Setup Series-6003

Security Setup

Version 9.0

Information in this document is subject to change without notice and does not represent a commitment on the part of Technical Difference, Inc. The software product described in this document is furnished under a license agreement or nondisclosure agreement. The software and this documentation may be used or copied only in accordance with the terms of that agreement.

All names of companies, products, street addresses, and persons are part of a completely fictitious scenario and are designed solely to document the use of People-Trak. Similarities to real companies, products, addresses, or persons are purely coincidental.

People-Trak is an extensively customizable HR software product. Screen and report samples rendered in this document reflect the default version of People-Trak. These samples may or may not match the screens and reports within your product if customization has been performed.

Technical Difference, Inc.
5256 S. Mission Road #210
Bonsall, CA 92003
(800) 273-3760
(866) 693-4869 (fax)

www.people-trak.com

(Revision 01/01/2014)

Contents

Notes

Workbook

Security Overview

This overview discusses the different types of access and includes some security recommendations and procedures.

Physical Access

Physical access is your first and strongest means of protecting vital information. Physical access is entirely in your hands. If an intruder cannot access a computer with access to People-Trak, the intruder cannot access People-Trak, period. It is your duty to make certain that proper controls are in place to make certain that workstations with access to People-Trak are properly secured.

For network installations, a facet of physical security that must be addressed is the directory rights granted to users who access the file server on which People-Trak has been installed. If a user has access to the directory, they can simply start the TDENGINE.EXE process through Windows Explorer, through DOS, or through the File Run option. This user will not necessarily have a user ID/password combination to gain entrance into People-Trak, but the user has an open door. Password cracker processes can be run against the software and the Microsoft Access databases are vulnerable to be copied.

One frequently overlooked facet of physical security is the issue of shared printers. If you have a shared printer in an area with public access and you print a document to that printer, the information on that document is not secure unless you are standing at the printer when the document is physically printed. If you print a document and leave it there, the contents of that document are subject to the scrutiny of every employee sharing that printer.

System Access

Once a user has gained physical access to People-Trak, the various controls provided by People-Trak are in force. The first control is system access. System access to People-Trak is controlled through the use of user ID/password combinations. Only those users with a valid user ID and password can gain access to People-Trak. Once access has been gained, the user is subject to the security established for that user. The default user ID/password combinations provided with People-Trak are DEMO/DEMO and MASTER/MASTER. Additional combinations for each of your users can be defined with the User Setup process.

User ID and passwords should be unique. Do NOT share user ID and passwords between users. If you forget your user ID and password combination, contact your Support Representative. People-Trak provides a limited use “backdoor” feature for this particular situation. Your Support Representative can provide the key to the backdoor.

Company Access

Access to the individual companies that you define within People-Trak is under your control. Any user can be given access to any combination of companies. For example, if you have a user who is not allowed to see archived data, you can restrict that user from the ARCHIVE Company. No access to that data through any function will be provided.

Module Access

Access to the individual modules provided with People-Trak is under your control. Any user can be given access to any combination of the modules. For example, if you have a recruiting staff that should have access to Applicant Management, but not to Personnel Management, you can limit the recruiting staff to the Applicant Management module.

Record Security

The record security option allows you to grant or deny access to groups of records using query statements. For example, if you are allowing department heads to use People-Trak for employee reporting purposes, you will develop a query filter for each departmental user that grants access to those employee records in each specific department. The query filter utilizes the full power of the query engine in People-Trak and allows you to extensively control access from one record to every record in the company.

Menu Access

Access to individual menu options is under your control. For each user, you can grant or deny access to any option listed on the File and Documents menus as well as some of the options on the Tools menu. The full Tools, Administration and Setup menu access is controlled by the Administrator setting in Security Setup.

Category Access

Access to the individual categories for the module that are provided with People-Trak is under your control. Workflows, Activities, Processes, Tables, Screens, Fields and Documents all have a category assigned to them. If you secure a category, you automatically secure all of the items in that category. This makes setting security very easy and thorough. If you do not allow access to a category, all of the items in that category are automatically set to no access as well and cannot be changed.

Workflow Access

Access to individual workflows for the module is under your control. For each user, you can grant or deny access to any of the workflows. If a user does not have access to a category, all of the workflows in that category are set to no access and cannot be changed.

Activity Access

Access to individual activities for the module is under your control. For each user, you can grant or deny access to any of the activities. If a user does not have access to a category, all of the activities in that category are set to no access and cannot be changed.

Processing Access

Access to individual processes for the module is under your control. For each user, you can grant or deny access to any of the processes. If a user does not have access to a category, all of the processes in that category are set to no access and cannot be changed.

Table Access

Access to updating individual tables for the module that are provided with People-Trak is under your control. For each user, you can grant or deny access to updating any of the tables. If you deny a user access to a table, that table will not be available for update in either the Edit/Print Table or Mass Update Table process in that module. If a user does not have access to a category, all of the tables in that category are set to no access and cannot be changed.

Screen Access

Access to individual data entry screens (standard and custom) for the module is under your control. For each user, you can grant or deny access to any of the data entry screens. If a user does not have access to a category, all of the screens in that category are set to no access and cannot be changed.

Field Access

You can control access for each user to every field in People-Trak. Unlike the other security features, field access has three states. You can prevent access altogether; the highest form of security. You can grant display-only access; the ability to see, but not change the data. Or, you can grant full access, which allows the user to both see and change data.

Restricting access to a process or screen does not restrict access to the fields associated with that process or screen. You must specifically restrict access to those fields, or they can be accessed in other areas of People-Trak.

If a user does not have access to a category, all of the fields in that category are set to no access and cannot be changed.

Document Access

Access to updating or viewing individual documents in People-Trak is under your control. For each user, you can grant or deny access to any of the documents. If a user does not have access to a category, all of the documents in that category are set to no access and cannot be changed.

