



Compuware  
Optimal Trace™

## Optimal Trace™ Enterprise Admin Tool 5.1 Users Guide

**August 2008.**

### Restricted Rights Notice

This document and the product referenced in it are subject to the following legends:

Access is limited to authorized users. Use of this product is subject to the terms and conditions of the user's License Agreement with Compuware Corporation.

© 2001–2008 Compuware Corporation. All rights reserved. Unpublished – rights reserved under the Copyright Laws of the United States.

U.S. GOVERNMENT RIGHTS-Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in Compuware Corporation license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii)(OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable. Compuware Corporation.

This product contains confidential information and trade secrets of Compuware Corporation. Use, disclosure, or reproduction is prohibited without the prior express written permission of Compuware Corporation.

### Trademarks

© 2008 Compuware Corporation. Optimal Trace™ is a registered trademark of Compuware. All rights reserved. All other trademarks are the property of their respective owners.

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>PREFACE</b> .....   | <b>3</b>  |
| 1.1      | Audience.....  | 3         |
| 1.2      | Conventions used in this document .....                            | 3         |
| 1.3      | Contacting Optimal Trace Customer Support .....                    | 3         |
| <b>2</b> | <b>INTRODUCTION TO THE OPTIMAL TRACE ADMINISTRATION TOOL</b> ..... | <b>4</b>  |
| 2.1      | Installing the Optimal Trace™ Enterprise Administration Tool ..... | 5         |
| <b>3</b> | <b>STARTING &amp; LOGGING INTO THE ADMINISTRATION TOOL</b> .....   | <b>6</b>  |
| 3.1      | Running the Administration Tool .....                              | 6         |
| 3.2      | Logging into the Administration Tool .....                         | 6         |
| 3.3      | Configuring the Administrator Settings .....                       | 7         |
| <b>4</b> | <b>SCREEN LAYOUT</b> .....   | <b>8</b>  |
| <b>5</b> | <b>FILE MENU</b> .....   | <b>9</b>  |
| 5.1      | Synchronizing Projects Option .....                                | 9         |
| 5.2      | Show/Hide Project Baselines .....                                  | 9         |
| 5.3      | Save Option .....  | 10        |
| 5.4      | Monitor Connected Users Option .....                               | 10        |
| <b>6</b> | <b>USERS IN OPTIMAL TRACE</b> .....                                | <b>11</b> |
| 6.1      | Add User Option .....  | 11        |
| 6.2      | Delete User Option.....  | 12        |
| 6.3      | Working with Users .....   | 13        |
| 6.4      | Setting Users Passwords .....                                      | 13        |
| <b>7</b> | <b>GROUPS IN OPTIMAL TRACE</b> .....                               | <b>14</b> |
| 7.1      | Add Group Option .....   | 14        |
| 7.2      | Delete Group Option.....   | 15        |
| 7.3      | Working with Groups.....   | 15        |
| 7.3.1    | Multiple Group Membership & Permissions.....                       | 16        |
| <b>8</b> | <b>SETTING PERMISSIONS ON PROJECTS AND PACKAGES</b> .....          | <b>17</b> |
| 8.1      | Security Enabling a Project.....                                   | 17        |
| 8.1.1    | Setting Permissions while Users are connected .....                | 17        |
| 8.2      | Setting Project Level Permissions.....                             | 18        |
| 8.3      | Setting Package Level Permissions .....                            | 20        |
| 8.4      | Removing Security & Permissions from Projects.....                 | 21        |
| 8.5      | Permission Approaches & Common Deployment Techniques .....         | 21        |
| 8.5.1    | Pessimistic Permissions .....                                      | 21        |
| 8.5.2    | Optimistic Permissions .....                                       | 22        |
| 8.5.3    | Locking down Project Baselines.....                                | 22        |
| 8.6      | Permissions Precedence .....                                       | 23        |
| <b>9</b> | <b>DELETING SERVER LOG FILES</b> .....                             | <b>24</b> |

---

## 1 Preface

This manual is a User's Guide for the Optimal Trace™ Enterprise Administration Tool. The Administration Tool ships as part of the Optimal Trace Enterprise Installation and is used to set up and configure Access Control in Optimal Trace. This involves creation of Groups, Users and Permissions on Optimal Trace Enterprise Projects.

### 1.1 Audience

This document is suitable for Optimal Trace Administrators who are responsible for setting appropriate permissions on projects as well as configuring appropriate sets of users and groups.

### 1.2 Conventions used in this document

This section describes conventions used in this document.

1. **Notes** are used to highlight aspects of usage which may be of interest for specific activities, for example:

|                                     |
|-------------------------------------|
| <b>Note:</b> This is a sample note. |
|-------------------------------------|

2. **Tips** are used to highlight tips which may be of interest for specific activities, for example:

|                                   |
|-----------------------------------|
| <b>Tip:</b> This is a sample tip. |
|-----------------------------------|

### 1.3 Contacting Optimal Trace Customer Support

For all technical problems and support queries, please logon to frontline at <http://frontline.compuware.com/products/ci/> Frontline contains the Optimal Trace forum as well as a FAQ area. Additionally, full up to date release information and contact numbers are provided.

Compuware telephone customer support can be contacted in the U.S. on 1-800-538-7822.

---

## 2 Introduction to the Optimal Trace Administration Tool

The Optimal Trace Administration Tool provides a highly flexible approach to Access Control allowing permissions to be set for Groups of Users and individual Users on given Optimal Trace projects, project baselines or project & baseline packages.

This ensures that project stakeholders are allowed access and editing capability on appropriate areas of the project or baseline.

Some common usage scenarios include:

- ❑ Allowing project stakeholders such as Business Analysts/Engineering etc. to have certain visibility levels into a project
- ❑ Allowing the 'QA team' to edit the Test Requirements project but have 'read-only' access to the Business Requirements
- ❑ Restricting Engineering teams to editing certain Packages or Groups of Requirements.
- ❑ Locking down 'reference' projects for use throughout the organization
- ❑ Locking down the Glossary in a project.
- ❑ Locking down archived (backups) of projects ensuring no changes can be applied.
- ❑ Locking down a Baseline so that nobody can edit it.
- ❑ Restricting 'Open' Access to sensitive projects.

Specific capabilities facilitated by the Administration Module are:

- ❑ The ability to security-enable specific projects and baselines.
- ❑ The ability to create Groups, Users and Permissions for specific Projects, Packages, the Project Glossary and Custom Properties for different parts of a project.
- ❑ The ability to configure certain users as Optimal Trace 'Administrators'
- ❑ The ability to use the same User Group structures for multiple projects.
- ❑ The ability to work offline and merge projects back to the repository, obeying appropriate permissions.
- ❑ The ability to monitor users connected to specific projects.
- ❑ The ability to purge log files on the server

Groups of users can be set up with specific permissions for given projects (or Baselines) allowing them to view or edit projects and sub-components. Projects can also be set as secure or left open, the latter case meaning that there is no security set on the project.

