New Security System and Users and Password

The upgrade to TOPS 2000™ v3.2.1 includes a new more sophisticated security system that implements user–based security through Domain Workstation Keys. As we move toward more web based functionality this new security system will provide you with greater flexibility and mobility. Increased user accountability, more security, and compliance.

This technology utilizes the Windows Network login scheme to allow a single user to log in to TOPS from any workstation on the network under a single key. In order to take full advantage of the new features, and user controls to the TOPS application and data across your network User Groups must be clearly defined.

Very Important! Your existing Users and Passwords along with permissions are converted as part of the upgrade. However, because the new Users and Passwords is group-based, your existing user groups are no longer valid. Each user will appear as an individual user group named "[user name] Group". New User Groups must be defined using the access and permissions settings in the new security system and Users must be re-assigned to one of these new User Group.

Take a moment to review the two provided examples of User Group settings based on job functions provided at the end of this document.

Start TOPS and login using your current user name and password, from the Main menu:

1. Click Administration on the menu bar.

2. The Administration drop-down menu list appears.

3. Select Users & Passwords from the drop-down menu list.
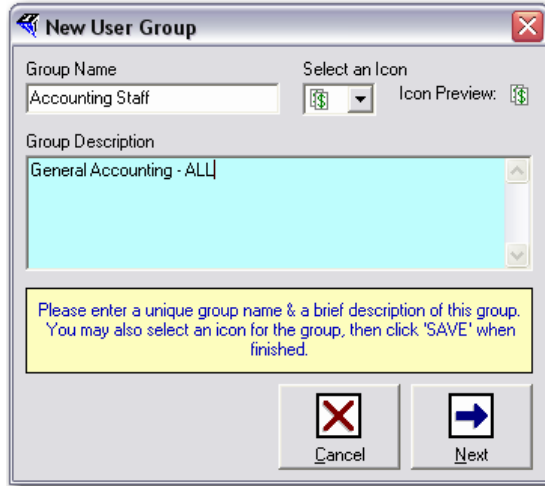
4. The User Control window appears.
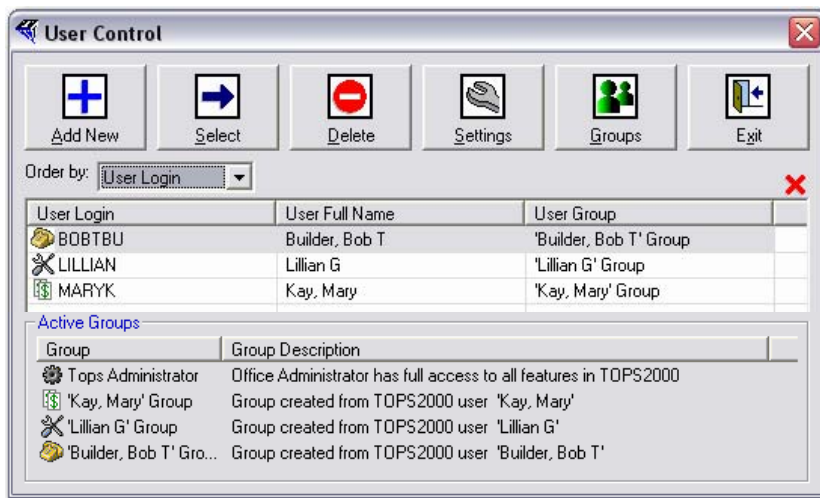
5. Click the Groups button located on the User Control window toolbar.