Denying Access

If you deny a user access to any component of People-Trak, that component will no longer be visible. For example, if you deny a user access to a field, that field will no longer show up on any screen and will not be included in the Select Field popup. Any report that includes that field cannot be run. If you deny access to a screen that is included on a workflow to which the user does have access, that screen will not show up in the screen dropdown, or if it is a sub screen, that button will no longer display. If a user is denied access to a function that is on the Shortcut Bar, the shortcut will still display but it will be disabled and its caption will be in white to denote that.

Check for Unauthorized Access

Each time a user logs into People-Trak a record is stored in the System Access Log. If a user attempts to log in, but fails to gain access, an attempt to log in is also stored. These access records can be used to determine if someone is attempting to or has succeeded in accessing People-Trak without authorization via the User ID and Password entry.

The information stored in the System Access Log includes the user name, date of the access, time of the access, and a comment. Since the time is stored, it is possible to check for access attempts that are outside normal operational hours.

To check the System Access Log, use the View Access Log utility. The access records are stored in the order in which they occurred. This utility is accessed by selecting the Utilities option on the Administration menu.

Recommendations

An effective security method depends on preparation and planning. These depend on a proper understanding of the features provided. If you do not fully understand the features provided, please consult your Support Representative. People-Trak comes with all security features

disabled and the standard passwords grant System Administrator privileges. You will be working from an unsecured environment to an environment that is secured to the desired level. Do not add, import, or interface security sensitive data into People-Trak until the appropriate level of security has been implemented.

When setting up users, delete or modify the default user ID/password combinations provided with People-Trak. These combinations are not only listed in the documentation, but they are typical of many software applications and they are obvious. Someone who is able to obtain physical access to People-Trak and this documentation could easily gain full access by guessing at the two default combinations. Either change the password for DEMO/DEMO and MASTER/MASTER or delete the combinations just as soon as you have completed combinations for your users.

Use only those security features that are required. Security features require process code to be executed thereby reducing processing speed. To optimize performance at all times, utilize only those security features that are actually required.

Copy Security from Another User

The security for the current user will be cleared and then the security from the specified user will be copied over to the current user. The term "security" means all settings related to security in both the Security Setup and Security Setup – Module processes.

Note: The Copy User Security option in the Security Setup - Module process follows the same procedure and has the same results.

Clear all Security for the Current User

The Clear Security for User option on the File menu of the Security Setup and Security Setup – Module screens allows you to clear all security for the current user. This means that the user will have unrestricted access, except for the following settings on the General tab, which are set to disabled (check box not selected):

- Administrator
- Show All Users in Inbox
- Create Freeform Reports
- Run Freeform Reports

If the Group Designator check box is selected for a user for which you are clearing security, you will be notified that this will clear the security for all users in the group. You then have a choice of continuing or not.

If the Group Name field is set for a user for which you are clearing security, that field will be cleared so the user is no longer part of that group anymore.

Security Setup

The Security Setup option on the Setup menu allows you to set up security for components that are enterprise-wide and across all modules: company and module. The Security Setup screen uses three tabs to record the user security information. These tabs are described below.

General Tab

The General tab is used to establish basic security information for each user. These basic areas and their features are listed and described below.

- Group Designator
- Group Name
- Administrator
- Show All Users in Inbox
- Create Freeform Reports
- Run Freeform Reports
- Design Mode
- Grid Sorting
- Display Only
- Allow File Search in Email
- Allow Help Edit

The Group Designator check box allows you to specify whether or not this user is to be used to control group settings. Select the check box to designate that this user controls a group. Clear the check box to designate that this user does not control a group. Clearing this check box will also clear the Group Name field for all users that had this user in that Group Name field. See Group Name below.

The Group Name field is the name of the group to which this user belongs. This field is supported by a Select User Group popup, which will show a listing of all users that have their Group Designator field selected. If the user is assigned to a group, that user is assigned the same settings as the group and the settings are for display only. If the user that controls the group has a setting change, all group members are also updated with the same setting change.

Note: You are allowed to manually change a group member but those changes will be overridden if the user that controls the group has a setting change.

The Administrator checkbox allows you to specify whether or not the user has administrator privileges. A user with administrator privileges is not subject to any security options, even if they are set. For example, if field security is set for an administrator, it is completely ignored. An administrator also has access to all of the Tools, Administration and Setup menu options. If a user is not an administrator, he has no access to the Administration and Setup menus, and on the Tools menu, he only has access to the Maintain Tables, Set Alarm and Inbox tools.

Note: Change the Administrator setting with caution. If you select the check box, you have just given the user complete access to everything in People-Trak. If you clear the check box, you have just removed administrator rights for that user. So, if you are the administrator and you accidentally clear the check box for your user and close Security Setup, you can no longer get to Security Setup to select the check box again!

The Show All Users in Inbox checkbox allows you to specify whether or not the user is to see his own Inbox tasks or tasks for all users. Normally, at least one user should be able to see all transactions. Otherwise, no one can determine if the tasks are actually being performed. For example, if various tasks and reports have been divided among the staff and scheduled with the Scheduler feature, then those tasks will show in a particular user's Inbox. If the user goes on vacation or is sick, no one will remember that these tasks are not being performed. If one user can see all of the tasks, the tasks will not be forgotten. Select the check box to show all user tasks in the user's Inbox. Clear the check box to only show the user's tasks in the user's Inbox. If this check box is selected for a user, the user will be able to toggle between Full Inbox and My Inbox. This feature is only available for HR users.

The Create Freeform Reports checkbox allows you to specify whether or not the user will be allowed to create freeform reports. Select the check box to allow the user to create freeform reports. Clear the check box to not allow the user to create freeform reports. The Freeform Report document type allows you to enter an SQL statement and a series of captions to create

reports that you could not otherwise create. The Freeform Reports feature bypasses all field security. If a user is allowed to create a Freeform Report, he or she can access any field within People-Trak.