When the Optimal Trace Enterprise user attempts to open a given 'security-enabled' project, the user's permissions are validated by the server software which resides on the Optimal

---

Trace Server. Levels of permissions dictate the perspective the client has and the level of access permitted.

Optimal Trace clients working with offline projects can change them at will, however permissions are checked on initiating a merge to a corresponding repository project.

**Tip:** On dialog boxes with columns, click the edge of a column to adjust the width. Optimal Trace retains the width. Therefore, when navigating between screens, column width remains the same as you changed it.

## **2.1 Installing the Optimal Trace™ Enterprise Administration Tool**

Optimal Trace Administrator is installed as part of both the Optimal Trace™ Enterprise Server and Optimal Trace™ Enterprise installations. For more details, see the *Optimal Trace Installation and Configuration Guide*.

---

### 3 Starting & Logging into the Administration Tool

You can run the administration tool on any machine on which Optimal Trace Enterprise is installed.

#### 3.1 Running the Administration Tool

To run Optimal Trace™ Enterprise Administration Tool, from the Start menu move through Programs/Compuware/Optimal Trace Enterprise Server <Version No>/Optimal Trace Administrator Tool <Version No>. Equally you can run the administrator from the client using the same approach.

A splash-screen will appear and the Optimal Trace™ Administration Tool will load.

**Note:** If you did not use the default locations when you installed the software, then navigate to the directory where the software is installed and click on the Optimal Trace Admin Tool icon in the Optimal Trace Enterprise Server subfolder.

#### 3.2 Logging into the Administration Tool

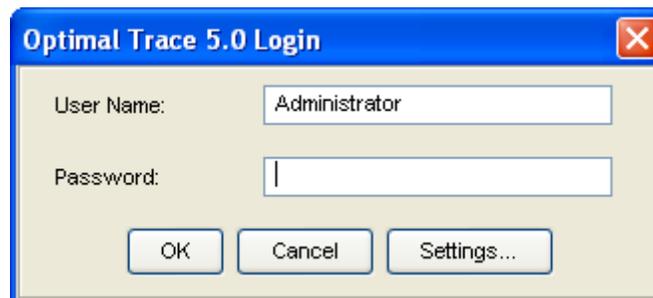
To access the administration tool, you must use log in with administrative privileges.

Out of the box, there is always a user called 'Administrator' with password 'password'. (See the note below for more details)

**Note: First time usage and the 'Administrator' user.** For convenience, Optimal Trace ships with a user called 'Administrator'. This is a special user that cannot be removed. This user has an initial password called 'password'.

For security reasons, it s strongly recommended to adjust this password after initial logon.

You are presented with a screen in Figure 1 - Login Screen below.



**Figure 1 - Login Screen**

As mentioned, on first usage you will use the 'Administrator' user name with default password. You will also want to configure the settings.

### 3.3 Configuring the Administrator Settings

The Administration tool needs to know where the location of the Optimal Trace server is as well as associated settings. This is in order to retrieve and update the administrative settings for that server. These details are specified in the settings screen.

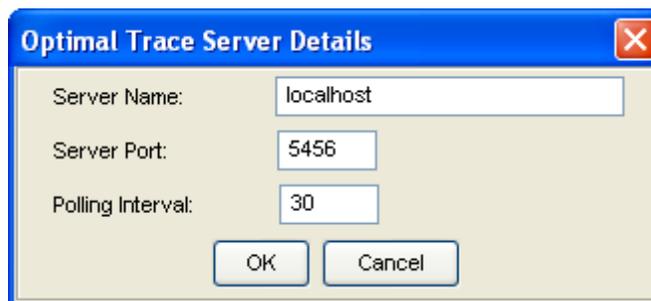


Figure 2 - The Settings Screen

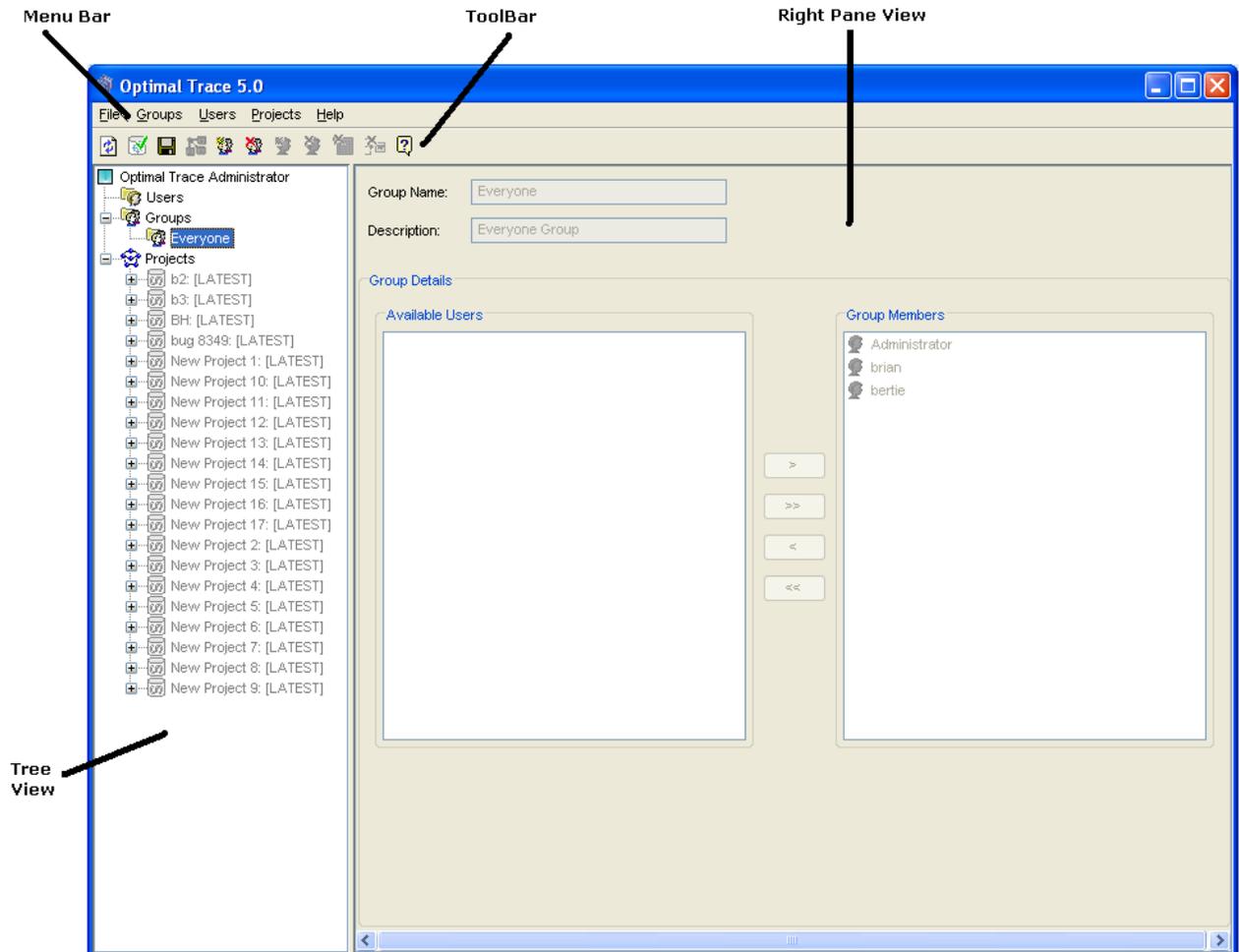
Enter your Server settings as per Table 1. Once you are happy with the settings, hit 'OK'.

