# Chapter 10

# Security

When you have your T.O.M. software fully operational, you will no doubt have several people that will want to have access to the information stored in the T.O.M. databases. Whether you are running T.O.M. from a multiple user network or a single computer, there will be other people at your district that you would like to give the ability to lookup, enter, or change information. The problem, of course, is that you don't want a situation where just anybody can do just anything in your T.O.M. software. This is where T.O.M.'s security feature comes in.

With T.O.M.'s security feature you can tell T.O.M. who can get into T.O.M. and what can they do when they're in T.O.M. This prevents both unintentional mistakes and willful sabotaging of information. There are two parts to T.O.M.'s security:

- **Users security:** The main component of T.O.M.'s security is Users. A user is a person who is authorized to use the T.O.M. software. By entering Users, you are telling T.O.M. both *who* is authorized to run the T.O.M. software and *what* they are authorized to do while running the T.O.M. software.
- **Groups security:** A Group is a shortcut for entering User information. A group is nothing more than a set of permissions that can be copied when entering a User. Groups let you establish sets of common permissions that can be copied to a new user. You can then individualize these permissions for a user as you enter them.

  You may always change the permissions assigned to a User by a Group or you may always reset the permissions of a User to the standard permissions of a Group. ***Remember: Groups are not Users. They are only tool that help you create a User quickly.***

  T.O.M. ships with three pre-loaded groups: Administrator, Clerk and Inquiry. These three sample groups are three common profiles of the type of Users you will most likely set up in you T.O.M. security.

This chapter is divided into these sections:

- **T.O.M. Security for Users.** Explains how to set up user permissions.
- **T.O.M. Security for Groups.** Explains how to set up group permissions.
- **Understanding Permissions.** Describes each of the permissions you can set for users and groups.

ⓘ *T.O.M Tip*

**What if I have other T.O.M products? Also, if there are employees I want to have permissions to all our T.O.M. products, do I have to add the users and their permissions to each application?**

In addition to setting up security for the Employee Management system, you can set up permissions for people using the GIS Routing and Student Conduct applications. You can do this in the Users Permissions screen.

# T.O.M. Security for Users

You can set up the permissions that a user has to the Employee Management, GIS Routing, or Student Conduct software. To save time and prevent errors, you can create user groups and add permissions to each of those groups. Then, when you add users to the system, you can select a user group for that employee.

For example, one default user group is called Administrator. This user group has the permissions that a person who is designated as an administrator should have. When you select Administrator as the user group for a user, those permissions are applied to the user. You can then customize those settings by clicking the Product Permissions button on the User Maintenance screen.

***NOTE: If you do not select a User Group for the user, that user will not have any permissions unless you click the Product Permissions button and permissions to the user.***

This section explains:

- Adding a User
- Understanding the User Maintenance screen
- Customizing a User's Permissions
- Editing or Changing a User to Inactive
- Deleting a User

| | |
|---|---|
| ⓘ ***T.O.M Tip*** | **How do I control the permissions? Where can I learn more about the permissions?**<br><br>When you set up a user, you can assign several permissions to that user by selecting a group of permissions that you assign to that user. To learn more about customizing user permissions and what each permission means, see the<br>Understanding Permissions |

## Adding a User

1. Select Security>Users (Figure 10-1).

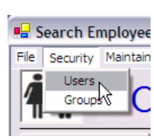



*Figure 10-1. Selecting Security>Users*

The Users screen displays.

2. Click the New button (Figure 10-2).

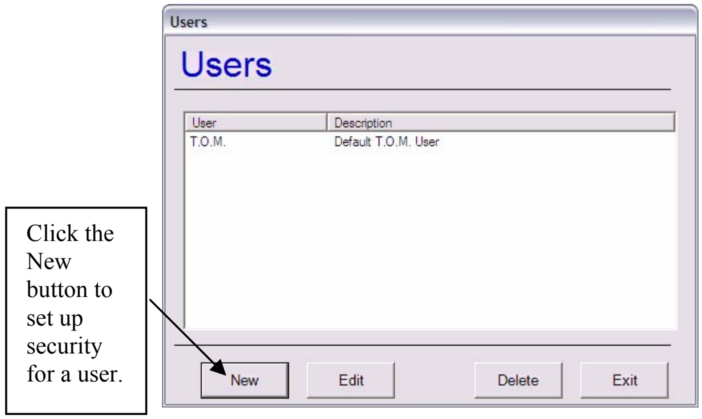



*Figure 10-2. The Users screen*

The User Maintenance screen appears.

3. Complete the screen. (For information about the fields on this screen, see the next section.)

Figure 10-3 shows the security settings for a sample user:

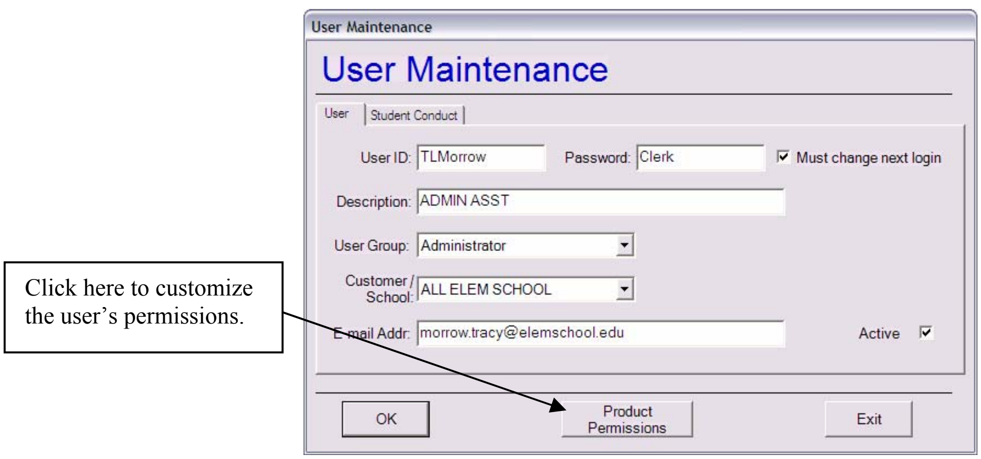



*Figure 10-3. Sample added user*

ⓘ ***T.O.M Tip***

**I selected the User Group for the user, but I wanted to give this particular user access to additional features. Where can I do that?**

To change the default settings the user is given by the User Group you assign them to, click the Product Permissions button on the User Maintenance screen. Then, read the Customizing a User's Permissions        Understanding Permissions

have for customizing user permissions.

