Setting Up Users and Access Rights

In

ReSure Online

ReSure Version 5 Revised June 2008

CONTENTS

1. OVERVIEW OF RESURE SECURITY

There are three kinds of security in ReSure:

1. **Role** determines what functions you can perform.
2. **Access** determines what data you can view. Access to data is determined by your Role and/or by the Risk Classes, Businesses and Countries that you have been permitted to view.
3. **Responsibility** determines which Sites and Entities have been assigned to you for collecting and updating renewals data.

There are five **Roles** that users can be assigned to:

1. **Administrator** – has access to all system data and functions including configuration
2. **Manager** – a senior person with access to all data.
3. **Business User** – people responsible for updating information
4. **Reviewer** – people with an overview of data but may have delegated responsibility to others
5. **Visitor** – usually external parties such consultants, brokers and insurers.

These roles have access and responsibility permissions as follows:

Role	Data Access Menu Functions Available	Access to Data	Responsibility
Administrator	Define, Collect, Publish	Add, Update or Delete any data.	Designated Sites and Entities
Manager	Collect, Publish	Add, Update or Delete any data.	Designated Sites and Entities
Business User	Collect, Publish	Restricted by specified Risk Class, Country and Business and specified Read/Write permissions	Designated Sites and Entities
Reviewer	Collect	Restricted to data for which user is responsible	Designated Sites and Entities
Visitor	Publish	Restricted by specified Risk Class, Country and Business and specified Read/Write permissions	None (no access to Collect function)

Only an Administrator can change a user's Roles and Access permissions. If you need these to be changed, please contact your Administrator.

Passwords

Any user can change their password - click on My Profile in the menu bar, then Change My Password. Passwords should be set to require renewal after a certain time.

Personal Details

You can change your Personal Details such as email address and phone numbers by clicking My Profile in the menu bar, then My Personal Details. Only the information in the Contacts area is relevant. It is important that you email address be correct, as the system uses email to contact you in regard to various issues.

2. ADDING OR UPDATING A USER

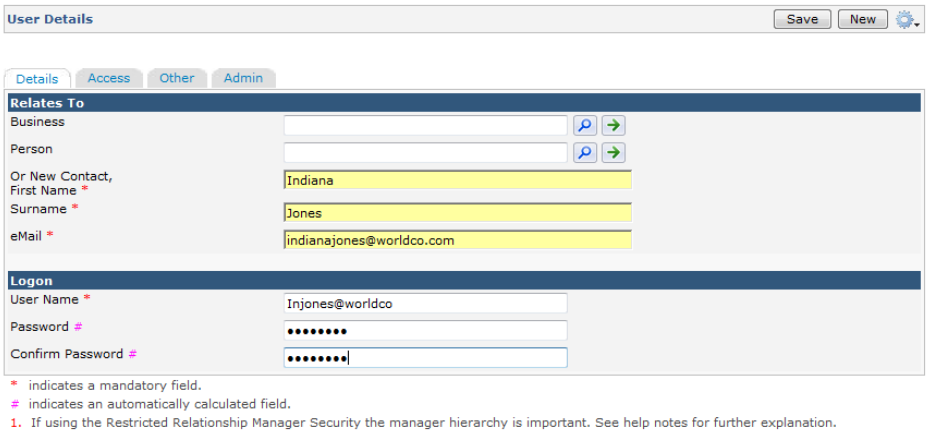
Go to **Define/Users/**and select an existing user, or click the **Add New User** button

Adding a New User Complete the **Details** tab on the **User Details** page as shown in the example below. Ignore the empty Business and Person fields – just complete the ones marked in yellow. The Business and Person fields will be updated automatically when you Save.

Logon: User Name may be the User's email address (recommended) or any form of name that you wish.

Password must be at least 6 characters and contain some numbers, eg "indiana99".

To update details of an existing user, click the View button next to Person to update information about the person on the Contacts page, then Save. Note that some details, such as email address, may be accessed *only* by this method, as they are not displayed on the User Details page.



When the **Details** tab is completed, click on the **Access** tab. Here you have the option to:

Configure Access below. If you select this option, and the user you are adding or updating is *not* an Administrator or Manager, you will need to subsequently set up the Risk Class/Business/Country data access, as described below. Select the **Membership:Subscription** (ReSure) and the **Role** (Business User, Visitor, etc) that applies to the new User.

