

Volume

6

Rights Management

Rintagi
Applications

**User
Guide**



robocoder*corporation*

Table of Contents

Overview	1
Authentication	1
Menu Authorization	2
Row and Column Authorization	3
Configuration	6
Adding a Company	6
Adding a Project	6
Default Row Authority	6
Column Authority Override	9
Row Authority Override	10
User Group Configuration	11
Adding a User	13
Impersonating a User	17
Report & Import Wizard	18

Overview

Rights management is an integral part of Rintagi. All of the rights management is automatically built in to all screens, reports or import wizards as they are generated. Row Authority is used to authorize access to row information; Column Authority is used to authorize column information. Together they form the role(s) for a user.

Authentication

A user name and password are required to access a Rintagi application. A password can be assigned or changed by an administrator once a user is established (as discussed in the next chapter).

Change Password

Command: Operation -> Manage User -> Change Password

The screenshot shows a web form titled "Change Password". At the top right are buttons for "Undo All", "Save", and a help icon. Below the title bar is a "Quick Filter" dropdown menu set to "Active Original Users". A user selection dropdown shows "John Doe" with a search icon. The main form area contains three fields: "New Password*" (password type), "Confirm Password*" (password type), and "Send Email Notice:" with a checkbox. A tooltip at the bottom explains the checkbox: "This is checked if an email notification is to be sent to the user that his/her password has been changed."

A password change notification may be sent to the user's email address. This fully-encrypted password is stored in the database so that not even professionals who have access to the database can decrypt it. Subsequently users may change their password by clicking the "Change Password" link from the login panel after successfully logging in.

New Password:	<input type="text"/>	<input type="button" value="Change"/>
Confirm Password:	<input type="text"/>	<input type="button" value="Cancel"/>

A forgotten password screen with a hint question and answer is also available when needed.

Menu Authorization

There are two authorization levels. For the first level, the login user can be granted access to each menu item by any of the following related entities:

1. User Groups
2. Companies
3. Projects
4. Agents
5. Brokers
6. Customers
7. Investors
8. Members
9. Vendors

Menu Permission

Command: Client Tier -> Menu -> Menu Permission

The screenshot shows the 'Menu Permission' window for 'TblSys (Systems Maintenance)'. The 'Menu ID' is 220. The table below lists various user groups and their permissions for different menu items.

	User Group	Company	Project	Agent	Broker	Customer	Investor	Member	Vendor
<input checked="" type="checkbox"/>	Everyone*								
<input type="checkbox"/>	Sys Administrator								

A row is automatically created in Menu Permission with “Everyone” checked when a menu item is created. “Everyone” can be unchecked and various specific permission groups can be assigned access. In the example above, the systems table maintenance screen is only available to the systems administrator. Additional user groups can be designated by adding more rows.

Row and Column Authorization

The second level of authorization is row and column authorization. Together they form another role for a user.

Once access to the menu level is attained, only the following columns will be permission-managed:

1. `UsrId` – Integer (The user login ID)
2. `UsrGroupId` – Smallint (The login user belongs to this group)
3. `UsrGroupLs` – Varchar (The login user belongs to these groups [comma-delimited and enclosed in parenthesis])
4. `CultureId` – Tinyint (The login user's culture)
5. `CompanyId` – Smallint (The login user belongs to this company)
6. `CompanyLs` – Varchar (A list of the companies the login user belongs to [comma-delimited and enclosed in parenthesis])
7. `ProjectId` – Smallint (The login user belongs to this Project)
8. `ProjectLs` – Varchar (A list of Projects the login user belongs to [comma-delimited and enclosed in parenthesis])
9. `AgentId` – Integer (The agent's ID, [sales representative, etc.])
10. `BrokerId` – Integer (This is the broker's ID)
11. `CustomerId` – Integer (This is customer's ID)
12. `InvestorId` – Integer (This is the investor's ID)
13. `MemberId` – Integer (This is the ID for the member, employee, etc.)
14. `VendorId` – Integer (This is the vendor's ID)
15. `InputBy` – Integer (This is the user login ID that created the record)
16. `ModifiedBy` – Integer (This is the user login ID that modified the record)

If you want more columns to be permission-managed than the above, simply add them to the table called “CtPermKey” and Rintagi will take care of the rest.