6. The User Group Control window appears.
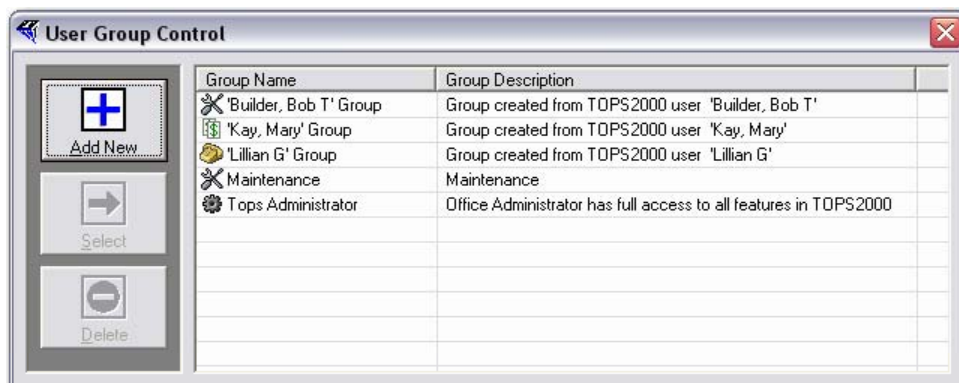
*Each user in your TOPS v3.2.1 system will appear as a group name. You will also find The **Administrator User Group** in your list. The TOPS Administrator is the only pre-set user group provided in the upgrade and it is* NOT *editable.*

7. Click the Add New button.

8. The New User Group window appears.

9. Enter the new Group Name in the Group Name field.

10. Select an Icon from the Icon drop down list.

11. Add a Group Description.

12. Click Next.

13. The User Group Control window appears.
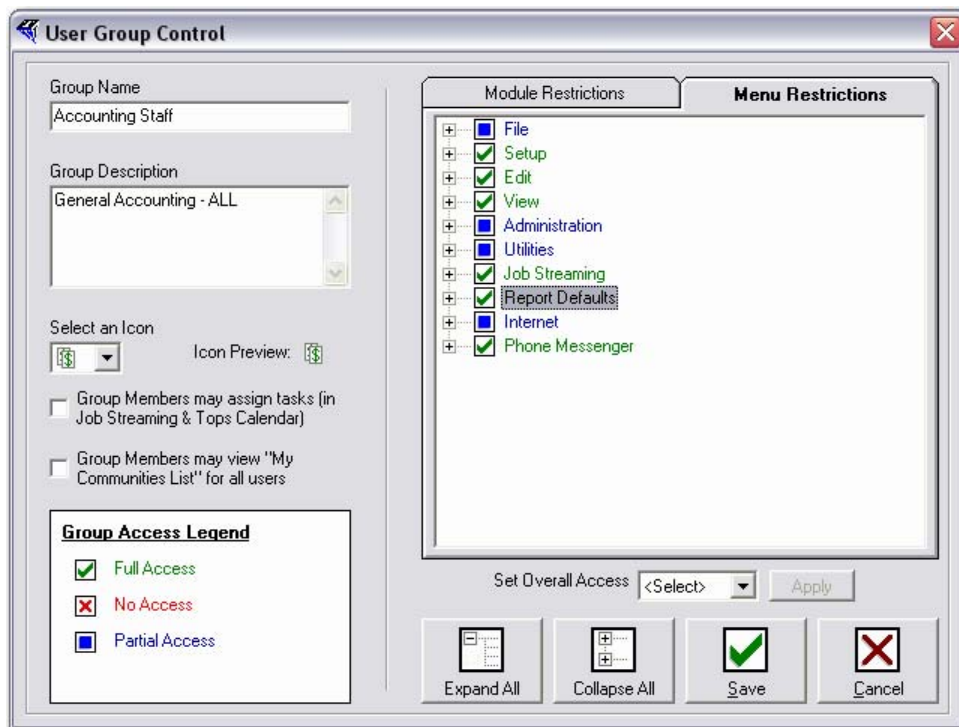
The window contains two tabs, one for Module Restrictions and one for Menu Restrictions. There is also a Group Access Legend describing the access types for each category, Full, Partial, No Access and Read Only. Based on the job function for the named User Group, begin defining access and permissions.