The Run Freeform Reports checkbox allows you to specify whether or not the user will be allowed to run freeform reports. Select the check box to allow the user to run freeform reports. Clear the check box to not allow the user to run freeform reports. The Freeform Report document type allows you to enter an SQL statement and a series of captions to create reports that you could not otherwise create. The Freeform Reports feature bypasses all field security. If a user is allowed to run freeform reports, he or she can see any secured data included on the freeform reports.

The Design Mode checkbox allows you to specify whether or not the user is allowed to use Design Mode when modifying an adhoc report. Design mode allows the user to change fonts, headings, colors and other attributes of report columns.

The Grid Sorting checkbox allows you to specify whether or not the user will be allowed to sort the data in grids. Normally, the data in grids can be sorted by clicking on the grid header for the column upon which the data is to be sorted. The data in the grid is then sorted by that column. Select the check box to allow the user to sort grid data. Clear the check box to not allow the user to sort grid data.

Note: You might have reports that are expecting the most recent information in the top row of a grid but someone sorted that grid in a completely different order. In this case, your report results will not be what you wanted. For this reason, you might want to limit who can sort grids. Even if Grid Sorting is turned off for a user, the Lookup screen grid can still be sorted.

The Display Only checkbox allows you to specify whether or not the user can only have display-only access to data. Select the check box to only give the user display-only access to data. Clear the check box to give the user access to fields as specified by the Display Only check box in the Field Properties screen for each field. If a user is set to Display Only, the New, Copy, Transfer and Delete record functions are disabled in all modules.

Notes A check box that allows you to specify whether or not the user can have access to notes when in a record. Select the check box to give the user access to notes. Clear the check box to not give the user access to notes, which will disable the Category Notes button on the Category Bar when the user is editing a record.

The Allow File Search in Email checkbox allows you to specify whether or not the user can have access to the file search capability when attaching files to an email. Select the check box to give the user access to the file search capability, which is then available by clicking the File Search button. Clear the check box to not give the user access to the file search capability, which means the File Search button is hidden.

The Allow Help Edit checkbox allows you to specify whether or not the user can have access to the Help Editor on the Help screen. Clear the check box not to give the user access to the edit help capability, which means that the Edit button is hidden on the Help screen.

Company Tab

The Company tab is used to specify the companies to which the user will have access.

Select the check box for the company to which the user can have access. Clear the check box for the company to which the user cannot have access. If you are updating your own user, you cannot deactivate your current company. If you are updating another user besides yourself, you are not allowed to deactivate all of the companies.

All of the companies currently defined are displayed. After access has been set, any list of companies displayed for that user reflects only those companies for which access has been granted. When using the Select Company option on the File menu, the list of companies does not include all companies, but only those to which access has been granted. Similarly, the Transfer *Record* option allows the user to transfer records from the current company to another company. The list of destination companies that is presented is subject to the security that has been defined on this tab.

If a user only has access to one company, the Select Company option is removed from the File menu and the shortcut is disabled.

Note: When a new company is added, all users automatically have access to that company until restricted using this Company tab.

Module Tab

The Module tab is used to select the modules to which the user has access.

By default, all modules, whether licensed or not, are listed and selected. If an unlicensed module has been selected on the Modules pane, it can only be accessed with proper licensing. A message will inform a user if the module has not yet been licensed.

Select the check box for the module to which the user can have access. Clear the check box for the module to which the user cannot have access. If you are updating your own user, you cannot deactivate your current module. If you are updating another user besides yourself, you are not allowed to deactivate all of the modules.

The next time the user logins in after access changes have been made, any list of modules displayed for that user will reflect only those modules for which access has been granted.

Note: When a new module is added, all users automatically have access to that module until restricted using this Module tab.

Security Setup - Module

The Security Setup - Module option on the Setup menu allows you to set up security for components that are enterprise-wide, but for the current module only: record, menu, category, workflow, activity, processing, table, screen, field and document. The Security Setup - Module screen uses ten tabs to record the user security information. These tabs are described below.

Record Tab

The Record tab is used to define a security filter that grants the user access to those records in the current module that meet the criteria defined in the filter. The filter is executed when the user selects the module. A list of records is generated from the query and this is the list to which the user is granted access.The Test button on this tab generates a list of the records that will be included when the user selects the module so you can check that the results of the specified query are what you intended.

This tab uses the standard query grid to select the records to which each user has access.

Menu Tab

The menu tab is used to select the menu options on each main menu to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the menus (File, Documents, Templates and Tools). The list box

on the right displays the menu options for the highlighted menu. You can navigate through the menus and select or deselect menu options.

Note: The Administration and Setup menus are not included on this tab because these menus are automatically secured by the Administrator setting on the General tab. If you are not an Administrator, you cannot access the Administration and Setup menus and can only access the common tools of Email Preferences, Set Alarm and Inbox on the Tools menu. Administrators are not subject to any of the security features in People-Trak. You can make security settings for an Administrator, but they will not be honored. The Tools option on this Menu tab only lists Email Preferences and Set Alarm because there is really no reason to ever secure the Inbox.

Select the check box for the menu option to which the user can have access. Clear the check box for the menu option to which the user cannot have access. Click the Toggle all options on this menu button to toggle all option check boxes for the current menu from selected to not selected, and vice versa.

Category Tab

The Category tab is used to specify the categories to which the user will have access.

Select the check box for the category to which the user can have access. Clear the check box for the category to which the user cannot have access.

All of the tabs to the right of the Category tab (Workflow, Activity, Processing, Table, Screen, Field and Document) contain the items that the category can secure. If you allow a user access to a category, you can still limit the individual items within that category. If you do not allow access to a category, all of the items in that category are automatically set to no access as well and cannot be changed.