Table 1 - Server Settings

| Item             | Description  |
|------------------|--|
| Server Name      | Enter the name for the Repository Server. On a standard network this will be the machine name where Optimal Trace™ Enterprise Server is running. If your Repository Server is running on your local computer, you can type 'localhost' in place of the computer's network name. Alternatively if you know the IP address of the server you can enter this. |
| Server Port      | Enter the port number that the Repository Server is running on. Ensure that this number matches the setting on the Optimal Trace Server. See the Optimal Trace Server help file for more details on setting this. By default both the server and client side settings are set to 5456.   |
| Polling Interval | This is the time setting that controls how often the administration tool queries the server for updates. You can adjust this upwards if you wish to have less frequent polling from client to server.  |

## 4 Screen Layout

Once you are logged into the Optimal Trace™ Administration Tool, the screen shown in Figure 3 - Optimal Trace™ Administration Tool General Layout appears.



**Figure 3 - Optimal Trace™ Administration Tool General Layout**

The screen above is comprised of the following sections:

- **Menu Bar** – i.e. the Main menu, containing menus, submenus, and options that can be used when working with the Optimal Trace™ Administration tool.
- **Tool bar** - contains a list of frequently used items that can be used when working with the Optimal Trace™ Administration tool.
- **Tree View** - contains the list of Users, Groups and Server based Projects.
- **Right Pane View** - contains specific detail relevant to the element selected in the Tree View.

---

## 5 File Menu

Use the File Menu to synchronize projects from the Admin Tool, save changes made and Monitor clients connected to given projects.

- From the Menu bar, click on File

### 5.1 Synchronizing Projects Option

As new Optimal Trace Projects can be created or removed from the repository after you have started the Administrator tool, you may occasionally need to refresh the project list. This may also be necessary if projects have had their package structure modified.

To synchronize the full list of projects:

- In the toolbar click on the  button.

**Note:** This option is also available by right clicking on a Project in the Tree View or through the 'Projects' menu.

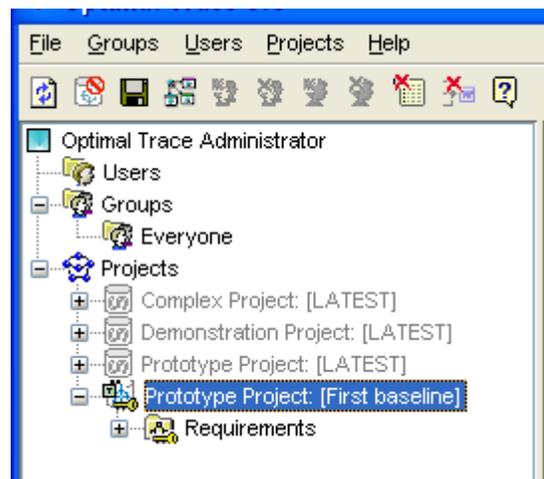
### 5.2 Show/Hide Project Baselines

Optimal Trace projects may have associated Project Baselines. By default when you open the Administrator tool Baselines do not show.

To display Baselines:

- In the toolbar, click on the  button.

As a result the baselines show in the Tree similar to: Figure 4 - Baselines showing in the Tree.



**Figure 4 - Baselines showing in the Tree**

To hide Baselines:

- In the toolbar, click on the  button.

---

### 5.3 Save Option

Use this option to save any modifications you have made to the configuration for Groups, Users or Permissions.

- From the Menu bar, click on File
- Click on the Save button.

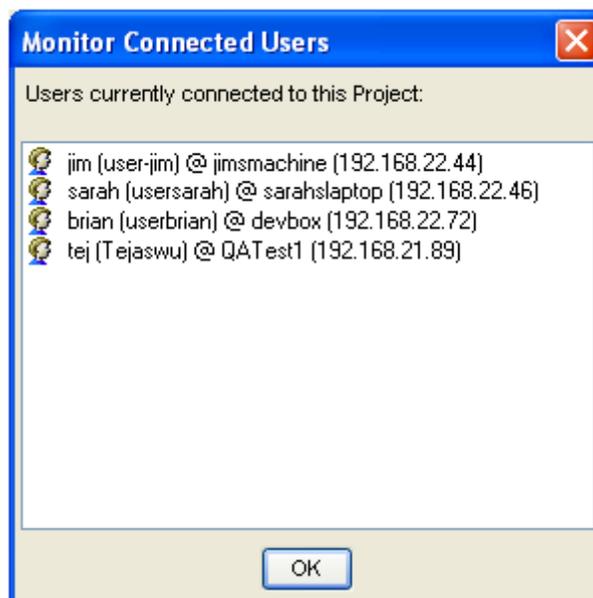
### 5.4 Monitor Connected Users Option

When setting permissions on a given project you may want to first check who is currently connected to that project.

Clicking the option will allow you see if anyone is currently connected.

- Select the Project you are interested in and from the Menu bar, click on 'File'
- Click 'Monitor Connected Users'

You are presented with the list of currently connected users as shown in: Figure 5 : Message Showing Users Currently Editing Project



**Figure 5 : Message Showing Users Currently Editing Project**

**Note:** This option is also available by right clicking on a Project in the Tree View or through the 'Projects' menu.

---

## 6 Users in Optimal Trace

The Users menu allows you create or delete specific Users in Optimal Trace. Only Users defined in the Administration tool can access secure projects. Users can be members of one or more Groups. Groups are used to collect users that have the same permissions on projects and/or packages. See section 7.3 Working with Groups for more on Groups.