If access will be the same across all menus or modules for a user group, you can quickly set the same option for all items at once by:

14. Click the down arrow for Set Overall Access field.

15. Select the Access Type, Full, None, or Read Only (for Modules).

16. Click Apply.

> -OR-

17. Click the [+] to the left of each menu item to Expand the list of options. You may expand or collapse all modules at once by clicking:
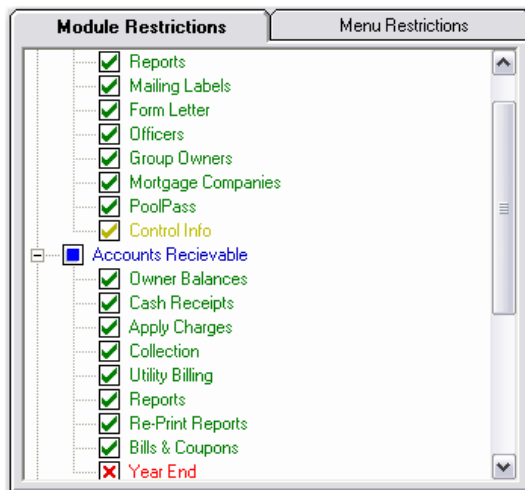
18. **Expand Tree-view** button   **Collapse Tree-view** button.

19. Click the checkbox to the left of each option until the desired Access type appears.

20. Repeat Steps 17 and 18 until all settings have been defined for each Menu option.

21. Click the Modules Restrictions Tab.

22. Repeat Steps 14 through 16 for blanket permissions or Repeat Steps 17 and 18 until all settings have been defined for each Module.

23. Click the checkbox if this User Group is allowed to assign tasks to others in Job Streaming Module (optional Add-on).

24. Click Save when finished.

25. You are returned to the User Group Control window.

26. Click Add New and continuing adding User Groups until all groups have been added.

27. Click Exit, you are returned to the User Control window.

Assign Users to a User Group

Now that all your user groups have been defined you are ready to update your user record and assign each user to the appropriate User Group.

From the User Control window:

1. Double-click the User Name in the list box.

2. The User Info window appears.

3. Click the User Group field down arrow.

4. Select the appropriate User Group for this user.

5. Click the Community Assignments button.

6. The Community List window appears.

7. Click the Select All button

   -OR-

8. Double click to select the desired community(s) this user may access.

9. Click Save, you are returned to the User Control window.

10. Repeat Steps 1 through 9 for all active users.

11. When finished, Click Exit from the User Control window to return to the TOPS 2000™ Main menu.

Delete A User Group

You will want to remove the user groups that were created during the upgrade.

To delete a user group, from the User Control window:

1. Click the Group button.

2. Click the User Group Name in the list box.

3. Click the Delete button.

4. Click Yes in the Delete validation dialog box to delete the named User Group or

5. Click Cancel to return to the User Group Control window.

Sample User Groups

The following tables are examples of how to setup access and permissions in your new User Groups that are required by the new security system in TOPS 2000™ v3.2.1.

1. We recommend that you set up User Groups based on job functions within your organization. Not all user require access to all modules or functions. You especially want to limit access to critical processes where an inexperienced employee may not understand the full impact of certain actions.

2. If you use temporary help for data entry throughout the year, a special user group limiting access to only certain modules and functions is a must have.

3. TOPS Payroll is another area where limiting access is advisable. Not everyone should have access to all areas of the payroll module.

4. Reports, is another critical area that should be reviewed carefully, company information should be accessible on a need to know basis and owner information should also be protected.

Group Name	Access	Permissions
Administrator has access to **ALL** functions and permissions. Defined by TOPS 2000™. Requires no setup	All Menus	
	All Modules	

Group Name	Access	Permissions
Accounting-Staff	Menu Restrictions Green indicates Full Access for all sub-menu options contained in this Menu. Blue indicates some sub-menu limitations exist within this Menu. Red indicates there is No Access to any sub-menu options	

Group Name	Access	Permissions
Accounting Staff	Module Restrictions Green indicates Full Access for all sub-menu options contained in this Menu. Blue indicates some sub-menu limitation exist within this Menu. Red indicates there is No Access to any sub-menu options Gold or Yellow indicates "Read Only"	

Group Name	Access	Permissions