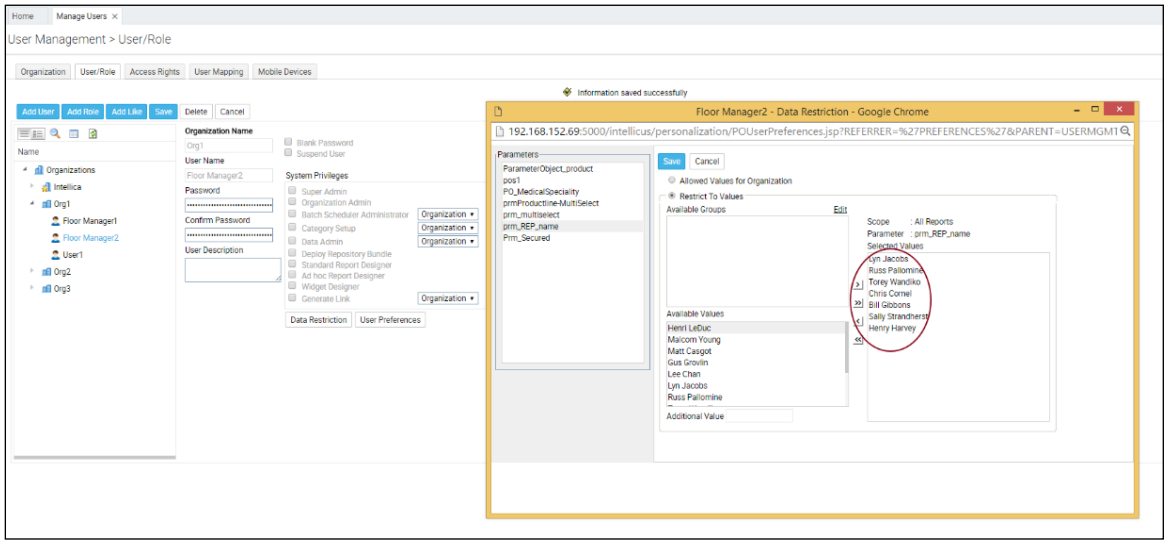

Figure 4: Data Restriction for ‘Floor Manager2’

For the "Store Manager”, select all the values of representatives allocated to "Floor Manager1" and "Floor Manager2".

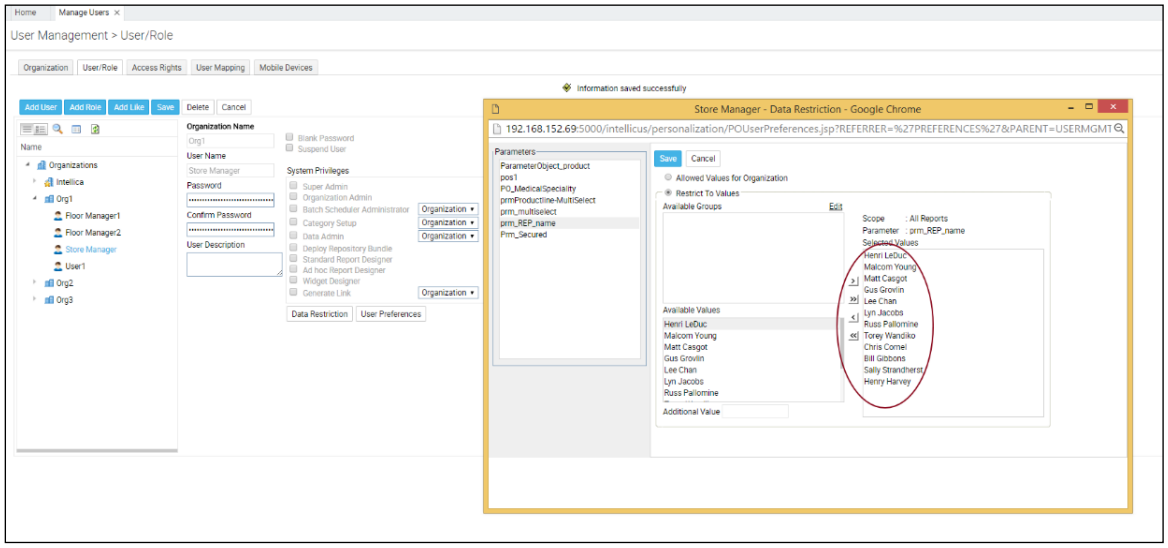

Figure 5: Data Restriction for ‘Store Manager’

4. Next, let us define the parameter “prm_REP_name” in a query of Query Object as shown in Figure 6. The below query fetches sales representatives according to the values assigned to parameter in steps 2 and 3.