Workflow Tab

The Workflow tab is used to select the workflows in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the workflows in the highlighted category. You can navigate through the categories and select or deselect workflows.

Select the check box for the workflow to which the user can have access. Clear the check box for the workflow to which the user cannot have access. Click the Toggle all workflows in this category button to toggle all workflow check boxes for the current category from selected to not selected, and vice versa.

If you happen to remove access to the default workflow for the user, the New and Open functions are disabled for that user when in that module.

Note: If a user has no access to a category, all of the workflows in that category are set to no access and cannot be changed.

Activity Tab

The Activity tab is used to select the activities in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the activities in the highlighted category. You can navigate through the categories and select or deselect activities.

Select the check box for the activity to which the user can have access. Clear the check box for the activity to which the user cannot have access. Click the Toggle all activities in this category button to toggle all activity check boxes for the current category from selected to not selected, and vice versa.

Note: If a user has no access to a category, all of the activities in that category are set to no access and cannot be changed.

Processing Tab

The Processing tab is used to select the processes in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the processes in the highlighted category. You can navigate through the categories and select or deselect processes.

Select the check box for the process to which the user can have access. Clear the check box for the process to which the user cannot have access. Click the Toggle all processes in this category button to toggle all process check boxes for the current category from selected to not selected, and vice versa.

Note: If a user has no access to a category, all of the processes in that category are set to no access and cannot be changed.

Table Tab

The Table tab is used to select the tables in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the tables in the highlighted category. You can navigate through the categories and select or deselect tables.

Select the check box for the table to which the user can have access. Clear the check box for the table to which the user cannot have access. Click the Toggle all tables in this category button to toggle all tables check boxes for the current category from selected to not selected, and vice versa.

If you deny a user access to a table, that table will not be available for update in either the Edit/Print Table or Mass Update Table process in any module. The user will still have access to the table to make selections whenever a field is supported by that table.

Note: If a user has no access to a category, all of the tables in that category are set to no access and cannot be changed.

Screen Tab

The Screen tab is used to select the screens in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the screens in the highlighted category. You can navigate through the categories and select or deselect screens.

Select the check box for the screen to which the user can have access. Clear the check box for the screen to which the user cannot have access. Click the Toggle all screens in this category button to toggle all screen check boxes for the current category from selected to not selected, and vice versa.

Note: If a user has no access to a category, all of the screens in that category are set to no access and cannot be changed.

Field Tab

The Field tab is used to select the fields in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the fields in the highlighted category. You can navigate through the categories and select or deselect fields.

In field security there are actually three different states and the list box uses text instead of check boxes to set the security. The three states for field security are No Access, Display Only, and Full Access. You can select any state by clicking on the label. The label will toggle between the three states. The No Access state hides the field from the user on any screens on which the field belongs. The Display Only state causes the data to be displayed on the screen just as it is with Full Access security, but the data cannot be modified. Click the Toggle all fields in this category button to toggle all field for the current category from one state to another.

There is also a special Notes category at the bottom, which lists the note fields. You can easily secure one or all of those note fields for the current module. The Notes screen itself can be secured in Security Setup, and if the Notes screen is visible to a user, secured categories of notes are not.

Note: If a user has no access to a category, all of the fields in that category are set to no access and cannot be changed.

Document Tab

The Document tab is used to select the documents in the current module to which the user has access. This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the documents in the highlighted category. You can navigate through the categories and select or deselect documents.

Select the check box for the document to which the user can have access. Clear the check box for the document to which the user cannot have access. Click the Toggle all documents in this category button to toggle all document check boxes for the current category from selected to not selected, and vice versa.

Note: If a user has no access to a category, all of the documents in that category are set to no access and cannot be changed

Lesson 1
Security Setup

Lesson Contents

This lesson covers the key, enterprise-wide settings in the Security Setup process.

Tutorials

Using Groups: demonstrates how to use groups in setting up security.

Administrator Setting: shows what the Administrator setting controls and how to change it.

Display Only Setting: demonstrates what the Display Only setting controls and how to change it.

Securing Companies and Modules: shows how to secure companies and modules.

Copying and Clearing Security: demonstrates how to copy security from a user and also clear security for a user.

Tutorial 1.1 – Using Groups

You have the option of using groups to control security for users who should have the same security settings. This tutorial will demonstrate how this works.

1. On the **Setup** menu, select **Security Setup**.

   The Security Setup screen is displayed and your DEMO user is highlighted.

   When you first enter the Security Setup screen, the user ID you used to access People-Trak (DEMO in this case) becomes the current user record being edited. You can use the list of users to select any other user for editing. In all of the Security Setup tutorials, we will just be changing the security for the DEMO user, so you can easily see the changes take effect.

2. Select the **Group Designator** check box.

   You have just made DEMO the "head" of the group. The next step is to assign other users to the DEMO group that should have the same settings as DEMO.

3. Select the **MASTER** user.

4. In the **Group Name** field, enter **DEMO**.

   The MASTER user is now assigned to the DEMO group and all of the DEMO user's security settings have been copied to the MASTER user. Any time the DEMO user security is changed, the MASTER user security will also be changed so that the DEMO and MASTER security settings are always identical.

   Note: The term "security settings" means the settings in both the **Security Setup** AND **Security Setup - Module** processes.

5. Try to change any of the check boxes for the **MASTER** user.

   You cannot because those settings are now display only. The MASTER user settings can only be changed from changes to the DEMO user.

   Let's make a change in the DEMO user's security and see how this then updates the MASTER user's security. First, make note that the Create Freeform Reports field is selected for the MASTER user.