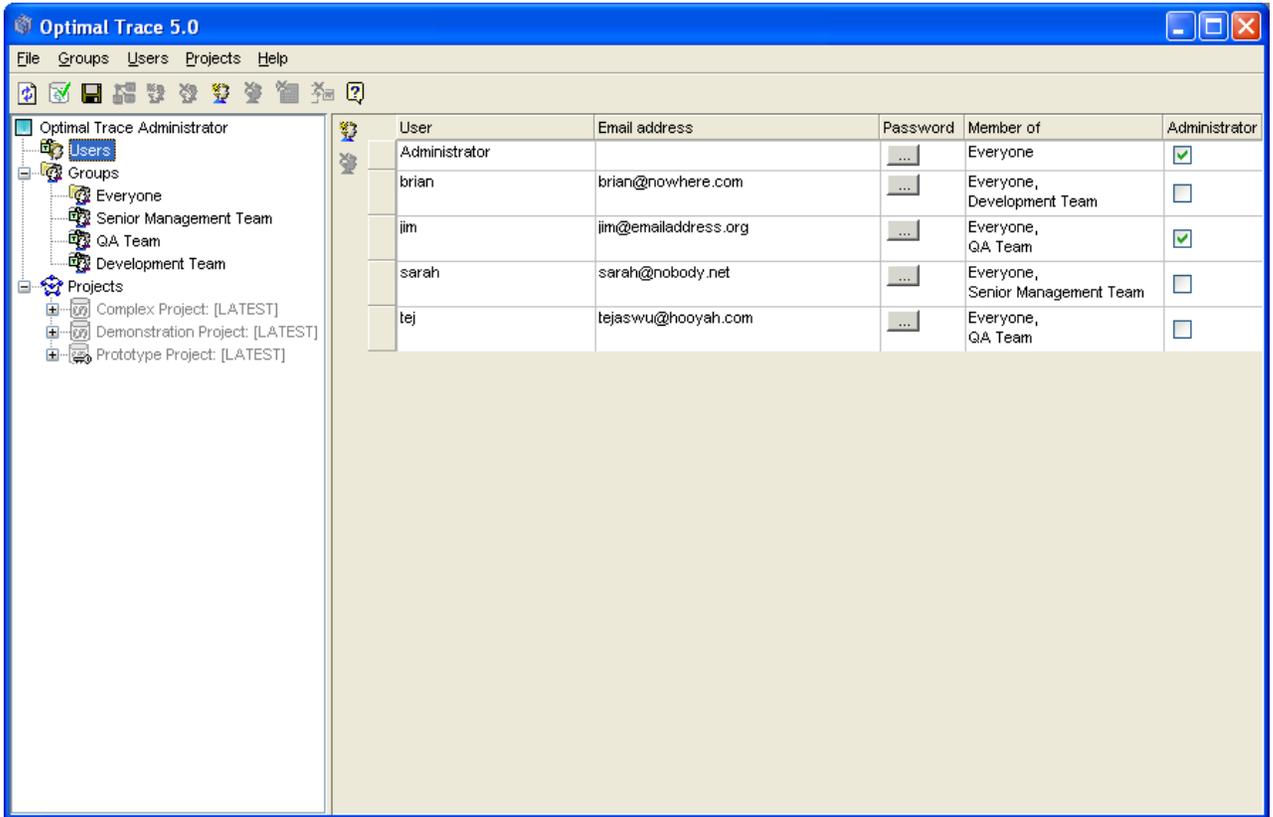
Users can also be directly associated with a given project, having permissions on that project or the project's packages without being a part of a Group. See section 8 Setting Permissions on Projects and Packages for more on permission assignments for Groups and Users.

Finally users can be set as 'Administrators'. Only users with this permission setting can run the administration tool thus allowing them edit permissions or otherwise administer Optimal Trace.

### 6.1 Add User Option

Use this option to create a new User. Users can be members of multiple Groups

- Select the 'Users' entry in the Tree View at which time all the current Users are displayed in the Detail View as shown in Figure 6 - List of Users showing Group membership.
- You can create Users from the Menu bar or using the  button in the main or context specific Toolbar.



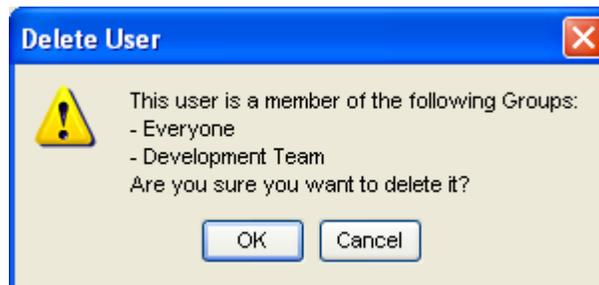
**Figure 6 - List of Users showing Group membership**

## 6.2 Delete User Option

Use this option to delete a User.

- Select the specific user that you want to delete. To do this you must highlight the User by clicking the button to the left of the entry and then click on the Delete User button. Alternatively use the menu option under 'Users'.

If you try to delete a User that is contained within a Group other than the everyone group, you will be prompted to confirm the deletion. A message appears as Figure 7 - Delete User Prompt in below.



**Figure 7 - Delete User Prompt**

---

**Note:** A reserved user called 'Admin' always exists in an Optimal Trace deployment. You cannot delete this user.

### 6.3 Working with Users

Each User comprises:

- **User Name** – The name of the User.
- **E-mail address** - The e-mail address of the User. This is used to allow users to be notified of changes made for registered project changes. See the Optimal Trace Enterprise Help manual for how to register for notifications.
- **Password** - The password for this user. The Password can be changed by clicking on the '...' button.
- **Administrator** - This setting means that this user can log into the Optimal Trace Administration tool and configure groups, users and permissions.
- A list of Groups that the user is a member of is also displayed.

### 6.4 Setting Users Passwords

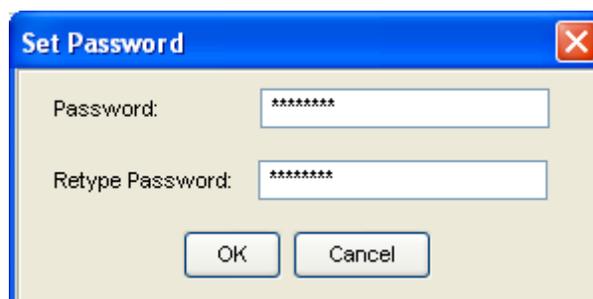
When you set up users it is good practice to change the password. Passwords can be changed in two places, from within the Administration tool or alternatively via the Optimal Trace client.