## Understanding the User Maintenance screen

When you add users to the system, you will need to complete the User Maintenance screen (Figure 10-4):

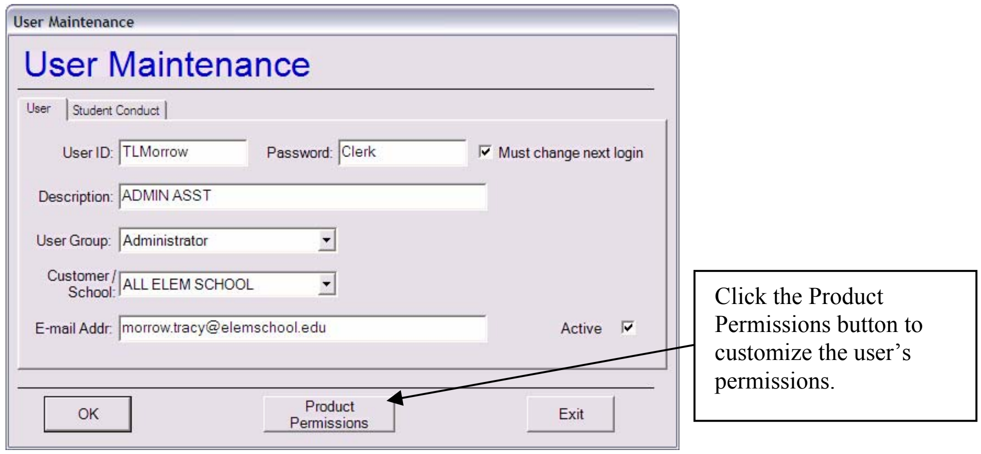



*Figure 10-4. User Maintenance screen*

- **User ID.** Allows you to specify the user identification code that allows the user to log in to the system. You can enter up to 20 alphanumeric characters into this field, meaning you can type letters and numbers. *This is a required field.*
- **Password.** Allows you to specify the password for the user. If you select Must change next login, the user is required to change the default password you typed into Password. You can enter up to 20 alphanumeric characters into this field.
- **Description.** Allows you to type a description for this user. You can enter up to 50 alphanumeric characters into this field.
- **User Group.** Displays the list of user groups added to the system. When you select  user group from the pull-down list, the settings created for that group are applied to this user. (For information about adding groups to the system, see the T.O.M. Security for Groups section. later in this chapter)
- **Customer/School.** This field is used if you have the T.O.M. Field Trip Software.
- **E-mail Addr.** Allows you to enter the user's email address.
- **Active.** When selected, allows the user to have access to the system.
- **Product Permissions.** Allows you to customize the settings that are applied to the user from your selection from the User Group pull-down list. *(If this button is available, click OK to close the screen, and then select the user and click the Edit button on the Users screen.)*

## Customizing a User's Permissions

This section contains information about customizing a user's permissions. If you want to learn what each of the permissions mean, see the Understanding Permissions section later in this chapter.

1. Either:

   - Select the user in the Users screen, and click the Edit button (Figure 10-5) .

   OR

   - Double-click the user.

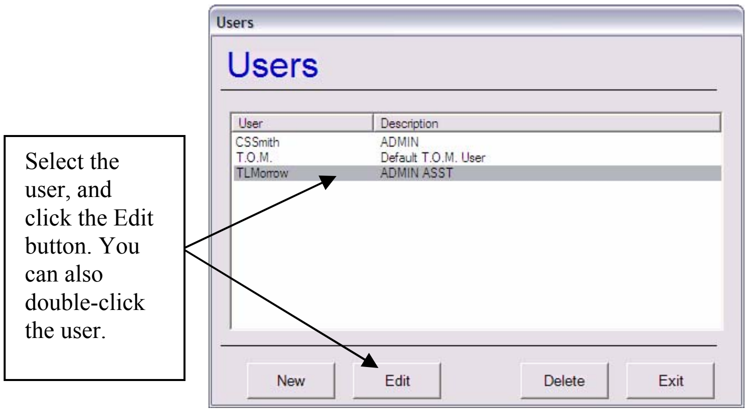



*Figure 10-5. Selecting a user*

The User Maintenance screen displays.

2. Click the Product Permissions button (Figure 10-6)

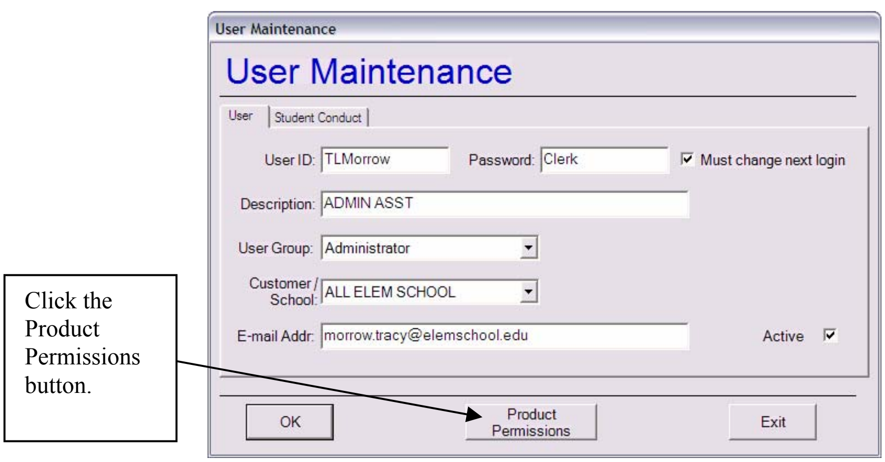



*Figure 10-6. Customizing a user's permissions*

The User Permissions screen displays (Figure 10-7).

3. Select the software product(s) you want to set permissions for, and click the Add button.

***NOTE: To remove permissions, select the software, and click the Remove button.***

4. Click on the product's name in the User's Products box. The permission categories for that product appear in the Permissions box.