Duplicate Access of User. If you have already set up Business Users, Reviewers or Visitors, and the User you are adding or updating will have the *same or similar* access permissions to an existing User, this option will copy the selected existing User's access permissions to the new user. It is not necessary to define Risk Class/Business/Country data access, although you may modify these permissions for the new User if they are not exactly the same as those of the existing User that you selected. Typically, you would select this option if the new User worked for the same part of the organisation as an existing User. Note that the new and existing Users' access permissions are *not* linked – if you subsequently change one, the other will not be updated. However, you can use this function to quickly update any other user access permissions to be the same as a specified user, as in the example below.

When updating a User's access permissions, this function *overwrites or replaces all existing ones*. This may be used to advantage in a situation like the following:

> There are 10 Users who have access to the data relating to their division of the organisation. You now wish to update their access permissions to include some Sites in a new Country, provide access to a new Risk Class, and remove access to an existing Risk Class. Make the necessary changes to the permissions of one user only, then use the **Duplicate Access of User** function to set the access permissions of the other 9 to be the same as for that person.

Add Access from User. Similar to **Duplicate Access of User,** but this function *adds access permissions without removing or overwriting existing ones.* If you used this function in the example above, it would *add* the access to the new Risk Class and Country, but would *not* remove access to the existing Risk Class. Another example:

> Joe (a Business User) is responsible for managing data in division A and has now been assigned additional responsibility for division B. Fred (a Business User in division B) already has the additional access permissions that Joe requires. Use the **Add Access from User** function to update Joe's access permissions so that they *include* those of Fred, but *without overwriting* Joe's original access permissions to Division A.

When you have completed this tab, Save and move to the **Other** tab.

Manager – select the existing User to whom the new User reports
Time Zone – set the Time Zone that the new User operates in. Default is AEST (GMT + 10:00)
Time Zone Auto Update – default is Yes, Time Zone will update when Daylight Saving changes.
Send Express Link by SMS – ignore

Now select the **Admin** tab.

In general you should not change any of the defaults on this tab.

Disable will remove the User's access to the system from the date that you specify. Disabled Users do not appear in drop down lists, but their history remains.

Click **Save** when completed.

If you have created a new User with no data access permissions, or if you need to modify the User's access permissions, proceed as below.

Note that Administrators and Business Managers have access to <u>all</u> data, and do not require access permissions to be set.

3. SETTING UP DATA ACCESS PERMISSIONS

A User's Data Access Permissions should always include the data for which they will be assigned Responsibility. It is possible in ReSure to assign Responsibilities to data that the user does not have access to, but this is not recommended.

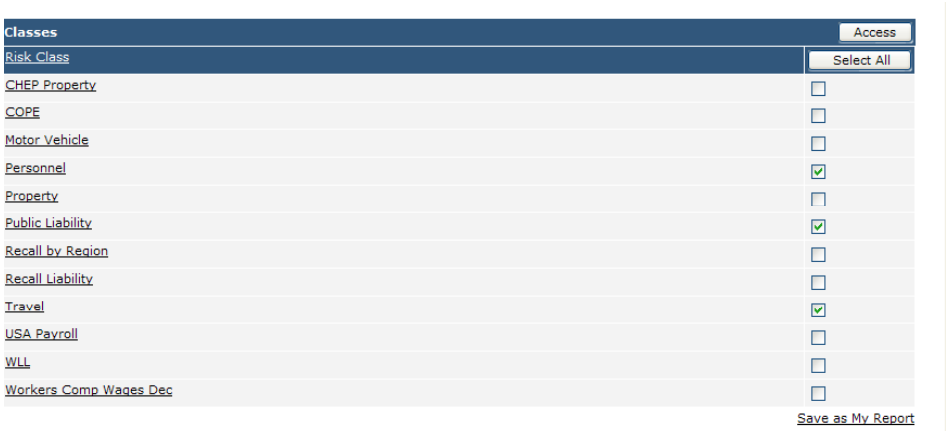
You do not need to set up Access Permissions if you have used the Duplicate Access of User or Add Access from User functions described above.

Access permissions for Business Users and Visitors are assigned by a combination of Risk Class, Business 1 and Country. Access to Sites is determined by Business 1 and Country. Access to Entities is determined by the Sites to which they are attached *plus* the Risk Class access.