**Note:** By default when a user is first created it will acquire the password: 'password'.

See the relevant section in the Optimal Trace Enterprise help for details on how to change password directly from the Optimal Trace Enterprise. Common practice is to inform users by mail once they are set up advising them to change their password. They can then do this directly from within the client.

To change the password from the Administration tool:

- Select the specific user. To do this you must highlight the User by clicking the button to the left of the entry and then click on the '...' button.
- Now you will see a screen similar to Figure 8 - Setting a User's Password
- Set the user's password directly in the fields provided. Once happy with the password entered, click the 'OK' button.



**Figure 8 - Setting a User's Password**

## 7 Groups in Optimal Trace

Within an Optimal Trace deployment, Groups represent sets of users with the same access rights. In general these users will have similar permissions on a given set of one or more projects and will tend to be part of specific teams, for example the Business Analysts or Q/A Team.

Use the Groups menu to create, or delete specific Groups of Optimal Trace Users.

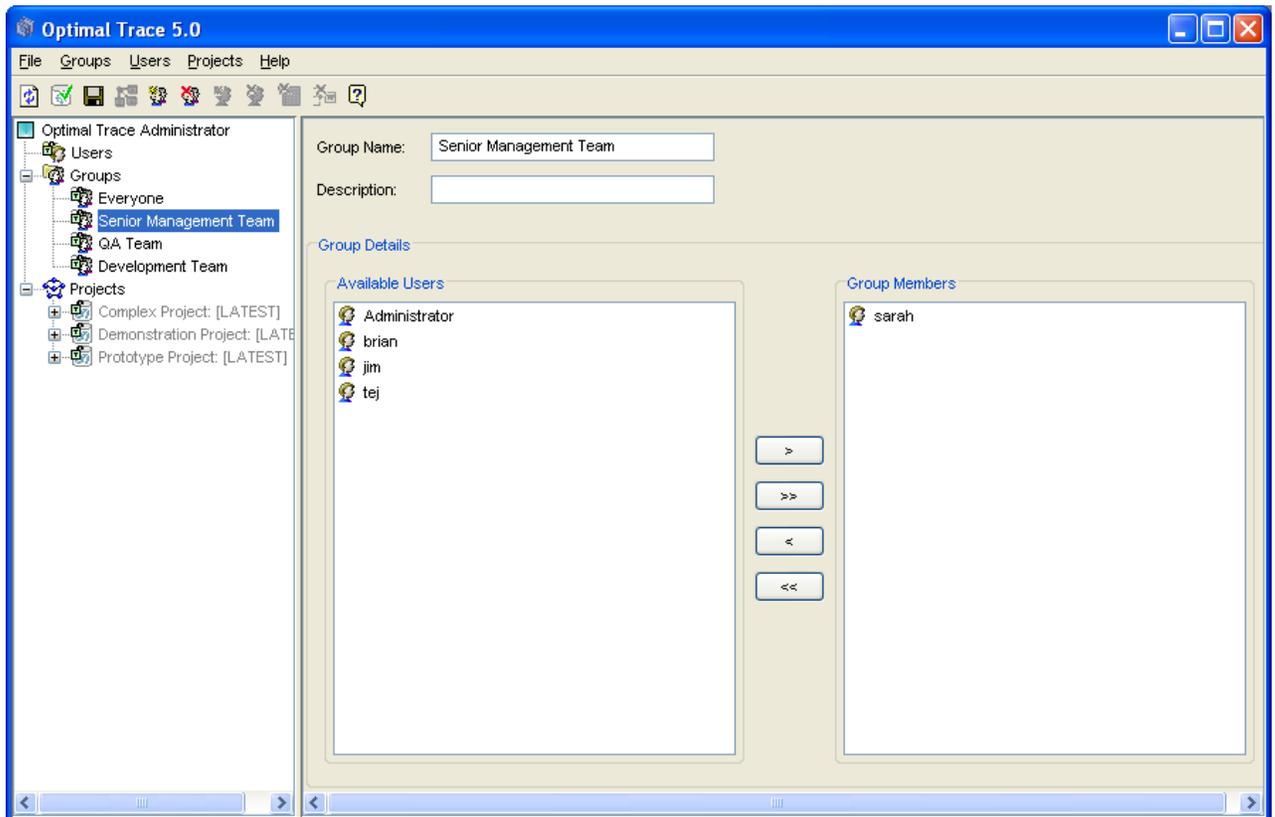


Figure 9 - Groups in Optimal Trace

### 7.1 Add Group Option

Use this option to set up a new Group. You would likely group users into teams such as Business Analysts, QA, and Engineering etc. There is however no restriction on the number of Groups you can create.

**Tip:** Sometimes you may want to have the same team work on multiple projects at the same time with different permission levels. For example, a shared QA Team might work on 'Test Spec Project A' and 'Test Spec Project B' with read only access to A and write access to B. In this case you would likely set up two groups the first would be 'QA Team - A' the 2<sup>nd</sup>: 'QA Team - B'. You would then assign these teams appropriate permission levels.

- 
- Select the 'Groups' entry in the Tree View
  - From the Menu bar, click on Groups and the screen shown in Figure 10 - The Groups Menu will appear.
  - Click on Add Group, the screen shown in Figure 9 - Groups in Optimal Trace will appear.



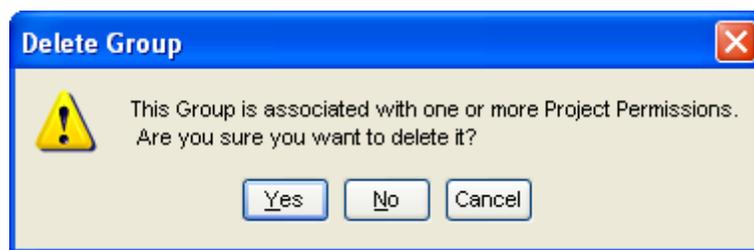
**Figure 10 - The Groups Menu**

## 7.2 Delete Group Option

Use this option to delete a Group.

- Select the specific group that you want to remove in the Tree View.
- From the Menu bar, click on Groups and Click on Delete Group.

If you attempt to delete a Group that has an association with a project then you are prompted to confirm the deletion. A message appears as Figure 11 - Delete Group Prompt in below.



**Figure 11 - Delete Group Prompt**

## 7.3 Working with Groups

Each Group comprises:

- **Group Name** – The name of the Group.
- **Group Description** - a more detailed outline of the Group.
- **Group Members** - This represents the Users that are contained in this group. These users can be added or removed from the Group. Each Group will contain a set of zero or more users. Use the '>' button to add a selected User to a Group. Use the '<' button to remove a User from a Group. The '>>' and '<<' buttons add or remove all users respectively.