Anyone who has access to the screen/report that retrieves data from a table that does not contain any of the above permission-managed columns may access all the data inside that table.

A user can be designated to ‘view’, ‘add’, ‘update’ and/or ‘delete’ on a particular row. Any column can be designated as “Visible and Enabled for Edit”, “Visible but not Editable”, or “Invisible”.

In summary, the following functionalities are available:

1. One user may have many roles,
2. A user may have different roles within a combination of company, project and application,
3. A user may impersonate many other users and take on their roles,
4. If there is a conflict assigning authorities within a role, the last one takes precedence (pessimistic),
5. If there is a conflict among roles, the one with higher authorities takes precedence (optimistic),
6. Classified information may only be revealed to specified Column Authorities,
7. Approval can be performed only by specified Column Authorities;
8. A user may belong to multiple companies, multiple projects, and multiple user groups,
9. Unlimited hierarchy for companies, projects, etc.
10. Default roles can be overridden in individual screens and reports.

Configuration

Because rights management is integral to Rintagi it is built in to all screens or reports as they are generated. Row Authority is used to authorize access to row information; Column Authority is used to authorize column information. Together they form the role(s) for a user.

Adding a Company

Mandatory: Rintagi must find at least one company in this table. During installation one company is installed into the table named “Company”. This table is inside the database with a name that ends with “Cmon”. A screen has not yet been established for this table because more columns can be added to this table. For the present, use the “fire-host-mode” of the SQL Server Management Studio to add more companies to this table.

Adding a Project

Optional: As with adding companies, projects can be added via the “fire-host-mode” of the SQL Server Management Studio. Use this same procedure for adding to the Customers, Vendors, Agents, Brokers, etc. tables.

Default Row Authority

Mandatory: One and only one row must be checked as the Administrator of this table. Any additional user-defined Default Row Authorities must be assigned to User Groups as roles.

Appropriate permissions are:

1. All
2. None
3. Self

Default Row Authority

Command: Rule Tier -> Authorization -> Row Default

Row Authority Default

Export RichText Undo All Save ?

20 1 of 1 Filter All On

Authority ID	Row Authority Description*	Select*	Add*	Update*	Delete*	Administrator*	Pwd Override	User*	User Group*	Culture*	Company*
9	Administration Special	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		All	All	Self	All
8	All access	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Administrative Override	All	All	Self	All
7	No access	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		None	None	Self	None
4	View all and Edit	All	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		All	All	Self	All
6	View all only	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		All	All	Self	All
5	View all, Add, Edit and Delete	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		All	All	Self	All
2	View self and Edit	Self	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Self	Self	Self	Self
1	View self only	Self	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Self	Self	Self	Self
3	View self, Add, Edit and Delete	Self	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Self	Self	Self	Self
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					

Row Authority Default

Export RichText Undo All Save ?

1

Authority ID	User*	User Group*	Culture*	Company*	Project*	Agent*	Broker*	Customer*	Investor*	Member*	Vendor*	Delete
	All	All	Self	All	All	All	All	All	All	All	All	Delete
Administrative	All	All	Self	All	All	All	All	All	All	All	All	Delete
	None	None	Self	None	None	None	None	None	None	None	None	Delete
	All	All	Self	All	All	All	All	All	All	All	All	Delete
	All	All	Self	All	All	All	All	All	All	All	All	Delete
	All	All	Self	All	All	All	All	All	All	All	All	Delete
	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Delete
	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Delete
	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Self	Delete