5. Click on the + sign in front of a permission to expand the permission list. (For a description of the permissions, see the next section in this chapter.)

6. Click in the boxes in the Authority column to give the selected permission to the user.

***NOTE: You can resize the Description column by clicking in the heading row and dragging it.***

7. Complete the screen.

   Figure 10-7 shows how one user has customized permissions:

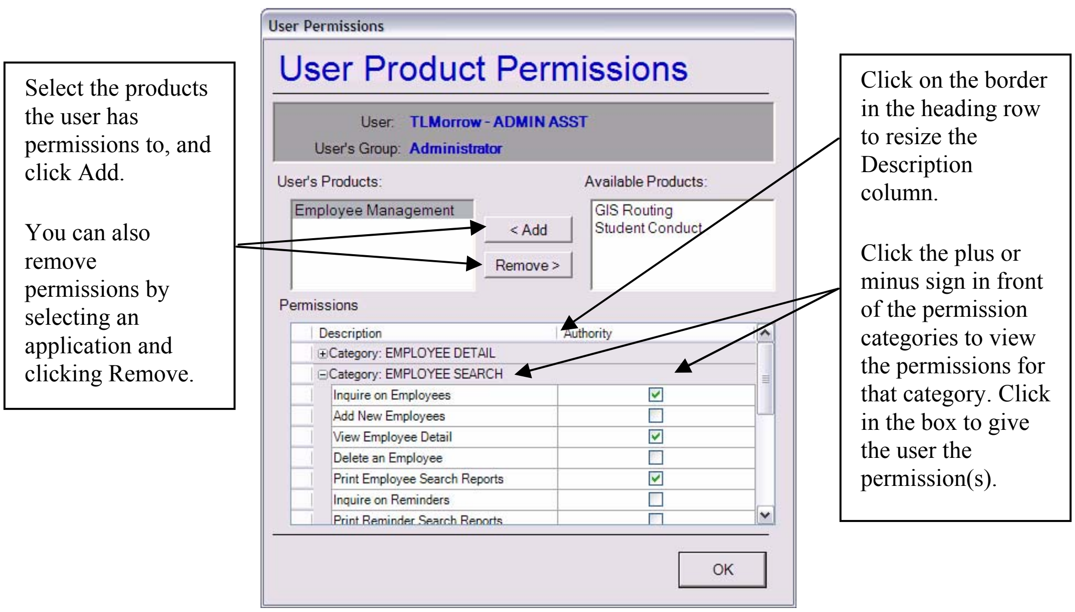



*Figure 10-7. Sample completed User Permissions screen*

## Editing or Changing a User to Inactive

You can easily change a user's permissions. You can delete a user from the system, but if you do that, you are permanently removing that user. You might consider changing the user's status to inactive. That way, that user remains in the system but will be unable to log in.

**To change a user to inactive:**

1. Either:

   - Select the user in the Users screen, and click the Edit button (Figure 10-8) .

   OR
   - Double-click the user.

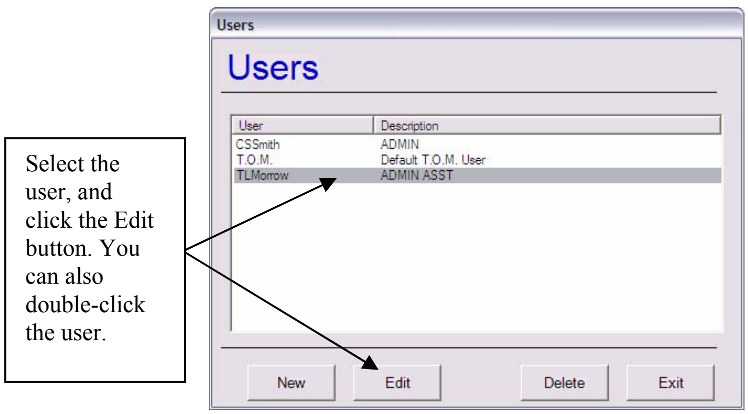



*Figure 10-8. Selecting a user*

   The User Maintenance screen displays.

2. Click the Product Permissions button (Figure 10-9)

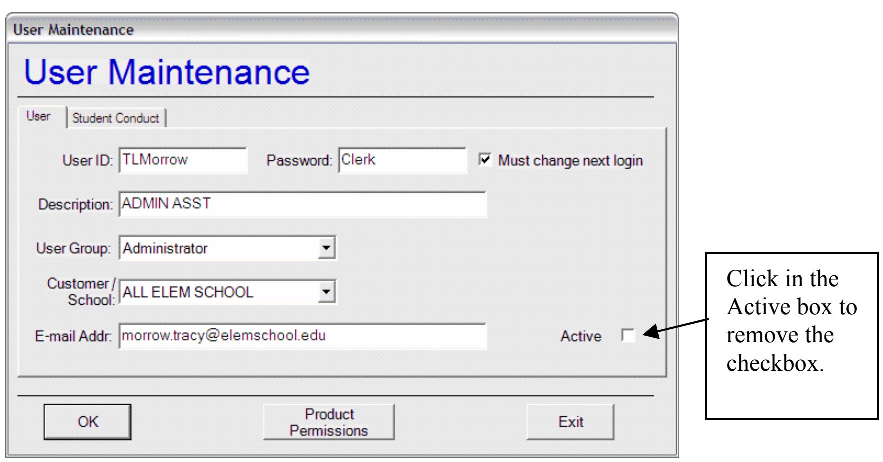



*Figure 10-9. Customizing a user's permissions*

3. Click OK to save your changes.

## Deleting a User

When you delete a user, you are permanently removing that user from the system.

***NOTE: As stated in the previous section, you might want to consider changing the user's status to Inactive. That way, they remain in the system but will be unable to log in.***

1. Either:

   - Select the user in the Users screen, and click the Edit button (Figure 10-10) .

   OR
   - Double-click the user.