6. Select the **DEMO** user.

7. Clear the Create Freeform Reports check box.

8. Select the **MASTER** user.

   The Create Freeform Reports check box is now cleared for the MASTER user because it is cleared for the DEMO user that controls the group to which the MASTER user is assigned.

   Let's get the group fields back to the way we started.

9. Select the **DEMO** user.

10. Select the Create Freeform Reports check box.

11. Clear the **Group Designator** check box.

12. Select the **MASTER** user.

    Confirm that the Group Name field for the MASTER user is now blank. When you clear the Group Designator check box for the head of a group, all of his or her "groupies" will also have the Group Name field cleared.

13. Close the **Security Setup** screen.

14. Continue with the next tutorial.

Tutorial 1.2 – Administrator Setting

The Administrator setting is very powerful. If a user has the Administrator check box selected, that user is not subject to any of the security features in People-Trak. You can make security settings for an Administrator, but they will not be honored. If you are not an Administrator, you cannot even access the Administration and Setup menus and can only access the common tools of Inbox, Maintain Tables, and Set Alarm on the Tools menu.

By default, the DEMO user is set to be an Administrator. Let's take a look at the Tools, Administration and Setup menus while we are an Administrator.

1. Click the **Tools** menu and leave that menu displayed.

   All of the tools in People-Trak are available to you.

2. Move the cursor over to the **Administration** menu and leave that menu displayed.

   All of the administration options in People-Trak are available to you.

3. Move the cursor over to the **Setup** menu and leave that menu displayed.

   All of the setup options in People-Trak are available to you.

   Now, let's demote ourselves to a non-Administrator.

4. On the **Setup** menu, select **Security Setup.**

5. On the **General** tab, clear the **Administrator** check box for the **DEMO** user.

6. Close the **Security Setup** screen, saving your changes.

7. Click the **Tools** menu and leave that menu displayed.

   There are now only four options available: Inbox, Maintain Tables, and Set Alarm. These are the common tools that are available to everyone.

   The Administration menu is no longer visible because all of its options are only available to Administrators.

8. Move the cursor over to the **Setup** menu and leave that menu displayed.

   There are only two options still available: Security Setup and Security Setup - Module. The only reason these options are there is because we have left these for training purposes only; we have to have a way to get back into the Security Setup processes. In a live environment, the Setup menu would be completely removed for a non-Administrator user. So, if you are the administrator and accidently clear the Administrator check box and close Security Setup, you will no longer be able to access Security Setup!

9. Click off the menu to close it.

   For the rest of the security training, we are going to leave DEMO set as a non-Administrator so we can see the changes we make in the Security Setup processes take effect. If we were an Administrator, all of our changes would be ignored because Administrators have full access no matter what the security settings are.

Tutorial 1.3 – Display Only Setting

You can set a user to be display only, which is a very powerful setting. Let's see how this works.

1. Open **Donald Stern's** record.
2. Click in the **Middle Name** field.

   Note that the color of the field is still blue, which is the Normal color. This means that this field is editable.
3. Change **Donald's Middle Name** from **Edward** to **Edwardo**.

   You were able to make that change just fine.

   Now, let's see what happens when you change your user to be display only.
4. Close **Donald's** record, without saving the changes.
5. On the **Setup** menu, select **Security Setup**.
6. Select the **Display Only** check box.
7. Close the **Security Setup** screen, saving your changes.

   Before we go back into Donald's record to have a look-see, let's see how making a user display only affects the File menu and Shortcut Bar.
8. On the **File** menu, look for the **New Employee** option.

   It is not there. This is because you cannot create new records when you are set to display only.
9. On the Shortcut Bar, click **New Employee**.

   Nothing happens, because this shortcut has been disabled. You can tell that a shortcut is disabled when its caption is white instead of black. Also, when you move your cursor over a disabled shortcut, it does not highlight.
10. Now, open **Donald Stern's** record.

    Note that the color of all of the fields on the Personal screen is gray. This means that all fields are display only and cannot be changed.
11. Click in the **Middle Name** field.
12. Try to change **Donald's Middle Name**.

    No such luck.
13. Go to some other fields on the **Personal** screen and check those out.

    All are display only.

14. On the **File** menu, look for the **New Employee** option.

    Not there, just like on the Organizer desktop's File menu. You also won't see the Save, Delete, Copy and Transfer options. You are only allowed to select Open Employee, Close Employee and some other non-update options. In addition, you can see that the options that were missing on the File menu are also disabled on the Tool Bar.

15. Close **Donald'**s record.

    Ok, let's set your user back to having edit ability again.

16. On the **Setup** menu, select **Security Setup**.

17. Clear the **Display Only** check box.

    As you can see, there are several other setting on this General tab that we have not discussed yet. You will learn more about these settings when you take other training courses.

18. Close the **Security Setup** screen, saving your changes.

19. Continue with the next tutorial.

Tutorial 1.4 – Securing Companies and Modules

You can give each user access to the companies and modules he needs and remove access to those he does not. Here's how.

1. On the **File** menu, select **Select Company** to display a list of the companies to which you currently have access, excluding your current company. There should be one: **ARCHIVE**. Click **Cancel** to close the screen.

2. Select the **Security Setup** option and click the **Company** tab.

   The tab shows a list of the companies that have been defined. This list will be dynamic and will change as companies are added or deleted.

3. Clear the **ARCHIVE** check box.

4. While you are at it, try to clear the **ACTIVE** check box as well.

   As you can see you cannot deactivate your current company. If you were updating another user besides yourself, you would not be allowed to deactivate all of the companies.

5. Close the **Security Setup** screen, saving your changes.

6. On the **File** menu, look for the **Select Company** option.

   It is not there. This is because you now only have access to one company, ACTIVE. This is your current company, so there is no other company to select. In this case, the Select Company option is not available.