Schema Characteristic	Description
Authority Id	This internal ID uniquely represents this row authority default.
Row Authority Description	A description of the Default Row Authority (50 characters or less).
Select	The appropriate report and menu permission selection.
Add	Check if this Row Authority allows insertion.
Update	Check if this Row Authority allows updating.
Delete	Check if this Row Authority allows deletion.
Administrator	Check if this is a system administrator Row Authority.
Password Override	User group password required when this authority is selected, if needed.
User	The selected permission for user-related items.
User Group	The selected permission for user-group related items.
Culture	The selected permission for a culture.
Company	The selected permission for company related items.
Project	The selected permission for project related items.
Agent	The selected permission for agent related items.
Broker	The selected permission for broker related items.
Customer	The selected permission for customer related items.
Investor	The selected permission for investor related items.
Member	The selected permission for member related items.
Vendor	The selected permission for vendor related items.

Column Authority Override

Optional: The column default before override is visible, editable and exportable. As screen columns are being defined, the screen column authorities for the default authority are automatically defined. Each column can be designated as non-visible, read-only or non-exportable. Additional column authorities can be added to each column. Moreover, tooltips, labels, error message can also be overridden.

Column Authority Override

Command: Rule Tier -> Authorization -> Column Authority Override

Authority Override (COL)
Export RichText New Copy Undo All Save Delete

Screen: Screen Column Properties

AdmScreenObj 10: ScreenObjId 100 [Default] 1 of 1 Module: Administration

Screen Object*: AdmScreenObj 10: ScreenObjId

Visible: ☒

Non-Editable: ☒

Exportable: ☒

Tool Tips:

Label Override:

Error Message:

Entity Type:

Entity Value:

Priority: 100

This is the label to override the default defined in screen column property.

Schema Characteristic	Description
Screen Object	This is the screen column that requires authority overrides.
Visible	The selected screen column is visible when checked, invisible when unchecked, for the selected entity (described below).
Non-Editable	The selected screen column is non-editable when checked, editable when unchecked, for the selected entity (described below).

Exportable	The selected screen column is exportable when checked, non-exportable when unchecked, for the selected entity (described below).
Tooltips	The assigned tooltips for the selected screen column is used when this is empty, otherwise this will take precedence for the selected entity (described below).
Label Override	The assigned label for the selected screen column is used when this is empty, otherwise this will take precedence for the selected entity (described below).
Error Message	The assigned error message for the selected screen column is used when this is empty, otherwise this will take precedence for the selected entity (described below).
Entity Type	This can be Agent, Broker, Company, Culture, Customer, Investor, Member, Project, User, User Group, Vendor, or any value assigned as authority item in the table CtPermKey. Empty means everyone.
Entity Value	The available value for the selected entity type will show up when the appropriate entity type is selected. Empty means everyone.
Priority	This is the priority in case of conflict. 100 is assigned as default.

Row Authority Override

Optional: Any additional instruction here will override the Default Row Authority (defined previously) when accessing this selected screen or report.

Row Authority Override

Command: Rule Tier -> Authorization -> Row Authority Override

Row Authority Override Export RichText Undo All Save

Screen: Report:

Module:

10 1 of 1 Filter All On

Screen	Report	Row Authority*	Select*	Add*	Update*	Delete*	User*	User Group*	Culture*	Company*	Project*
User Manager		Administration Special	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	All	All	All	All	All
User Manager		View all, Add, Edit and Delete	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	All	All	All	All	All
User Manager		View self, Add, Edit and Delete	Self	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Self	Self	All	Self	Self
User Manager		All access	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All	All	All	All	All

Row Authority Override Export RichText Undo All Save

Screen: Report:

Module:

Culture*	Company*	Project*	Agent*	Broker*	Customer*	Investor*	Member*	Vendor*	Delete All
All	All	All	All	All	All	All	All	All	Delete
All	All	All	All	All	All	All	All	All	Delete
All	Self	Self	Self	Self	Self	Self	Self	Self	Delete
All	All	All	All	All	All	All	All	All	Delete

User Group Configuration

Mandatory: To set up other users at least one user is required and this user should have administrative rights. Every user must belong to one or more user groups. Contents in the grid below shall override the default row and column authorities. If there is a conflict, specific shall override general in the order of (System, Company, Project) and then the last one wins.