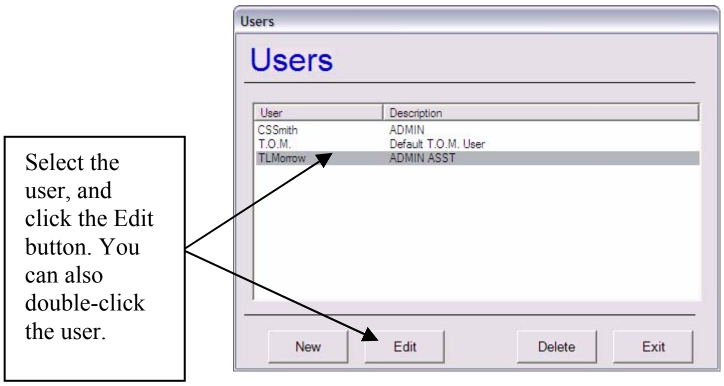



*Figure 10-10. Selecting a user*

2. Click the Product Permissions button (Figure 10-11)

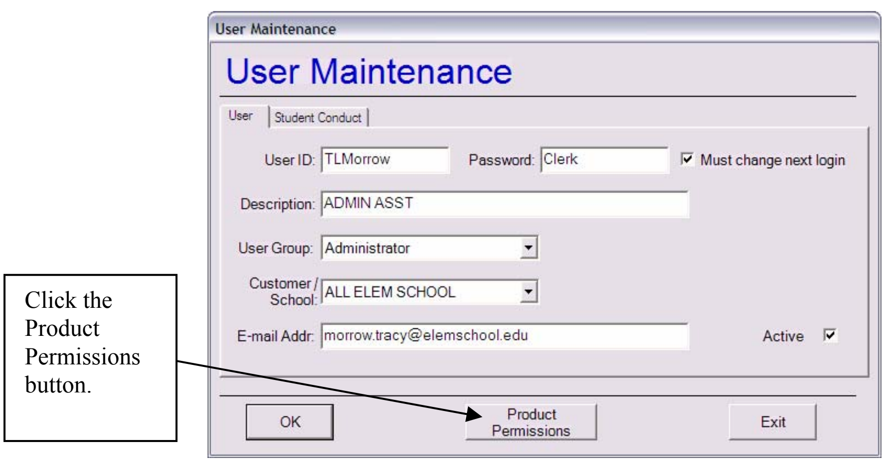



*Figure 10-11. Customizing a user's permissions*

   The User Permissions screen displays.

3. Select the applications in the User's Product box, and click the Remove button. Figure 10-12 shows that the user's permissions have been removed:

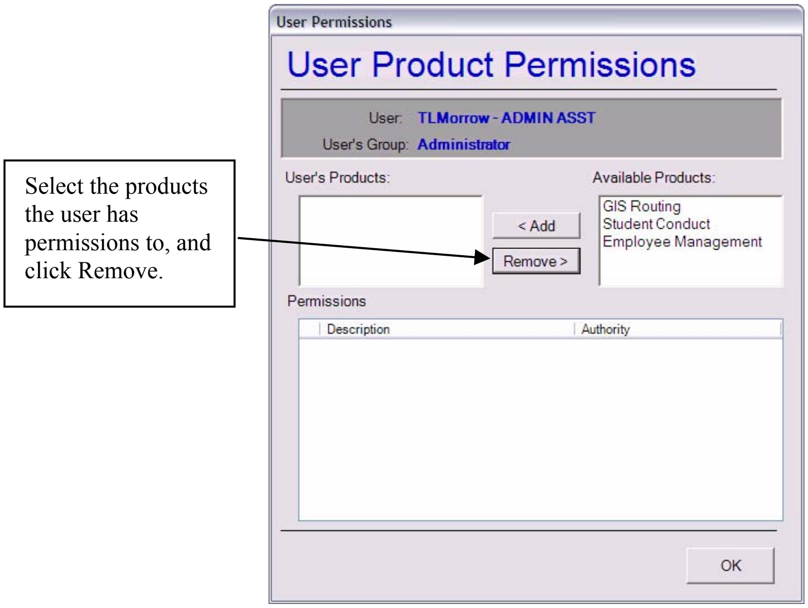



*Figure 10-12. Sample of removed user permissions*

4. Select the user, and click the Delete button (Figure 10-13).

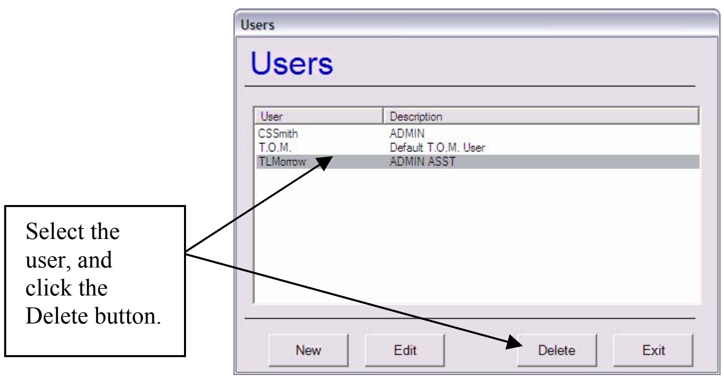



*Figure 10-13. Deleting a user*

5. Click OK to confirm the deletion.

# T.O.M. Security for Groups

You can set up groups as a way to quickly add permissions to users. When you select a user group for a user, the T.O.M. software copies the group's permissions to the user. Then, as described in the previous section, you can customize the user permissions.

This section contains the following:

- Adding a User Group and Setting Its Permissions
- Editing or Changing a User Group to Inactive
- Deleting a User Group

## Adding a User Group and Setting Its Permissions

1. Select Security>Groups (Figure 10-14).

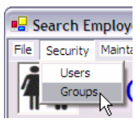



*Figure 10-14. Selecting Security>Groups*

The Groups screen displays.

2. Click the New button to add a user group (Figure 10-15).

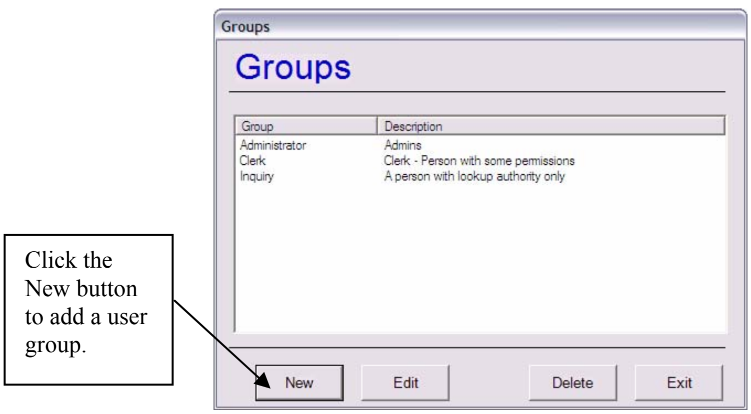



*Figure 10-15. Clicking New on the Groups screen*

The Groups Permissions screen displays (Figure 10-16).