---

**Note: The 'Everyone' Group.** For convenience, Optimal Trace ships with a Group called 'Everyone'. This is a special Group that contains all users. You cannot remove users from the Everyone group.

Each project that becomes security-enabled (see section 8.1 Security Enabling a Project) automatically has a 'modify' capability set for the Everyone group. This means that when you initially switch a project to be security-enabled, Everyone will be able to modify that project.

For more on setting Project Permissions see section 8.

### **7.3.1 Multiple Group Membership & Permissions.**

Optimal Trace allows a given User to be a member of more than one Group. In reality, each User will tend to have membership in at least two Groups, the special 'Everyone' group and a more specific Group such as QA etc.

In the case where a user has multiple Group membership and there is a difference in permissions for a given project, then the maximum permission level is applied.

See section Table 2 : Multiple Permissions Matrix for a full matrix outlining Permission Levels for multiple Group membership.

---

## 8 Setting Permissions on Projects and Packages

Optimal Trace Enterprise allows permissions to be set for Projects and Packages. The basic premise behind the Optimal Trace Access Control model is that a project can be security enabled meaning it now adheres to the permissions established for that project.

There are typically a number of approaches taken when considering permissions. These are outlined later in section 8.5 Permission Approaches & Common Deployment Techniques.

**Note: Project Baselines & Permission.** All capabilities applicable to Optimal Trace projects are also applicable to Project Baselines also. You can assume in the following sections that whenever a capability is mentioned with respect to a project, that same capability also is applicable for project baselines.

### 8.1 Security Enabling a Project

Initially all Optimal Trace Repository Projects are non-secure meaning that no permissions are established.

In order to set permissions:

- Select the specific project within the Tree View.
- Click the  button in the vertical toolbar.

**Note:** This option is also available by right clicking on a Project in the Tree View or through the 'Projects' menu.

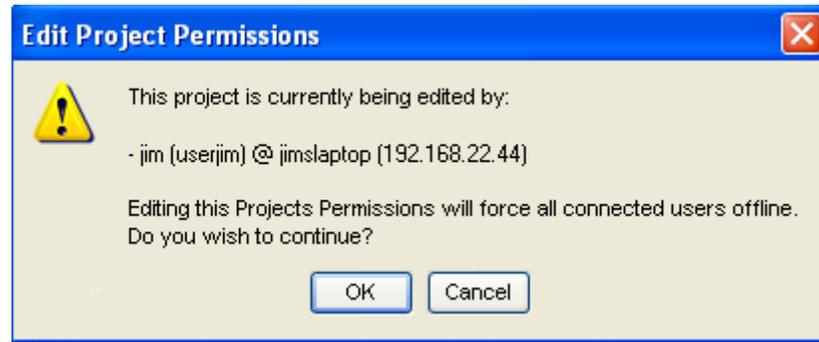
If there are users currently connected to the project then a confirmation message appears. See section 8.1.1 Setting Permissions while Users are connected for more.

Once you start editing permissions on a project the project appears in the Tree View with a key adjacent to the entry. See Figure 14 - Setting Project Level Permissions

#### 8.1.1 Setting Permissions while Users are connected

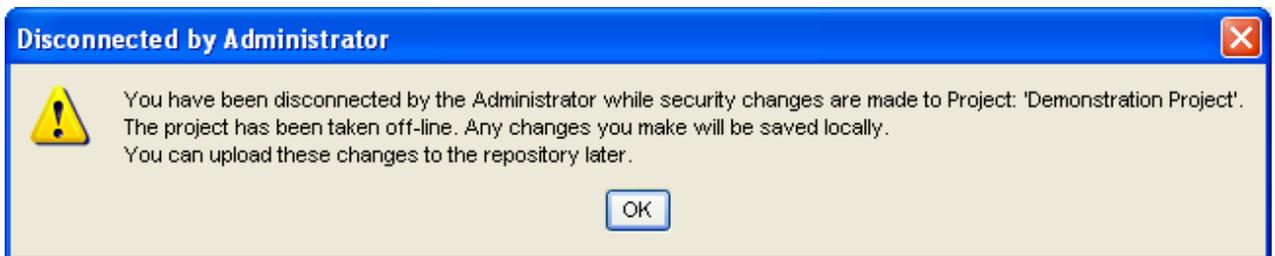
In order to set permissions no users can be connected to that project.

Consequently if you attempt to edit permissions while users are connected you will be informed with a message listing the users and prompting you to confirm your intentions. A screen appears as per Figure 12 - Connected Users when an attempt is made to edit Permissions



**Figure 12 - Connected Users when an attempt is made to edit Permissions**

If you proceed to edit then these connected users will be forced offline with a message appearing for those users similar to Figure 13 - Client side message for users being disconnected. Users are free then to continue editing offline until such time as you have saved any changes made to the permissions.