User Group

Command: Operation -> Manage User -> User Group

User Group Export RichText New Copy Undo All Save Delete ?

Accountant 1 of 1

UserGroup ID: 2
 User Group Name*: Accountant
 Default RowAuthority*: View all and Edit
 Default ColAuthority*: Default
 Company: robocoder corporat

10 1 of 1 Filter All On

Company	Project	System	Row Authority*	Col Authority*	Default	Delete
		Common Area	View self only	Default	<input checked="" type="checkbox"/>	Delete
		Template	Administration Special	Default	<input checked="" type="checkbox"/>	Delete
robocoder corporation	RC - Test1	Administration	View all only	Default	<input checked="" type="checkbox"/>	Delete
robocoder corporation	RC- Test2	Administration	Administration Special	Default	<input checked="" type="checkbox"/>	Delete
		Administration	View all and Edit	Data Entry	<input type="checkbox"/>	Delete
					<input type="checkbox"/>	Delete

* Contents in the grid above shall override the default row and column authorities specified. If there is a conflict, the last one wins.

Schema Characteristic	Description
User Group ID	An internal ID that uniquely identifies this user group.
User Group Name	The unique User Group Name (50 characters or less).
Default Row Authority	The row authorization to be used as the default.
Default Column Authority	The column authorization to be used as default.
Company	The user group belongs to this company, if applicable.
Company (data grid)	This company may override default authorities.
Project	This project may override default authorities.
System	This system may override default authorities.
Row Authority	This row authority for the selected combination of Company, Project and System for this user group will override the default.

Column Authority	This Column Authority for the selected combination of Company, Project and System for this user group will override the default.
Default	Check when the Column Authority selected is a default for all systems.

Adding a User

Mandatory: The User Manager must be assigned administrative rights in order to set up other users. The user manager screen is composed of three tabs:

1. Main Info
2. Status
3. Represent

User Manager: Main Info

Command: Operation -> Manage User -> User Manager

The screenshot displays the 'User Manager' application window. At the top, there is a toolbar with buttons: Export, RichText, New, Copy, Undo All, Save, Delete, and a help icon. Below the toolbar, there are input fields for 'Email Address', 'User Name', and 'User Group', along with a 'Quick Filter' dropdown set to 'Active Original Users'. The main area shows the 'Main Info' tab selected, with sub-tabs for 'Main Info', 'Status', and 'Represent'. The user details for 'John Doe' (User Id: 57) are displayed. Fields include: Login Name* (John Doe), User Email (John.Doe@robocoder.com), User Name (John Doe), User Groups* (a list with 'Software Specialist', 'Solution Developer', 'Sys. Administrator' selected, and 'Systems Engineer'), User Culture* (U.S. English), Default Company, Default Project, and Default System* (Administration). On the right side, there are checkboxes for 'Internal User' and 'Technical User', and an 'Impersonating*' field set to '1'.

Schema Characteristic	Description
User Id	The internal ID uniquely identifying this user.
Login Name	The unique login name for this user.
User Email	User's email address, if available.
User Name	User's name in full.
User Groups	A list of the user groups that this user belongs to. (User must belong to at least one user group).
Culture	The culture setting for this user.
Default Company	The company to be selected after login.
Default Project	The project to display after login.
Default System	The system to display after login.
Internal User	Check if server-side printers should be made available for this user.
Technical User	Check if a detailed technical error trace should be made available to this user.
Impersonating	Click the appropriate link to view/edit the impersonated user.