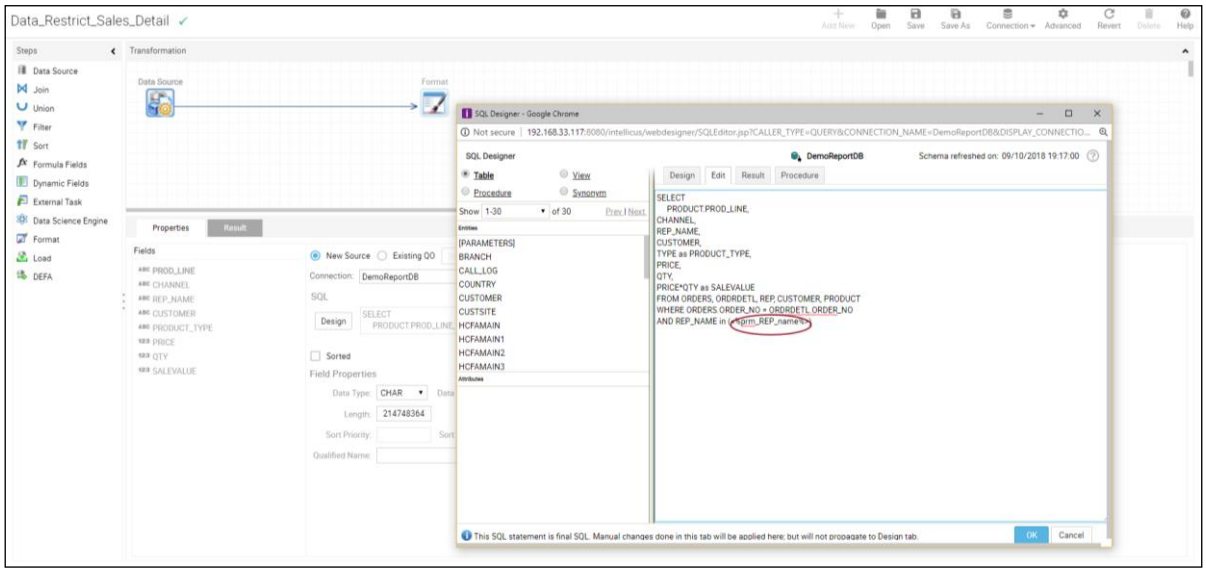

Figure 6: Query Object Editor to Define Parameter

5. Now, when the ‘Floor Manager1’ logs in and runs a report using the above mentioned Query Object, only the restricted list of values of representatives appear as shown in Figure 7:

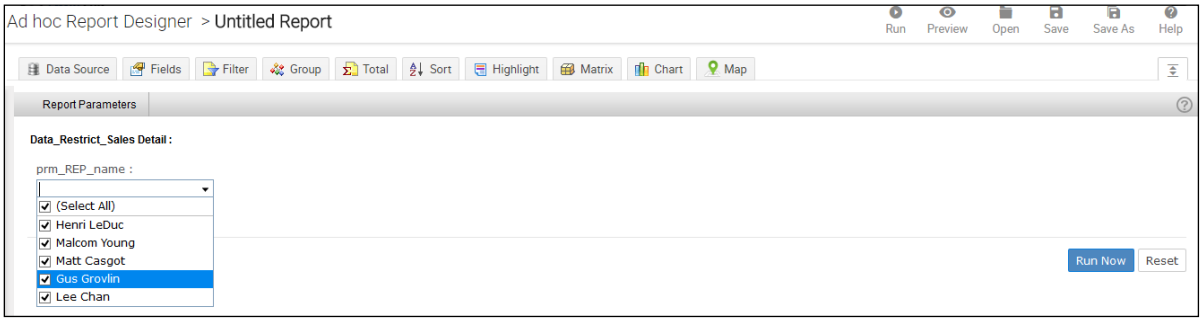

Figure 7: Run Report as ‘Floor Manager1’