3. Type the name of the group. This is a required field.

4. Select the software product(s) you want to set permissions for in the Available Products box, and click the Add button.

***NOTE: To remove permissions, select the software, and click the Remove button.***

4. Click on the product's name in the Group's Products box. The permission categories for that product appear in the Permissions box.

5. Click on the + sign in front of a permission to expand the permission list. (For a description of the permissions, see the Understanding Permissions section in this chapter.)

6. Click in the boxes in the Authority column to give the selected permission to the user.

***NOTE: You can resize the Description column by clicking in the heading row and dragging it.***

Figure 10-16 shows that the Clerk II user group has permission to view employee notes.

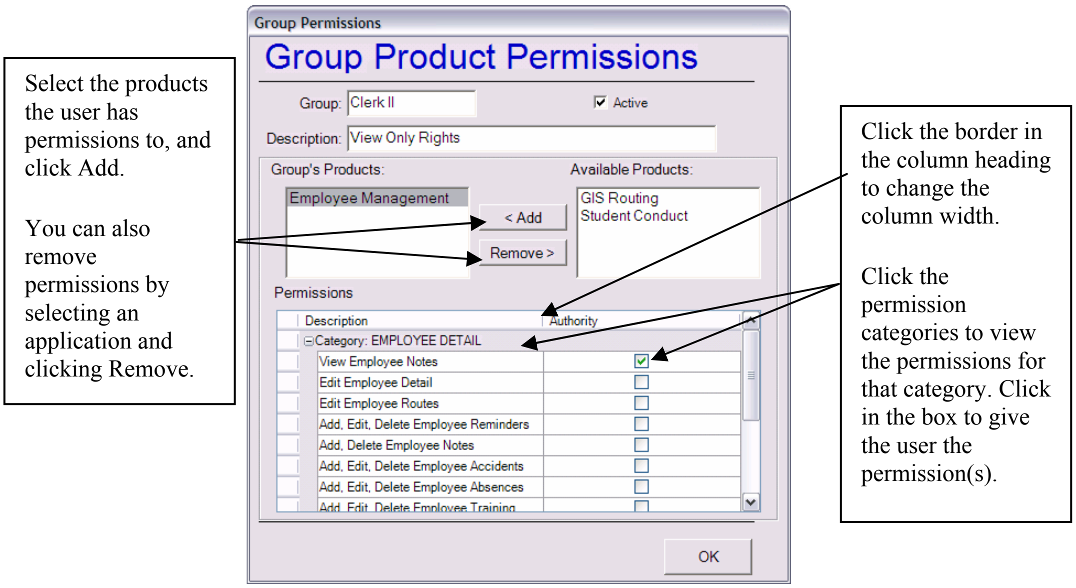



*Figure 10-16. Sample user group*

## Editing or Changing a User Group to Inactive

You can easily change a user group's permissions. You can delete a user group from the system, but if you do that, you are permanently removing it. You might consider changing its status to inactive. That way, it remains in the system but does not appear in the User Group pull-down list in the Users screen.

**To change a user group to inactive:**

1. Either:

   - Select the user group, and click Edit (Figure 10-17).

   OR

   - Double-click the user group.

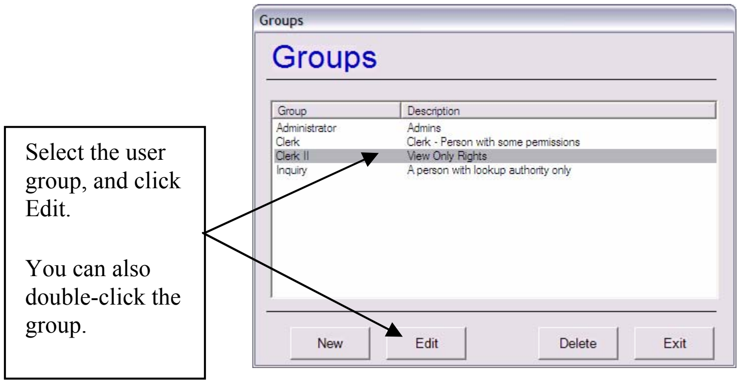



*Figure 10-17. Selecting a user group*

The Group Permissions screen displays.

2. Click in the Active checkbox to remove the checkmark. Figure 10-18 shows that the user group Clerk II has been changed to inactive:

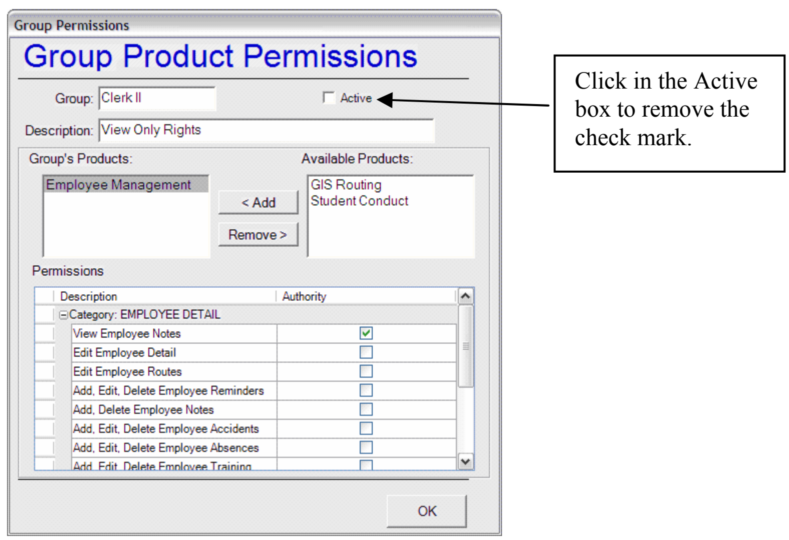



*Figure 10-18. Changing a user group to inactive*

3. Click OK to save your changes.

## Deleting a User Group

When you delete a user group, you are permanently removing it from the system. Also, keep in mind that you can not delete a user group that has users assigned to it. Before you delete the user group, you need to change the users currently assigned to this group to another group. Then, you will be able to delete the group.