User Manager: Status

User Manager

Export RichText New Copy Undo All Save Delete

Email Address: User Name: User Group: Quick Filter: Active Original Users

John Doe

Main Info Status Represent

Failed Attempt: 0

Last Success: Friday, September 19, 2008

Last Failed: Monday, March 24, 2008

Hint Question:




Hint Answer:

Active: ☒




Modified On: 9/19/2008 7:37:55 PM

Schema Characteristic	Description
Failed Attempt	The number of times that this user has failed at login.
Last Success	The last time that this user successfully completed login.
Last Failed	The last time that this user failed to login.
Hint Question	The hint question to be used if password is forgotten. (Hint will be emailed to user).
Hint Answer	The hint answer requiring a match to generate email.
Active	Uncheck this if this user needs to be disabled.
Modified On	The date this user was last modified.

User Manager: Represent

User Manager [Export](#) [RichText](#) [New](#) [Copy](#) [Undo All](#) [Save](#) [Delete](#)   

Email Address: User Name: User Group: Quick Filter: [Active Original Users](#) ▼

John Doe ▼   

[Main Info](#) [Status](#) [Represent](#)

Companies:

Projects:

Investor:

Customer:

Vendor:

Agent:

Broker:

Member:

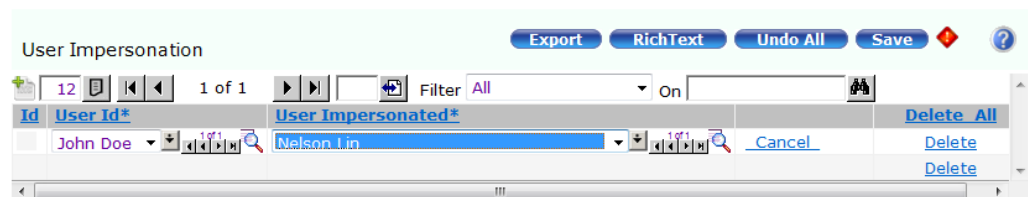
Schema Characteristic	Description
Companies	The user has access to this list of the companies (empty field indicates all companies).
Projects	The user has access to these projects (empty field indicates all projects).
Investor	The user has access to this investor (empty field indicates all investors).
Customer	The user has access to this customer (empty field indicates all customers).
Company	This user group belongs to this company, if applicable.
Vendor	The user has access to this vendor (empty field indicates all vendors).
Agent	The user has access to this agent (empty indicates all agents).
Broker	The user has access to this broker (empty indicates all brokers).
Member	The user has access to this member (empty field indicates all members).

Impersonating a User

Optional: The administrator may designate impersonation capabilities to a user so that he/she would inherit additional rights provided by the impersonated users, including viewing and editing additional data. A supervisor who needs to monitor his/her subordinates will find this useful. In the case of a sudden dismissal, impersonation also enables another employee to take over the duties of the dismissed user temporarily and immediately.

User Impersonation

Command: Operation -> Manage User -> User Impersonation



Report & Import Wizard

For reporting, rights management is automatic on criteria only. Advanced data filtering can be done by passing the following parameters to the Stored Procedure called by the Regular Field Clause (defined in Report Definition):

Parameter	Data Type	Description
@Usrs	varchar(1000)	Advanced: A list of the current login user ID, UsrId, followed by the impersonated UsrId, if any, delimited by CHAR(191).
@RowAuthoritys	varchar(1000)	Advanced: A list of the current login row authority ID, followed by the impersonated row authority ID, if any, delimited by CHAR(191).
@UsrId	int	The user ID of the current login.
@usrName	nvarchar(50)	The username of the current login user.
@currCompanyId	smallint	The current company ID.
@wClause	varchar(4000)	The simplest form of this is “WHERE 1=1” but it may also contain a special filter rule defined in the client tier.

Warning: Anyone having access to any import wizard may import data to the designated tables.