Similarly, for ‘Floor Manager2’, the restricted list appears as shown in Figure 8:

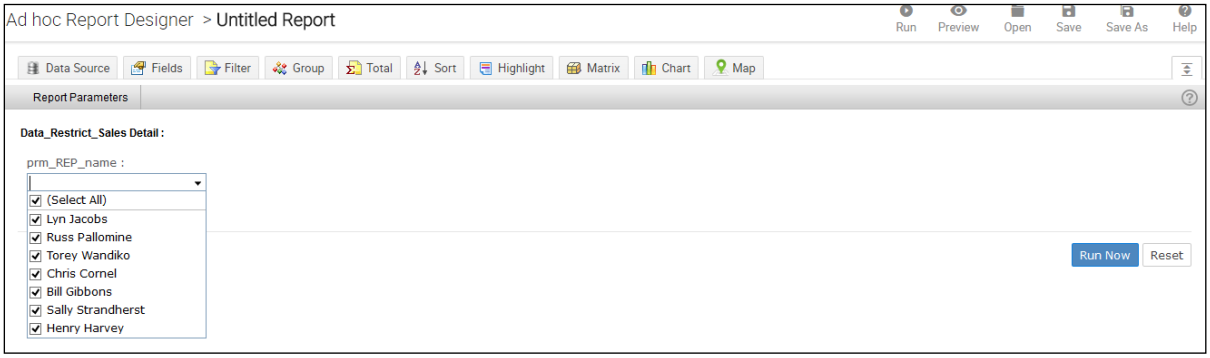

Figure 8: Run Report as ‘Floor Manager2’

When the ‘Store Manager’ logs in and runs the same report, the entire representatives list appears as shown in Figure 9:

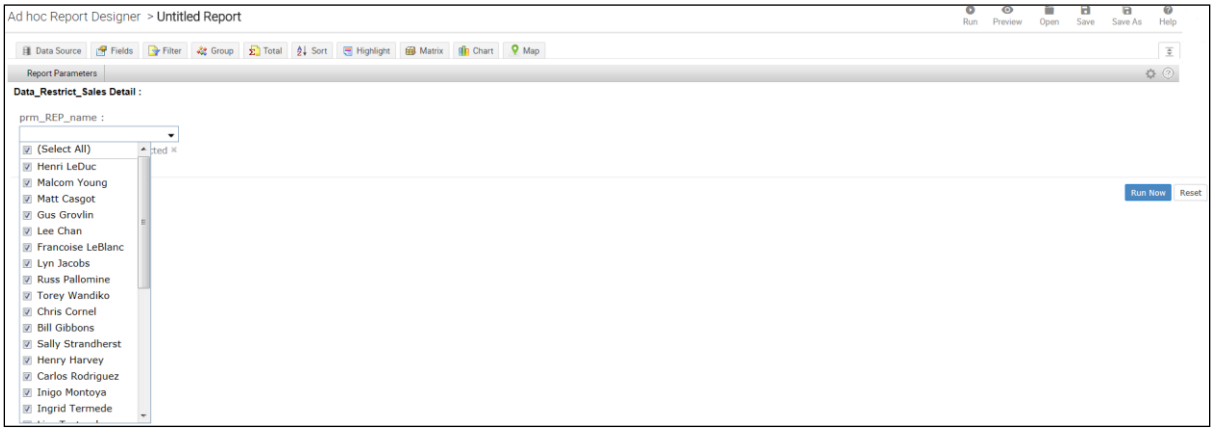

Figure 9: Run Report as ‘Store Manager’

You can thus restrict users, access to specific set of data as per their role.

Data (Row-Level) Security on High Speed View (OLAP Cubes)

Intellicus implements security policies that restrict data access based on users' roles. Suppose there are employees who have access to their respective set of insurance data. Data Restriction in Intellicus would facilitate each employee to view insurance data of their respective countries only. There is also a manager who can view insurance data of all the countries.

1. As a super administrator, you can configure a set of parameter values for each user. The user can thus select value(s) from the specified set only.
   To apply this data security restriction, you need to specify a parameter as 'Data Restriction' type under Navigate > Repository > Report Objects > Parameter (or under Navigate > Design > Parameter Object).