***NOTE: As stated in the previous section, you might want to consider changing the user group's status to Inactive. That way, it remains in the system but does not appear in the User Group pull-down menu in the Users screen.***

***To delete a user group:***

1. Either:

   - Select the user group, and click Edit (Figure 10-19).

   OR

   - Double-click the user group.

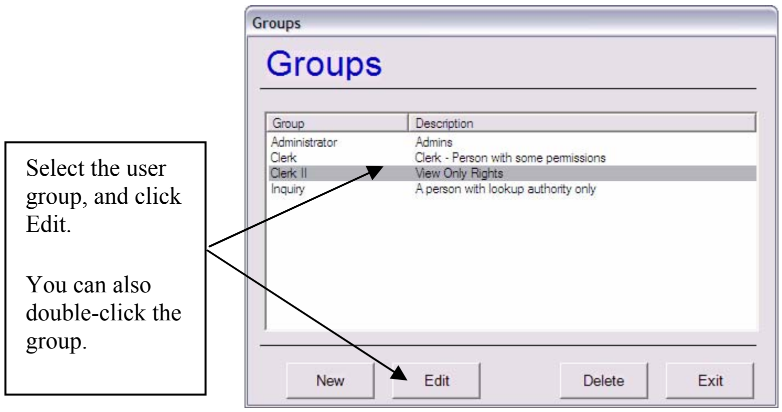



*Figure 10-19. Selecting a user group*

   The Group Permissions screen displays.

2. Select the products for which the user group has permissions.

3. Click the Remove button to remove the user group's permissions to that software. Figure 10-20 shows that the user group Clerk II no longer has permissions to any of the applications.

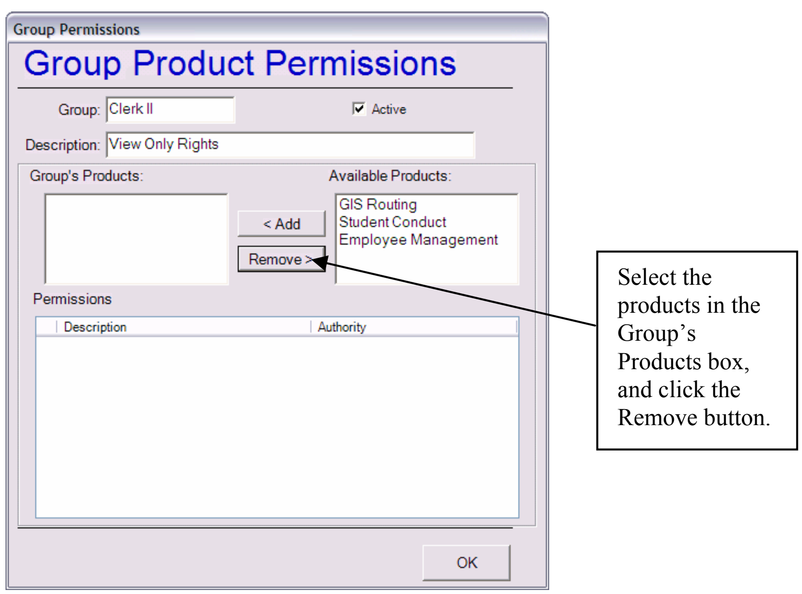



*Figure 10-20. Removing a user group's permissions*

3. Click OK to save your changes.

4. Select the user group, and click the Delete button (Figure 10-21).

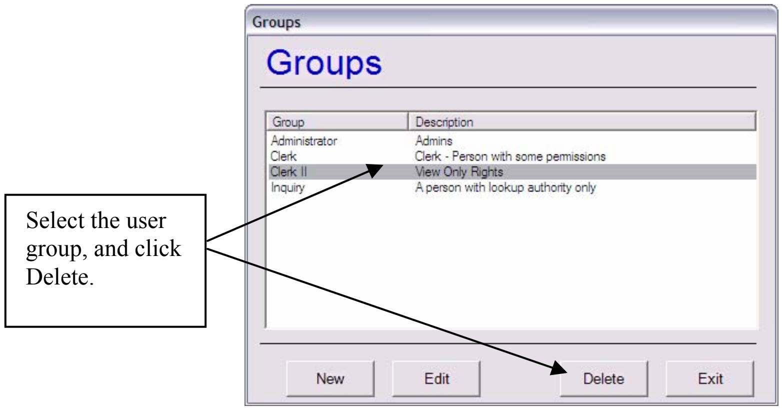



*Figure 10-21. Deleting a user group*

5. Click OK to confirm the deletion.

# Understanding Permissions

You can set up permissions at the group level and then customize them at the user level. However, the process for creating permissions is the same regardless of whether you are creating user or group permissions. For this reason, the graphics you see in this section show the User Permission screen, but the process and explanation of each permission is the same for group permissions.

| | |
|---|---|
| ⓘ ***T.O.M Tip*** | **What's the difference between setting group and user permissions?**<br><br>When you set up group permissions, you can assign that group of permissions to a user. This saves you time when you are adding users because you can assign that group of permissions to the user. Then, you can customize those group permissions for the user. |

This section contains the following information:

- **General Information about Setting Permissions.** Explains a few things you should consider when deciding how to set permissions for users and groups.
- **Understanding how the Employee Screen is Organized.** Explains the relationship between the Employee screen and the permissions you can set for each of the tabs on that screen.
- **Understanding the Permissions Categories.** Describes each of the permissions you can set in each category.

## General Information about Setting Permissions

When setting permissions, keep the following in mind:

- When you specify that a user or group has permissions to add, edit, or delete employee detail information (such as Add, Edit, Delete Employee Accidents), that user will be able to change the information in your employee database.
- When you specify that a user or group has permissions *only* to the View options (such as View Employee Notes), that user or group will not be able to change the data in your database.
- When you specify that a user or group has permissions *only* to the print permissions (such as Print Employee Detail reports), that user or group will not be able to change the data in your database. They will only be able to print reports.