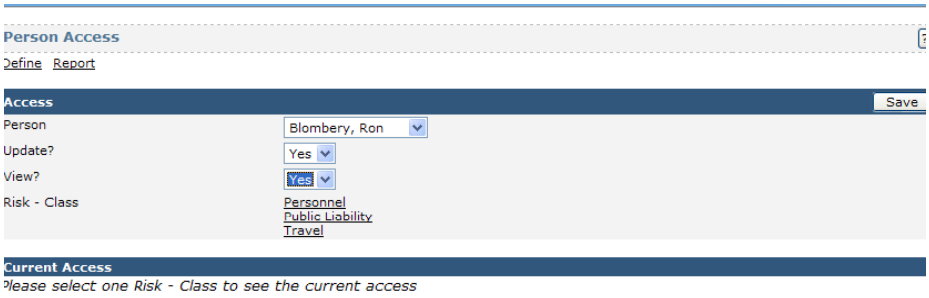
These permissions are assigned from the perspective of the objects: Risk Class, Country and Business 1. Each of these maintains a list of users who have access to values within that object. It is possible, however, to see access permissions from a User's perspective by using the Define / Access report.

When setting up more than one User, it is easiest to focus on the object first, and assign the Users to the object values, rather than deal with all rights for each User.

Access to Risk Classes



- Define/Risk Class
- Check the box(es) that correspond to the Risk Class(es) that the user will have access to, or Select All and uncheck, as appropriate. (In the above example, we have selected Personnel, Public Liability and Travel)
- Click the Access button



- From the Person combo, select the user that you wish to give the rights to.
- Note that there is a list of Risk Classes shown that corresponds to those you have selected.
- If you wish, you can click on each Risk Class to see the other users who have access to that Risk Class.
- Select whether the user will have rights to Update and View data (normally "Yes" and "Yes")
- Click Save. The new user is added to the list.
- If you need to assign the same rights to another user, just select them in the combo, set the Update and View combos, then Save.
- To revoke access rights, select the Risk Class link (if more than one is listed) and click the Remove Access button next to that user.

Access Report

From this page you can click the Report link which enables you to view a report by user, object or both. This report is also available from Define/Access.

Access to Country

- Select the Define / Reference Tables / Country
- Check the boxes for as many Countries as you wish the user to have access to, or Select all and uncheck.
- Click Access and proceed as set out for Risk Class, except use Country instead of Risk Class.

Access to Business 1

- Define / Reference Tables / Business 1, then check the boxes for as many Businesses as you wish the user to have access to, or Select all and uncheck.
- Click Access and proceed as set out for Risk Class, except use Business instead of Risk Class.

When finished, run the Access report to confirm all choices. It's easy to forget to set the Update and View combos, so check that the report shows Y where expected.

4. ASSIGNING RESPONSIBILITY

Responsibility for Sites and Entities may be done on an individual Site and Entity basis using the relevant data entry page. Responsibility may also be assigned in bulk from the Collect page by selecting the required list of Sites or Entities and then using the Set Person Responsible function.

Sites and Entities that have been set this way will then appear in a User's Collect page.

By default, when you Import data, you are set as the Person Responsible for it.

If not otherwise specified, Entities inherit the Person Responsible from the Site to which they are attached.

Assigning Site Responsibility

Before you commence, obtain an Access report for the person to be certain that their Responsibility is within their Access Rights.

Set the Site Filter to select the Sites that you wish to assign a Responsible person to, and Refresh

Check the list to ensure that it is the correct set of Sites

Note: The check boxes in the last column of the Site list play no part in the setting of responsibility for Sites or Entities. They are used for deletion only.

Click Set Person Responsible button

Set the Person who is to be made responsible for the Sites in the combo

Click Save – the Person Responsible is assigned to the selected Sites

You can repeat this as many times as you like, eg if a one person was responsible for three businesses, you might have to do this three times.

To confirm your action, it's a good idea to do a new search using the Person Responsible combo on the filter. This should show all the Sites you just set, plus any that may have previously been assigned to that person.

Assigning Entity Responsibility

The process is basically as for Sites.

Define / Entities to access the page.

If you are going to make the same person responsible for all the Entities attached to the Sites that they are responsible for, set the Advanced (Site) filter to exactly the same setting as you did for Sites. Then Refesh, and check the Entity listing to see that no other person is shown as responsible. If they are, then proceed as for Sites to Set Person Responsible for that list.

As with Sites, you may have to repeat this process several times if one person is responsible for several businesses.

Note that when a new Entity is created, whether by manual data entry, importing a spreadsheet, or rollover, the person Responsible is set to be the same as that for the Site to which it belongs.

To confirm your action, it's a good idea to do a new search using the Person Responsible combo on the filter. This should show all the Entities that you just set, plus any that may have previously been assigned to that person.

See also Delegating Sites and Entities.