   Let us first create a secure parameter "prm_Country" to fetch the countries' names. You must check the "Data Restriction" option and save the parameter. (To know more about creating parameters, please refer "WorkingwithParameterObjects.pdf").

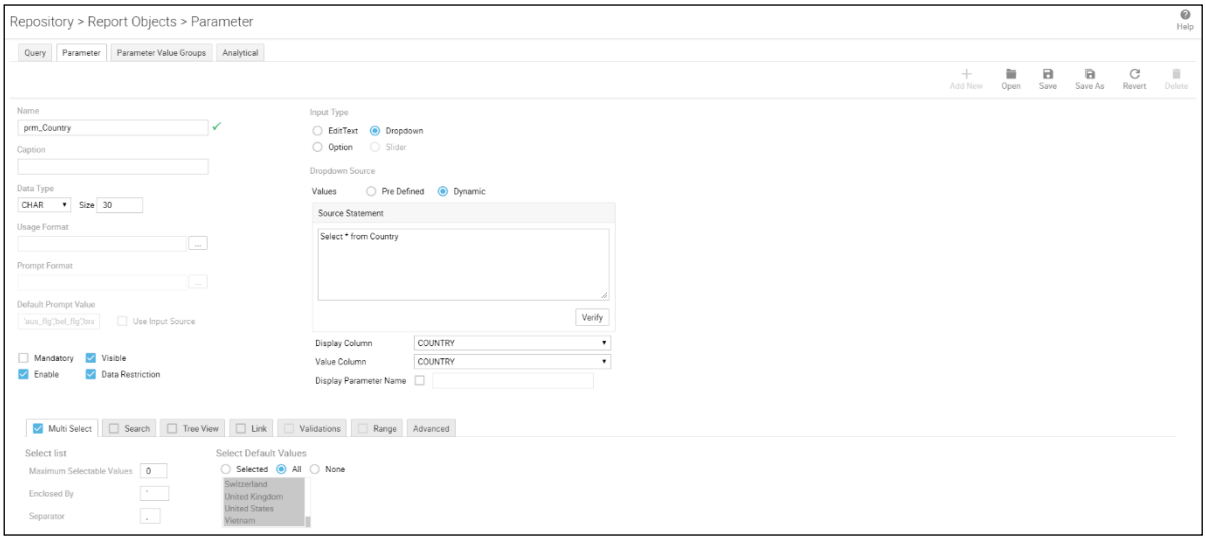

Figure 10: Parameter Object Editor: 'Data Restriction' Parameter

Users will be restricted to view data in reports based on Data Restriction parameter values assigned at the organization and user level (as mentioned in steps 2 and 3).

2. Apply data restriction at the Organization level. Go to Navigate > Administration > Manage Users > Organization to set data security restriction values for the organization. Select organization and click the Modify button. Go to "Data Restriction" tab under Modify Organization dialog box.

   For the parameter created in step 1, you can select 'Restrict To Values' option to specify allowed values from under **Available Groups/ Values**. Apart from these, you can also specify an **Additional Value** for your report parameters. Click Save.