**Am I restricted to giving users or groups only one type of permission such as only the Print or View permissions?**

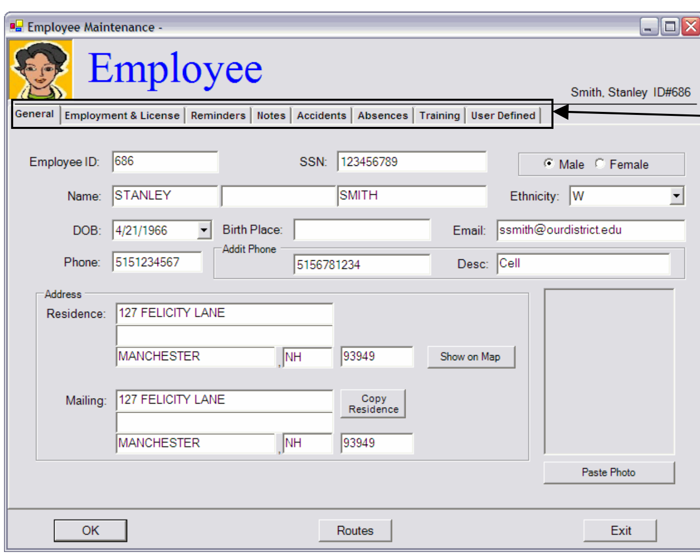
ⓘ ***T.O.M Tip***

No. You can give any number or type of permissions to users and groups, and you can select permissions from any of the categories.

## Understanding how the Employee Screen is Organized

The Employee Management system allows your organization to track many kinds of employee information. The types of information you can track are categorized on the Employee screen of the Employee Management software. Each tab allows users to view, add, edit, and delete information that is specific to the employees in your organization.

*Figure 10-22* shows you how the Employee screen looks. In this graphic, the General tab and its fields are "showing."




The tabs organize the types of employee information you can add to the system.

Each tab and its fields are discussed in the detail in the Users section of the manual.

*Figure 10-22. Employee screen*

To help you understand what the permissions are controlling, below is a brief description of the tabs on the Employee screen:

- **General Tab.** Allows users to view, add, edit, and delete personal employee information such as the employee's name, address, and phone numbers.
- **Employee & License Tab.** Allows users to add and edit information that is specific to an employee's position in your school district, his license information, and more phone numbers and addresses to his record.
- **Reminders.** Employees must often complete certain tasks (such as license renewal) that are time sensitive. This tab enables your organization to track the tasks that employees must complete as well as the tasks' due dates. Users can view, add, edit and delete reminders for individual employees and for groups of employees.

  A group reminder can apply to any number of employees, so when a group reminder is added to the Employee Management software, that one group reminder can be added to an unlimited number of employee records. Because this type of reminder affects so many records, you can allow some users to have permission to manage group reminders and other users to only be able to add, edit, and delete an individual employee's reminders.
- **Notes.** Allows users to view, add, edit, and delete notes from employee records. As you know, some employee information is sensitive, so you should keep this in mind when setting up permissions to the notes.
- **Accidents.** Allows users to view, add, edit, and delete employee accidents/incidents.
- **Absences.** Allows users to view, add, edit, and delete employee absences.
- **Training.** Allows users to view, add, edit, or delete employee training records on this tab. Like employee reminders, you can add training for an individual employee or for a group of employees. Because group training affects so many records, you can allow some users to have permission to manage group training and other users to only be able to add, edit, and delete an individual employee's training.
- **User Defined Tab.** Although the Employee Management system offers your organization many ways to add and track employee information, you might find that your district has special needs that are not included on any of the screens. If that happens, you can add customized fields to the system. You can then enter information into those fields. This tab allows users to view, add, edit, or delete this type of employee information.

ⓘ ***T.O.M Tip***

**Where can I see a list of all the fields on each tab?**

You might want to look through the chapters in the *Users Guide* section of this manual. A chapter is devoted to each tab on the Employee screen, and you can find a picture of the screen as well as a detailed description of each field on the tab and how that screen is used.

## Understanding the Permissions Categories

The T.O.M. Employee Management permissions are grouped into the following permissions categories:

- Employee Detail
- Employee Search
- File Menu
- Maintain Menu
- Security Menu

### *Employee Detail*

The employee detail permissions you set for users controls the level of access a user has to each tab on the Employee screen.

***NOTE: Because some employee information is very sensitive, you need to carefully considered the level of access you give each user.***

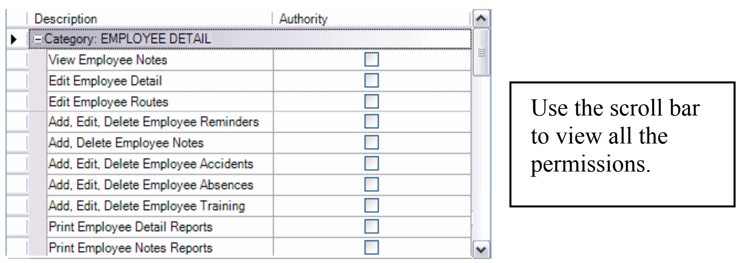



*Figure 10-23. Employee permissions*

You can set the following employee detail permissions for your users:

- **View Employee Notes.** Allows users to view employee notes that have been added to the system. When giving users permission to view notes, keep in mind that some notes might be of a sensitive nature.
- **Edit Employee Detail.** Allows users to edit employee information such as their social security number, date of birth, and contact information. Specifically, a user may modify information on the Employee General tab, Employment and License tab and the User tab. Users will also have permissions to edit custom fields that have been added to the system.
- **Edit Employee Routes.** Allows users to edit routes. or bus runs, that are assigned to employees.
- **Add, Edit, Delete Employee Reminders.** Allows users to manage employee reminders, meaning that they can add, edit, and delete individual employee reminders.