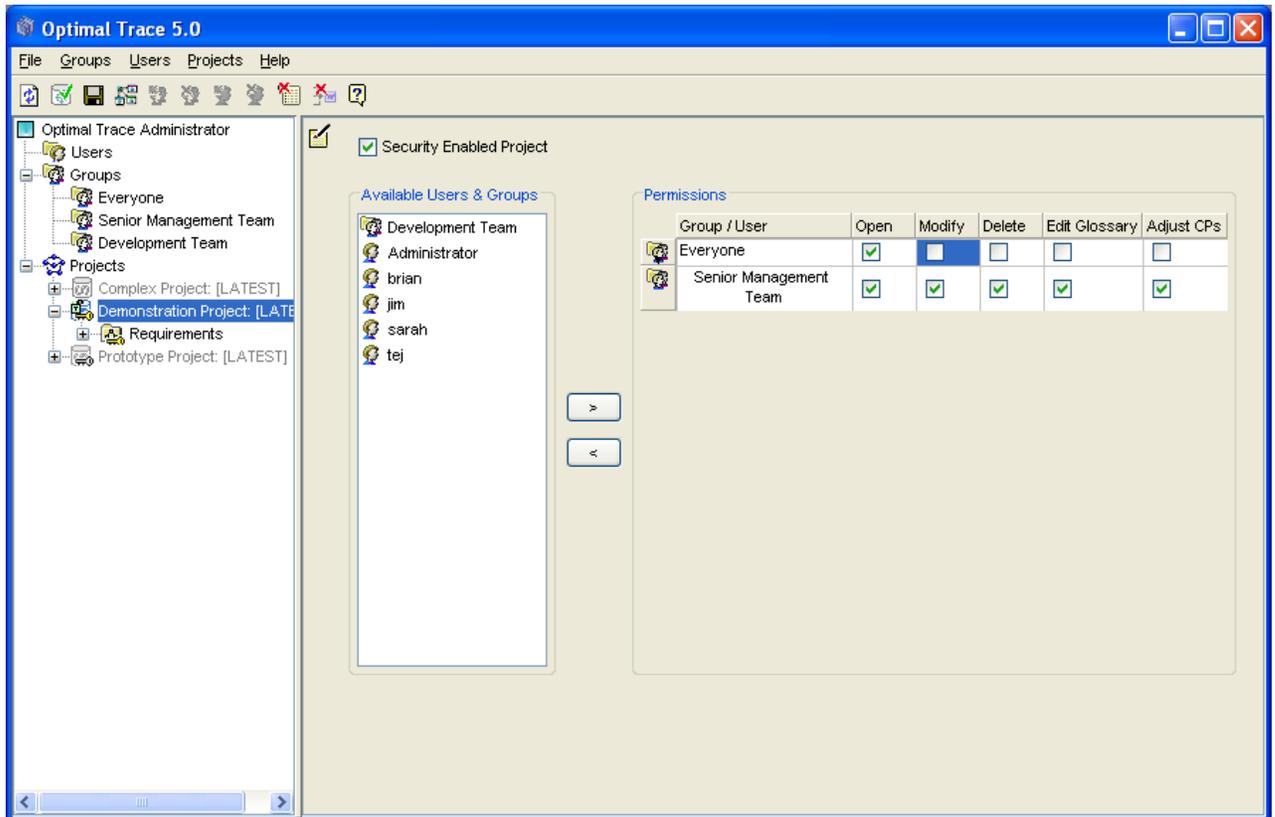
**Figure 13 - Client side message for users being disconnected**

## 8.2 Setting Project Level Permissions

Permissions can be set for Groups or individual Users for each project.

The following Permissions can be set:

- Can Open - allows the project to be opened
- Can Modify - allows the project to be modified/edited
- Can Delete - allows the project to be deleted
- Edit Glossary - allows the Glossary to be modified/edited
- Adjust CPs - allows custom properties defined at the project level to be modified



**Figure 14 - Setting Project Level Permissions**

In order to set Group or User permissions on the project:

- Select the specific Project within the Tree View.
- Select the specific Group or User within the list of 'Available Users & Groups' List.
- Click the '>' button.

This will move the selected Group or User to the permissions area where you can check or uncheck the appropriate permissions for the project.

You can select more than one Group or User by using the CTRL key while clicking the mouse as per normal windows conventions.

Once you set the project permissions, the system prompts you to confirm whether you wish to propagate that permission setting for all contained packages. If you accept the default of 'yes' this will cascade the 'modify' setting for that group or user across contained packages, otherwise the settings will only be for the project level itself.

**Tip:** When security enabling a project for the first time, it is a good idea to uncheck the 'Can Delete' checkbox for the Everyone group. This will then mean that your projects are safe from any accidental deletion.

**NOTE:** A User must have full access rights on a Project to be able to apply a Project Template.

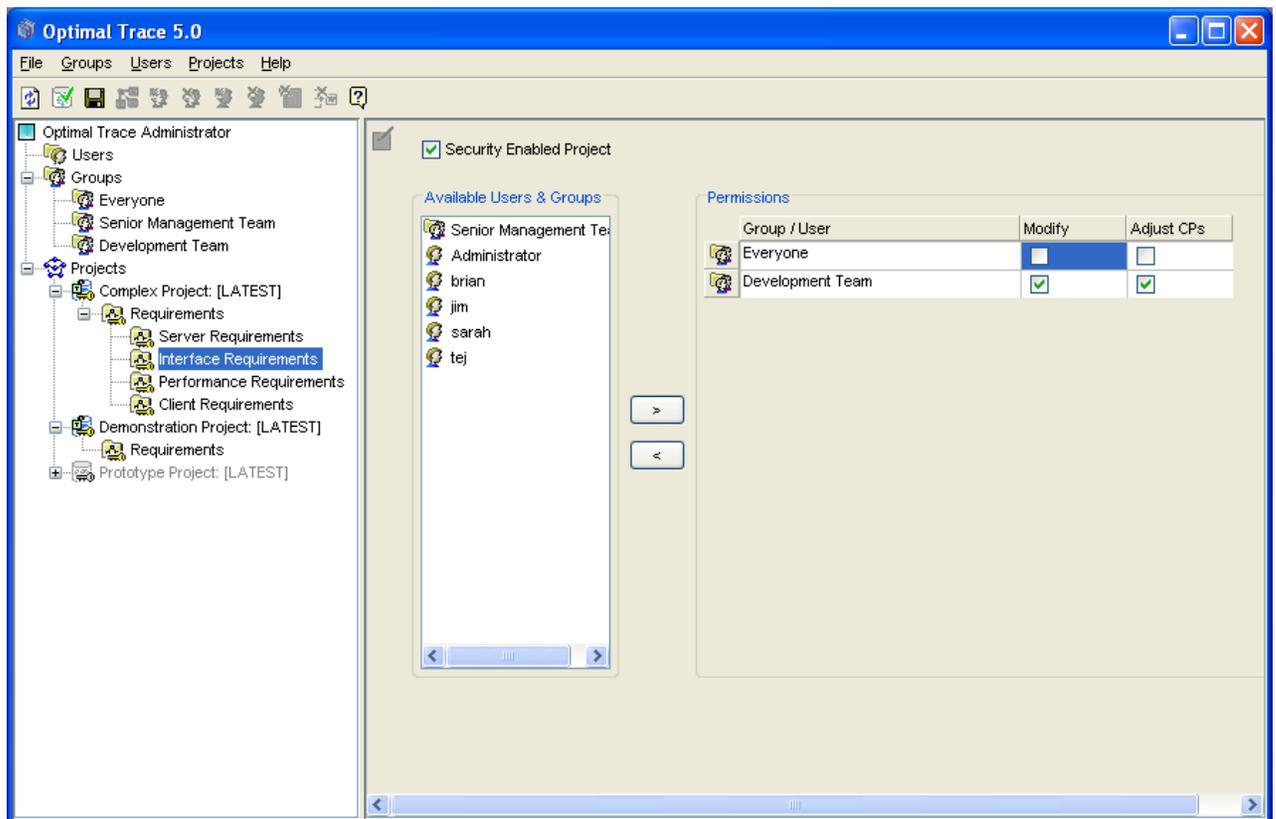
### 8.3 Setting Package Level Permissions

Permissions can be set for Groups or individual Users for each package in the project.