7. On the Shortcut Bar, click **Select Company**.

   Nothing happens, because this shortcut has been disabled. As you learned in the last tutorial, you can tell that a shortcut is disabled when its caption is white instead of black.

8. On the **Setup** menu, select the **Security Setup** option and click the **Company** tab. Restore access to **ARCHIVE**. Close the **Security Setup** screen, saving your changes.

9. Use the **Select Company** process to confirm that the **ARCHIVE** company has been reactivated. Close the screen.

   Now, let's restrict access to a module. The DEMO user has access to all modules. Note that you see the Safety Management module listed in the list of modules.

10. Select the **Security Setup** option.

11. On the **Module** tab, clear the **Safety Management** check box.

12. While you are at it, try to clear the **Personnel Management** check box as well.

    As you can see you cannot deactivate your current module. If you were updating another user besides yourself, you would not be allowed to deactivate all of the modules.

13. Close the **Security Setup** screen, saving your changes.

You should no longer be able to see Safety Management in the list of modules because you no longer have access to it.

14. Use the **Security Setup** process to reactivate the **Safety Management** module.
15. Close the **Security Setup** screen, saving your changes.
16. Continue with the next tutorial.

Tutorial 1.5 – Copying and Clearing Security

The Security Setup process, as well as the Security Setup - Module process you will learn about in the next lesson, allows you to copy security from another user as well as clear security for a user. We will learn about each of these features in this tutorial.

First, let's talk about copying security. Typically, when you are creating a new user that is similar to an existing user, you would use the Copy User in User Setup to create the new user and then make any changes that are unique to the new user. If you have an existing user that you later want to have the security controlled by another user, you would use the Group Name setting you learned earlier in this lesson. But, there might be times when you want to copy the security from one user to another and then change some settings after that. That is when you would use the Copy Security from User feature. Let's give it a whirl by copying the DEMO user's security settings to the MASTER user.

1. On the **Setup**, select **Security Setup**.

2. Verify that the **Display Only** check box is not selected for the **DEMO** user. You should have cleared that check box at the end of an earlier tutorial.

3. Select the **MASTER** user.

4. Select the **Display Only** check box.

   We now have the DEMO and MASTER users different on at least this one setting.

5. On the **File** menu, select **Copy Security from User.**

   The Copy Security from User screen is displayed.

6. In the **From User ID** field, enter **DEMO**. Click **Copy**.

   The security settings (specified in Security Setup and Security Setup - Module) for the DEMO user are copied to the MASTER user. To verify this, you should now see that the Display Only check box is cleared for the MASTER user. You would now typically change any settings that might be unique for the MASTER user.

   Now it's time to try the Clear Security for User option. First, let's make some security setting changes for the MASTER user so we can see what the Clear feature does with those settings.

7. On the **General** tab for the **MASTER** user, select the **Display Only** check box.

   All of the check boxes from Administrator down to the bottom of the tab are now selected.

8. On the **Company** tab, clear the **ARCHIVE** check box.

9. On the **Module** tab, clear the **Safety Management** check box.

10. Click the **General** tab so we can see where most of the changes will occur when we clear security.

11. Click the **Save** button to save all of these changes.

12. On the **File** menu, select **Clear Security for User.**

    The following message is displayed:

    Clear all security for MASTER

13. Click **Yes**.

    The security for MASTER is cleared. This means that the MASTER user now has unrestricted access, except for the following settings on the General tab, which are set to disabled (check box not selected):

    - Administrator
    - Show All Users in Inbox
    - Create Freeform Reports
    - Run Freeform Reports

14. These four settings give a user a lot of "power" so these can only be set manually.

15. Confirm that the settings listed above are now cleared. In addition, confirm that the **Display Only** flag has been cleared because this was a restriction that is now removed.

16. On the **Company** tab, confirm that the **MASTER** user now has access to the **ARCHIVE** company again.

17. On the **Module** tab, confirm that the **MASTER** user now has access to the **Safety Management** module again.

    As you can see, the Clear Security for User helps you to easily restore all access to a user. You can then make changes to the security as necessary.

18. Close **Security Setup**.

19. Continue with the next tutorial.

Lesson 2
Security Setup - Module

Lesson Contents

This lesson covers the key, module-specific settings in the Security Setup - Module process.

Tutorials

Setting Record Security: demonstrates how to set security at the record level.

Securing Menu Options: shows how to secure the menu options.

Securing Categories: demonstrates how to secure categories.

Securing Workflows, Activities and Processes: shows how to secure workflows, activities and processes.

Securing Tables, Screens and Documents: demonstrates how to secure tables, screens and documents.

Setting Field Security: shows how to set security at the field level.

Tutorial 2.1 – Setting Record Security

In People-Trak, record security is provided by using a filter to define what records are accessible. Let's see how this works.

1. On the **Setup** menu, select **Security Setup** and make sure the **Administrator** check box is cleared. Close the **Security Setup** screen, saving your change if necessary.

   This is necessary in order to see the changes we make in the Security Setup - Module process take effect. If we were an Administrator, all of our changes would be ignored because Administrators have full access no matter what the security settings are.

2. Click the **Open Employee** shortcut to start the lookup process.

3. Click the **Search** button to generate a list of all of the employee records in the ACTIVE company. Note the employee records that you can now see in the list.

4. Click the **Cancel** button to exit the **Lookup** screen without selecting a record for editing.

5. On the **Setup** menu, select **Security Setup - Module**.

   The Security Setup for Personnel Management screen is displayed with the Record tab open, which contains the standard query grid.

   Let's set our record security to only records where the Last Name starts with "S".

6. Enter the following query, as described below:

   Last Name Starts S

   Last Name is a field name and should be entered in the Field Name column. "Starts" is an operator and should be entered in the Operator column. "S" is the contents we are comparing and should be entered in the Contents column. We will not be using the "(", ")", Link, or the Row Mod columns for this example. Simply leave these blank.