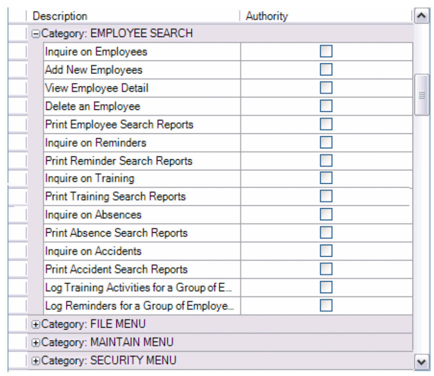
***NOTE: You can also give users permission to manage group reminders. This permission is available under the Employee Search category.***

- **Add, Delete Employee Notes.** Allows users to add and delete employee notes.
- **Add, Edit, Delete Employee Accidents.** Allows users to add, edit, and delete employee accidents.
- **Add, Edit, Delete Employee Absences.** Allows users to add, edit, and delete employee absences.
- **Add, Edit, Delete Employee Training.** Allows users to add, edit, and delete an individual employee's training records.

***NOTE: You can also give users permission to manage group training. This permission is available under the Employee Search category.***

- **Print Employee Detail Reports.** Allows users to access reports from the Employee General tab, Employment and License tab, and User tab.
- **Print Employee Notes Reports.** Allows users to print note reports. As mentioned before, it is possible that the notes your organization adds to the system are sensitive, so keep this in mind when giving this permission to users.

### *Employee Search*




Use the scroll bar to view all the permissions.

*Figure 10-24. Employee Search permissions*

You can set the following employee permissions:

- **Inquire on Employees.** Allows users to select criteria on the Employee screen and search the database using that criteria.
- **Add New Employees.** Allows users to add employees to your database.
- **View Employee Detail.** Allows users to view employee information.
- **Delete an Employee.** Allows users to delete employees from your database.

***NOTE: Rather than removing employees from your database, you can change their status from Active to Inactive. That way, the information remains in the database and can be included on reports. If you want to use this option rather than deleting employees, make sure you do not grant this permission to any users.***

- **Print Employee Search Reports.** Allows users to access reports from the Employee search screen.
- **Inquire on Reminders.** Allows users to search reminders.
- **Print Reminder Search Reports.** Allows users to access reports from the Reminder search screen.
- **Inquire on Training.** Allows users to search training records.
- **Print Training Search Reports.** Allows users to access reports from the Training search screen.
- **Inquire on Absences.** Allows users to search employee absences.
- **Print Absence Search Reports.** Allows users to access reports from the Absence search screen.
- **Inquire on Accidents.** Allows users to search accidents/incidents.
- **Print Accident Search Reports.** Allows users to access reports from the Accident search screen.

- **Log Training Activities for a Group of Employees.** Allows users to add training for a group of employees to the database. When a user adds training to a group of employees, that user is changing many records at one time.
- **Log Reminders for a Group of Employees.** Allows users to add reminders for a group of employees to the database. When a user adds reminders to a group of employees, that user is changing many records at one time.

***NOTE: In addition to allowing employees to add group training or reminders to the database, you can grant them permission to only add training records or reminder s to individual employees. This permission is found in the Employee Detail permission category.***

## File Menu

When you give users permissions to change items listed on the File menu, you are giving those users broad permissions. Those permissions affect the way that you use the system because the items in the File menu control the options you see in many Employee Management system pull-down lists.

Also, all the pull-down lists (with the exception of screens where you can add custom fields) have prebuilt lists that are included with the software. These prebuilt lists may have all the options you need to use the Employee Management system in your district. You should review the lists to see if they need to be customized to how your district wants to track information. That way, you will know which items in the File menu you want to change and who you want to give permissions to change those items.

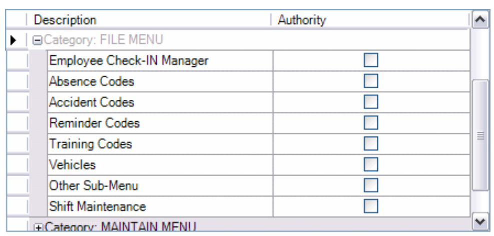



*Figure 10-25. File Menu permissions*

You can set the following File menu permissions:

- **Employee Check-IN Manager.** Allows users to manually check employees in using the Employee Check-In software and to supervise the check-in process.
- **Absence Codes.** Allows users to add, edit, and delete absence codes.
- **Accident Codes.** Allows users to add, edit, and delete accident codes, including Accident Types, Contributing Factors, Reasons In-Use, Injury codes, and Damage Codes.
- **Reminder Codes.** Allows users to add, edit, and delete reminder types and categories.
- **Training Codes.** Allows users to add, edit, and delete training codes.
- **Vehicles.** Allows users to add, edit, and delete vehicle types.
- **Other Sub-Menu.** Allows users to set codes for Employee Types, Employee Statuses, Ethnicity Codes, Vehicle Types, Division/Garages, Departments/Sections, and District Options.
- **Shift Maintenance.** Allows users to add, edit, and delete shifts.

## Maintain Menu

When you give users permission to the Maintain menu, you giving them permission to connect to, backup, and restore. Because the Employee Management system uses the databases to store your employee information, you should carefully consider which users you are going to give these permissions to.

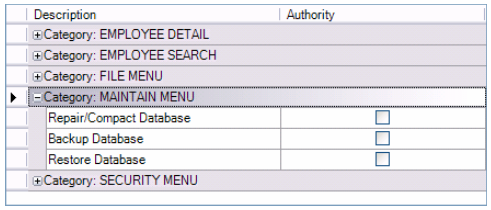



*Figure 10-26. Maintain Menu permissions*

- **Repair/Compact Database**. Allows users to run the Connect to Database utility. This utility is discussed in detail at the end of Chapter 1 of the Getting Started section of this manual.
- **Backup Database.** Allows users to backup the database.
- **Restore Database.** Allows users to restore the database.

## Security Menu

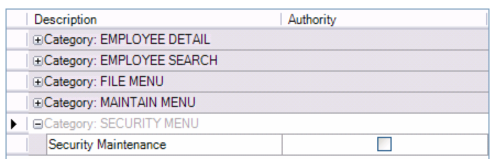



*Figure 10-27. Security permissions*

You can set only one security permission, Security Maintenance, but this setting controls which users can set up and change user and group permissions. Like the File and Maintenance permissions, this permission is very broad and affects how the Employee Management system is used at your organization. You should carefully consider who you want to give these permissions to.