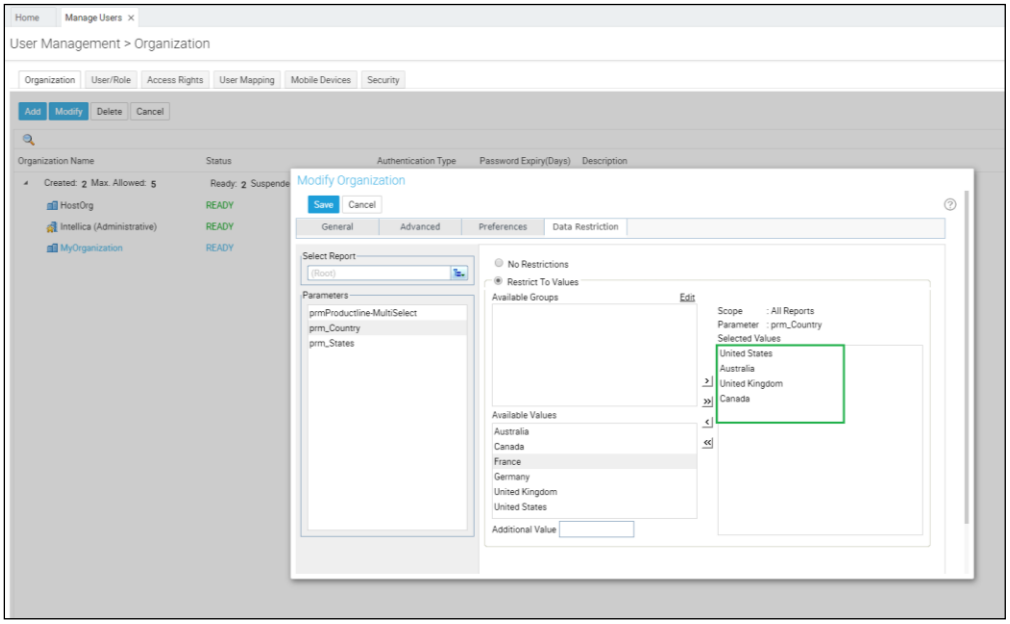

Figure 11: Data Restriction on Organization

3. Apply data restriction for the "Employee1" user as shown in Figure 12. Go to Navigate > Administration > Manage Users > User/Role. Expand the organization (as selected in step 1) from the left side of the screen to select the user. Next, click the **Data Restriction** button (that appears below the System Privileges section on Figure 12) to set the values for Employee1. Once you click Data Restriction button, it opens a new dialog box. In this dialog box, select the parameter with "Data Restriction" checked as created in step 1. You can select parameter values from under **Available Groups/ Values** when 'Restrict To Values' option is chosen. Click Save.

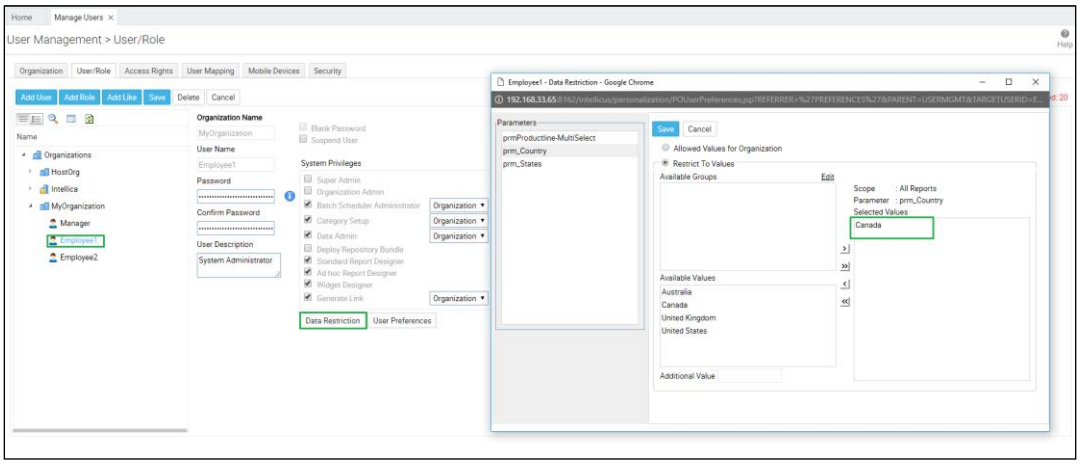

Figure 12: Data Restriction for 'Employee1'

Similarly, apply data restriction for the “Employee2” user as shown in Figure 13:

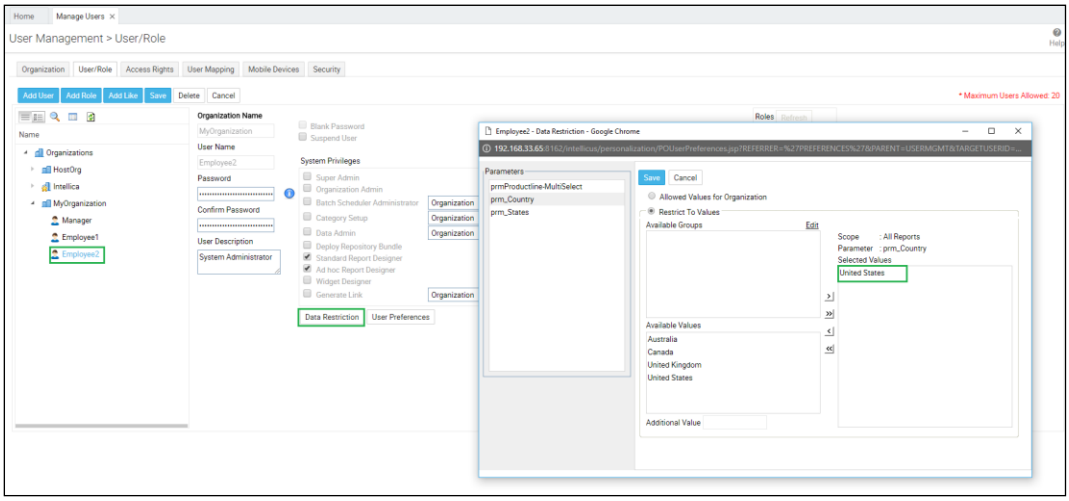

Figure 13: Data Restriction for ‘Employee2’

For the "Manager”, you can select the values of countries that are available for ‘Employee1’ and ‘Employee2’.

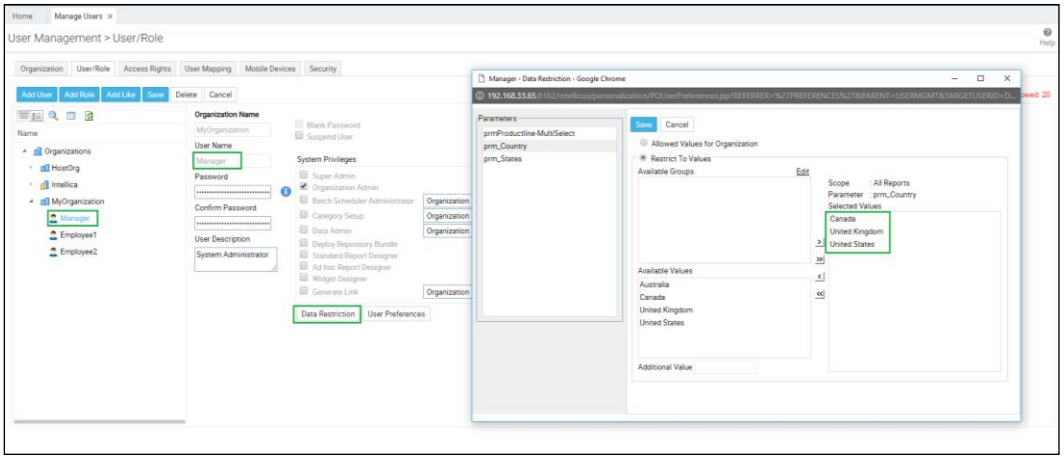

Figure 14: Data Restriction for ‘Manager’

4. Next, let us assign the parameter “prm_Country” to a dimension of Analytical Object as shown in Figure 15. This would fetch the intersection of values assigned to parameter in steps 2 and 3.