7. Click the **Test** button.

   You will see the results of the query in the Record Security Result Listing, which should list all employees with a last name that starts with "S".

8. Close the **Document Viewer**.

9. Close the **Security Setup for Personnel Management** screen.

10. Click the **Open Employee** shortcut. Click the **Search** button to generate a list of all of the records in the ACTIVE company.

    This list will now be subject to the security just established. Note that the list only includes last names that start with "S".

11. Click the **Cancel** button to exit the **Lookup** screen without selecting a record for editing.

12. Select the **Security Setup - Module** option.

13. Click on the **Last Name** row in the query grid.

14. On the Tool Bar, click the **Delete Row** button to remove the query statement we added.

15. On the Tool Bar, click the **Save** button to save your changes and stay in the **Security Setup for Personnel** Management screen.

16. Continue with the next tutorial.

Tutorial 2.2 – Securing Menu Options

The Menu tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the menus (Audit, File, Documents, Templates and Tools) that are the same across all modules. The list box on the right displays the menu options for the highlighted menu. Let's define what options are available on these menus for our DEMO user.

1. You should still be in the **Security Setup for Personnel Management** screen.

2. On the **Menu** tab, select the **File** menu in the middle list box. Clear the **New Employee** check box. For the **Documents** menu, clear the **Adhoc Reports** check box. For the **Templates** menu, clear the **Email Templates** check box. For the **Tools** menu, clear the **Maintain Tables** check box.

3. Close the **Security Setup for Personnel Management** screen, saving your changes.

   Now, let's confirm that the security works.

4. Click the **File** menu and leave that menu displayed.

   Note that the New Employee option is no longer on the menu.

5. Move the cursor over to the **Documents** menu and leave that menu displayed.

   Note that the Adhoc Reports option is no longer on the menu.

6. Move the cursor over to the **Templates** menu and leave that menu displayed.

   Note that the Email Templates option is no longer on the menu.

7. Move the cursor over to the **Tools** menu and leave that menu displayed.

   Note that the Maintain Tables option is no longer on the menu.

   The Shortcut Bar is also secured using the File menu settings. Let's verify this.

8. Click the **New Employee** shortcut on the Shortcut Bar.

   As you can see, you cannot access this option as a shortcut either. Note that the Edit Table and the Documents shortcuts have also been disabled. The Documents shortcut was disabled because it is used to access Adhoc Reports, which you disabled on the Documents menu.

   These menu security settings apply only to the current module.

9. Select the **Safety Management** module and look at the menus you changed.

   Those menus have not been changed at all. We only changed those menus for the Personnel Management module.

10. Return to the **Personnel Management** module.

11. Use the **Security Setup - Module** process to restore access to all of the menu options you disabled.

12. Close the **Security Setup for Personnel Management** screen, saving your changes.

    Let's just do a quick check of one of the menus we originally changed to see that everything is back to normal.

13. Click the **File** menu and leave the menu displayed.

    Verify that the New Employee option you just reactivated is listed again on the menu.

14. Click off the menu to close it.

15. Continue with the next tutorial.

Tutorial 2.3 – Securing Categories

Workflows, Activities, Processes, Tables, Screens, Fields and Documents all have a category assigned to them. If you secure a category, you automatically secure all of the items in that category. This makes setting security very easy and thorough. If you do not allow access to a category, all of the items in that category are automatically set to no access as well and cannot be changed. Let's secure a category and see how this works.

1. On the **Setup** menu, select **Security Setup - Module**.

2. On the **Category** tab, clear the **Attendance** check box to deny access to this category.

   The following message is displayed:

   Access to all items in this category has been denied.

3. Click **OK**.

   Let's verify that this is true.

4. Click on each of the tabs to the right of the **Category** tab and confirm that all of the settings are now cleared.

   The Workflow through Document tabs are all based on category. When you secured the Attendance category, all of the items in that category were automatically secured.

5. On the **Document** tab, try to select one of the documents in the **Attendance** category.

   You are notified that you cannot grant access to this item because the parent category is secured. This is true with any of the items controlled by category.

6. Close the **Security Setup for Personnel Management** screen, saving your changes.

   Let's take a look at a couple of the items that have now been secured in the Attendance category.

7. On the **Documents** menu, select **Adhoc Reports**.

   You won't be able to find any of the documents in the Attendance category in the All Adhoc Reports category listing on the right. It so happens that you also won't see an Attendance category in the list of categories on the left. Keep in mind that the categories when in the Explorer are Explorer categories, not the secured categories. The reason the Attendance Explorer category disappeared in this case was because the documents in the Attendance category that we secured also had Attendance as their Explorer category. This might not always be the case. The key thing to know is that if you secure a category, any documents assigned to that category will no longer be accessible using any method.

8. Close the **Adhoc Reports** screen.

9. On the **Tools** menu, select **Maintain Tables**.

   Again, the Attendance category is not listed in the category listing on the left and the tables in that category are not in the All Tables listing either.

10. Close the **Maintain Tables** screen.

    Let's check one more place.

11. In the **Categories** pane, look for the **Attendance** category.

    It isn't there because that category has been secured. We won't take the time to confirm that the category is secured in all the other places that it could be. You will have to trust me that this category has its hatches battened down.

12. On the **Setup** menu, select **Security Setup – Module.**

13. On the **Category** tab, select the **Attendance** check box to give access to this category.

14. Click on each of the tabs to the right of the **Category** tab and confirm that all of the settings are now selected.

15. On the **Document** tab, clear one of the document check boxes in the **Attendance** category.

    You can do this because that category is not secured. This is true of any of the items controlled by category. You can have the category not secured and then pick and choose which items in that category to secure, if any.