Unlike at the Project Level, Package Level Permissions are set to allow modification for the package. In essence, this means that if a package is marked as modifiable for a specific group or user then that Group or User may edit all aspects of the package. Note that this includes the ability to delete the package if desired.

Package Level Permissions can also be set to allow modifications to Custom Properties for that package. This allows specific groups or users to modify the custom properties used by a package and all aspects of that package. It also allows these users and groups to adjust the 'Share Custom Properties' setting for a package.

As with Projects, for Packages, Permissions can be set for single or multiple Groups or users.



**Figure 15 - Setting Package Level Permissions**

In order to set Group or User permissions on the package:

- 
- Select the specific package within the Tree View.
  - Select the specific Group or User within the list of 'Available Users & Groups' List.
  - Click the '>' button.

This will move the selected Group or User to the permissions area where you can check or uncheck the modifiable permission for the package.

You can select more than one Group or User by using the CTRL key while clicking the mouse as per normal windows conventions.

Once you set the package permissions and if there are child packages then the system prompts you to confirm whether you wish to propagate that permission setting for all contained packages. If you accept the default of 'yes' this will cascade the 'modify' setting for that group or user across the contained (or child) packages, otherwise the settings will only be for the selected package.

#### 8.4 Removing Security & Permissions from Projects

From time to time, you may to decide that it is no longer appropriate to have security set up for a project in this instance:

- Select the specific project within the Tree View
- Click the  button in the vertical toolbar.
- Uncheck the 'Security Enabled' checkbox.

**Note:** When removing security from a project, all permissions settings for the project and any subordinate packages are removed. This action cannot be undone. The system prompts you to confirm this action.

#### 8.5 Permission Approaches & Common Deployment Techniques

Here we outline a number of common usage scenarios for applying Access Control. Depending on your needs one or more of these approaches may be appropriate for your scenario.

##### 8.5.1 Pessimistic Permissions

This scenario assumes that you have a number of groups, say 'QA Team', 'Business Analysts' & 'Engineering' and further that you only want to allow one (or a few) of these groups/users to have edit (or other) capability.

This scenario may reflect a stage in analysis where you have arrived at a solidified version of the project and wish to lock down the majority of the project for the majority of Groups/Users.

- Select the project (in the Tree) for which you wish to apply security.
- Edit the project permissions by clicking the  button in the vertical toolbar.

- 
- The project will by default be open for editing by the group 'Everyone' so uncheck the following:
    - a. Can Modify
    - b. Can Delete
    - c. Edit Glossary
  - Now add the specific Group/User(s) that you wish to set as having 'modify' permissions for either the project or the specific package or packages.

### 8.5.2 Optimistic Permissions

This Scenario assumes that you want to open up the project to the majority of users but want to restrict a selected few. In effect, the default with this approach is that all Users have maximum permissions on the project except for a select number who are explicitly set to not have certain permissions.

- Select the project (in the Tree) for which you wish to apply security.
- Edit the project permissions by clicking the  button in the vertical toolbar.
- The project will by default be open for editing by the group 'Everyone'. Leave this as is.
- Now add the specific Group/User(s) that you wish to set as being restricted.
- Uncheck the 'Can Modify' etc. permissions for the specific restricted Groups/Users as appropriate.

### 8.5.3 Locking down Project Baselines

This scenario assumes that you want to lockdown a given Baseline of a project during Analysis or afterwards such that everyone can open but nobody can edit. The baseline is available for possible rollback at a later time. Additionally it is locked down so that no users can modify however all can review.

In the Optimal Trace Enterprise client do the following:

- Click the 'Project > Baselines > Create Baseline' menu option. Enter a suitable name and description e.g. 'Version 2'

Now in the Administration Tool:

- Synchronize all Projects with the Repository so that we can see the new project baseline. See section 5.1 Synchronizing Projects Option for more on this area.
- Click on the  button to display all baselines. See section: 5.2 Show/Hide Project Baselines for more on displaying baselines.
- Edit the project permissions for '<Project Name> (Version 2)' by clicking the  button in the vertical toolbar.

- The project baseline will by default be open for editing by the group 'Everyone' so uncheck the following at project level for the everyone Group:
  1. Can Modify
  2. Can Delete
  3. Edit Glossary

The Project Baseline can be open by everyone but read-only for all.

### 8.6 Permissions Precedence

Optimal Trace allows users to be members of multiple Groups. Additionally, users can also be directly assigned with permissions without being a member of a Group.

In general the following rule dictates permissions:

**Note: The Permissions & Precedence Rule.** If a User is a member of 2 or more Groups with different permission levels then the maximum allowable permission takes precedence EXCEPT if a user is directly assigned permissions on a given project or package then that permission level takes precedence.

The following table outlines expected behaviour where multiple permission levels are encountered. Assume four Groups; Analysts, QA, Engineering, Managers and 2 users Jill and Paul.

**Table 2 : Multiple Permissions Matrix**

| User   | Is a Member of   | Permission set   | Result              |
|--|--|--|---------------------|
|  Jill |  QA<br> Engineering    | QA: 'Can Modify' = yes<br>Engineering: 'Can Modify' = no                                   | Jill can Modify     |
|  Paul |  Analysts<br> Managers | Analysts: 'Can Open' = no<br>Managers = 'Can Open' = yes                                   | Paul can Open       |
|  Jill |  QA<br> Engineering    | QA: 'Can Modify' = yes<br>Engineering: 'Can Modify' = no<br><i>Jill: 'Can Modify' = no</i> | Jill can NOT Modify |
|  Paul |  Analysts<br> Managers | Analysts: 'Can Open' = no<br>Managers = 'Can Open' = yes<br><i>Paul: 'Can Open' = no</i>   | Paul can NOT Open   |

---

## 9 Deleting Server Log Files

The 'Projects' menu allows the user to delete the 'Change History Log' and the 'Project Update Log' that are stored on the server for the project selected in the tree.

As a project evolves over time, the Change History Log and Project Update Log can become quite large. In some circumstances these files can have an impact on application performance.

The 'Change History Log' contains a list of all changes made to the project. This list can be viewed by looking at the 'Change History' for the project in the Optimal Trace Enterprise Client. If you are experiencing performance problems with a project, deleting the Change History may help to alleviate these problems.

The 'Project Update Log' is used when updating a word document that was previously generated from this project. This log file is used to record all changes that were made since the document was generated, thus allowing the document to be updated. You can safely delete the 'Project Update Log' for a particular project if you do not intend to use the 'Update Document' mechanism in the Optimal Trace Enterprise Client.

**Note:** you can still update documents that are generated after you delete the Project Update Log. However you will be unable to update any older documents, any generated before deleting the Log.