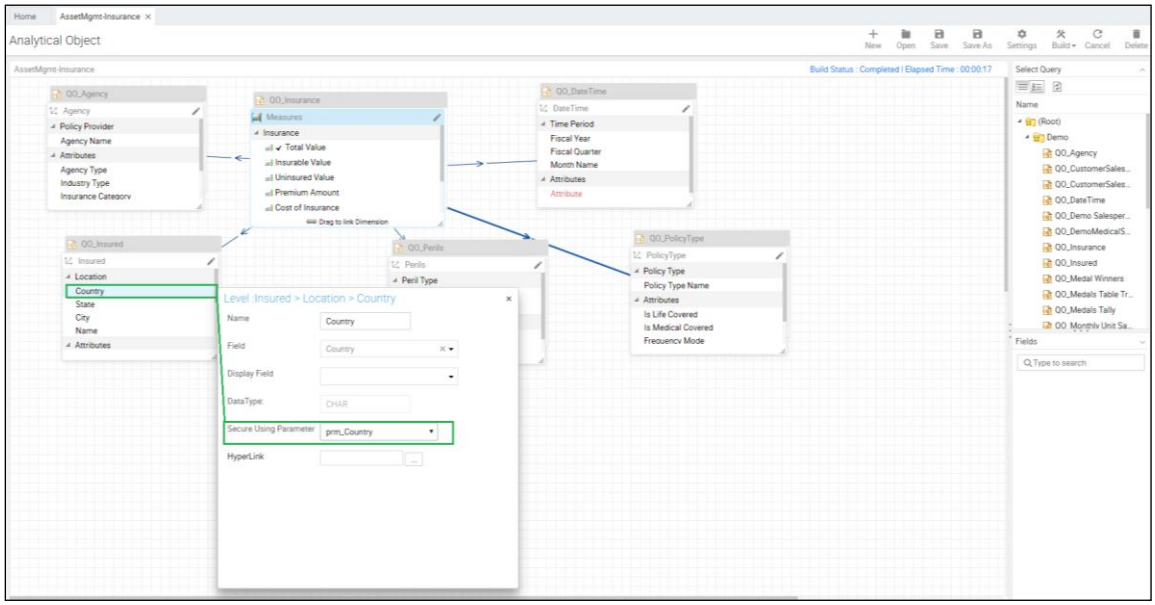

Figure 15: Analytical Object Editor to Define Parameter

5. Now, when the ‘Employee1’ logs in and runs a report using the above mentioned Analytical Object, only the restricted list of values of countries appear as shown in Figure 16:

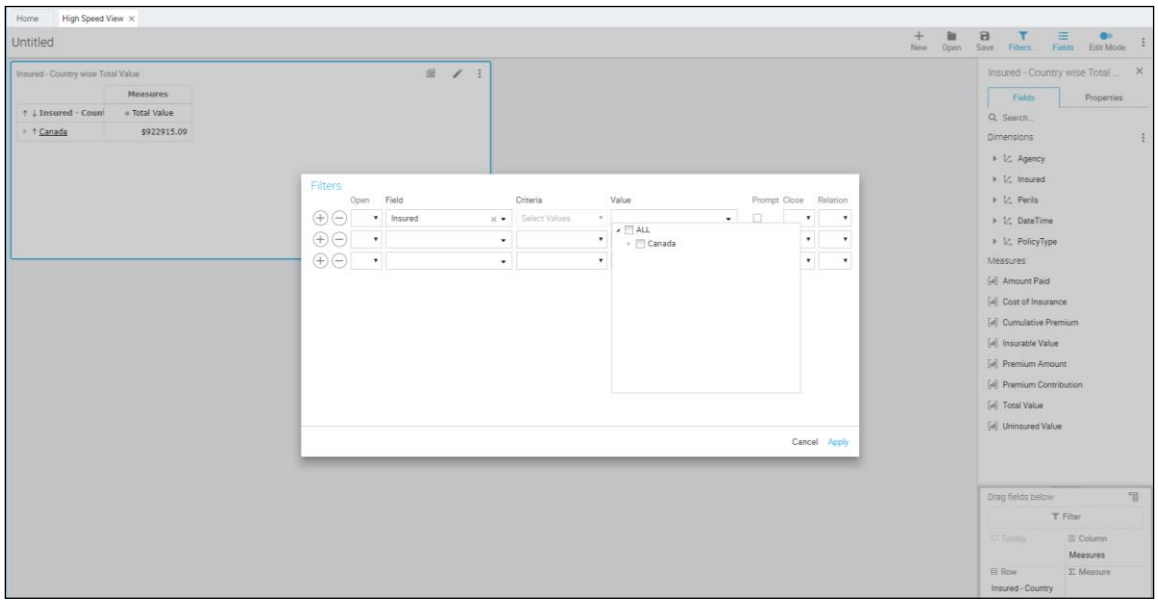

Figure 16: Run Report as ‘Employee1’

Similarly, for ‘Employee2’, the restricted list appears as shown in Figure 17:

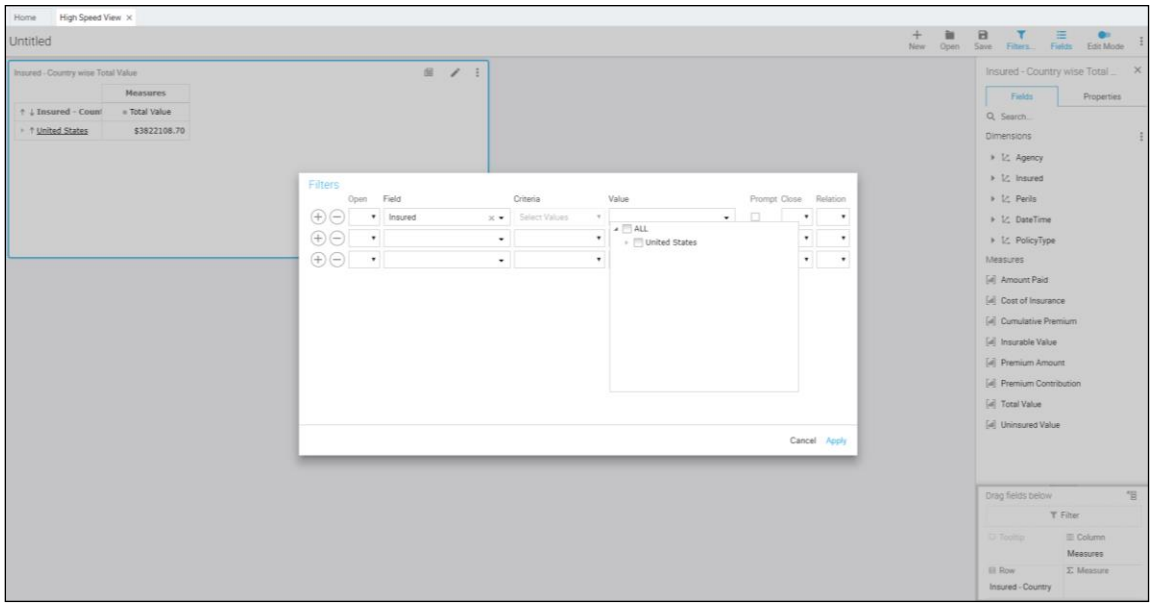

Figure 17: Run Report as ‘Employee2’

When the ‘Manager’ logs in and runs the same report, the entire countries list appears as shown in Figure 18:

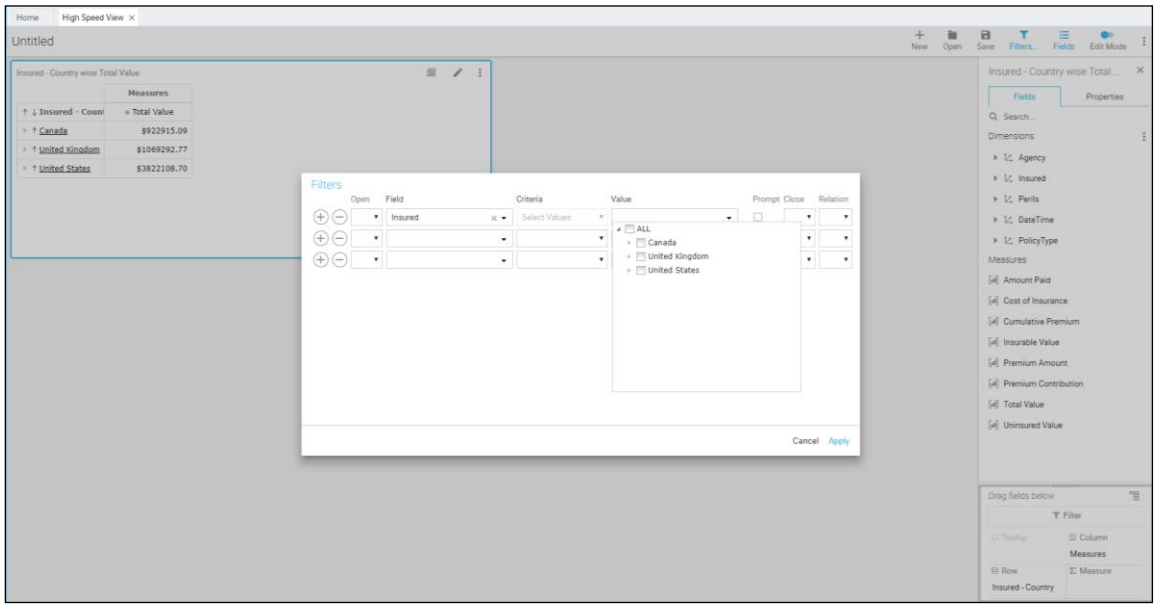

Figure 18: Run Report as ‘Manager’