16. Select the document check box you just cleared.

17. Close the **Security Setup for Personnel Management** screen, saving your changes.

18. In the **Categories** pane, look for the **Attendance** category.

    It is there now, as it should be.

19. Continue with the next tutorial.

Tutorial 2.4 – Securing Workflows, Activities & Processes

As we learned in the last tutorial, Workflows, Activities and Processes are just some of the items that can be secured by category. If you secure a category, you automatically secure all of the items in that category and you cannot change those settings. In our case, we have no categories secured, so we can pick and choose what items we want to secure. Let's start with securing workflows.

1. On the **Setup** menu, select **Security Setup - Module.**

2. Click the **Workflow** tab.

   This tab contains three list boxes. The list box on the left displays the users. The list box in the middle displays the categories. The list box on the right displays the workflows in the highlighted category. Let's change a few settings and try it out.

3. In the **Personal** category, clear the check box for the **Name and Address** workflow and any other workflows in that category

4. In the **User** category, clear the check box for the **Standard - Employee** workflow and any other workflows in that category.

   You have just removed access to the DEMO user's default workflow and all available workflows in a category. We will see what that affects in a minute.

5. Click the **Activity** tab.

   This tab is just like the Workflows tab, except it is for Activities.

6. In the **Personal** category, clear the check box for the **Employee Manager** and any other activities in that category.

7. Click the **Processing** tab.

   This tab is also just like the Workflows tab, except it is for Processing.

8. In the **Attendance** category, clear the check box for the **Attendance Batch by Employee** process.

9. Close the **Security Setup for Personnel Management** screen, saving your changes.

   Now, let's confirm that the security works. The Standard - Employee workflow is the DEMO user's default workflow, so we should not be able to use the standard record functions to access that workflow.

10. On the Shortcut Bar, click **New Employee.**

    Nothing happens, because this shortcut has been disabled. The Open Employee shortcut is also disabled.

11. Open the **File** menu and note that the **New Employee** and **Open Employee** options are not listed. Click off the menu to close it.

12. In the **Categories** pane, open the **User** category.

Since you secured all the workflows in that category, you should not even see a Workflows subcategory anymore.

13. In the **Categories** pane, open the **Personal** category.

    The Activities subcategory is no longer listed because all the activities in this category have been secured.

14. In the **Categories** pane, open the **Attendance** category and then open the **Processing** subcategory.

    The Attendance Batch by Employee should no longer be listed.

    The Workflows menu is no longer displayed because you secured all of the workflows available on that menu in the current module.

15. Move to the **Activities** menu and leave that menu displayed.

    The activities that you deselected in the Personal category, including Employee Manager, are no longer listed.

16. Move to the **Processing** menu and leave that menu displayed.

    The Attendance Batch by Employee is no longer listed.

    All security worked like a charm! Now, let's reset everything back to the way it was.

17. Use the **Security Setup - Module** process to restore access to the workflows, activities and processing you disabled.

18. On the Tool Bar, click the **Save** button to save your changes and stay in the **Security Setup for Personnel Management** screen.

19. Continue with the next tutorial.

Tutorial 2.5 – Securing Tables, Screens & Documents

Tables, Screens and Documents are also secured by categories. Since we have no categories secured right now, we can pick and choose what items we want to secure. Let's start with securing tables.

1. You should still be in the **Security Setup for Personnel Management** screen.
2. Click the **Table** tab.

   This tab, as well as the Screens and Documents tabs you will see in a minute, has the same three list boxes as the tabs we just saw in the last lesson.
3. In the **Attendance** category, clear the check box for the **Attendance Account** table.
4. On the **Screen** tab, in the **Status** category, clear the check box for the **Status** screen.
5. On the **Document** tab, in the **Compensation** category, clear the check box for the **Average Salary by Gender** document.

   Now, let's verify that this security is now in effect.
6. Close the **Security Setup for Personnel Management** screen, saving your changes.
7. On the **Tools** menu, select **Maintain Tables**.

   You should no longer be able to see the Attendance Account table in either the All Tables list or the Attendance list.
8. Close the **Maintain Tables** screen.
9. On the Shortcut Bar, click **Open Employee** and open any record.
10. In the **Screen** dropdown, look for the **Status** screen, which should be the second screen in the list.

    It is not there because you can no longer access it. It also won't be available to you when in the Custom Screens process.
11. Close the record.
12. On the **Documents** menu, select Adhoc Reports.
13. In the **All** category, look for the **Average Salary by Gender** document.

    It is not there as expected. Now would typically be the time we would look in the category to see if it is there, but the Explorer screen is unique. The categories you are seeing here are explorer categories, not the categories that are used for security. In the case of Average Salary by Gender, it has a category of Compensation, but an explorer category of EEO. The explorer categories can be anything you want and you can have as many as you want. So, in our case, we would need to check the EEO category to see if Average Salary by Gender is still there.

14. In the **EEO** category, look for the **Average Salary by Gender** document.

    It is not there.

15. Close the **Adhoc Reports** screen.

    The table and document we secured will also not show up in the Categories pane either. We won't take the time to confirm that now. Just know that wherever an item might show up, it will not be available if it is secured for the current user.

16. Use the **Security Setup - Module** process to restore access to the items you secured in this lesson.

17. Close the **Security Setup for Personnel Management** screen, saving your changes.

18. Continue with the next tutorial.

Tutorial 2.6 – Setting Field Security

Unlike the other security settings, field security has three different states. Fields can be set to Full Access, Display Only or No Access. Here's how to do it.

1. Open **Donald Stern's** record.

2. Click in the **First Name** field and note that this field is completely editable. Click in the **Last Name** field and note that this field is also completely editable.

   Now, let's secure them.

3. Close **Donald Stern's** record, without saving any changes you might have made.

4. On the **Setup** menu, select **Security Setup - Module**. Click the **Field** tab.

   This tab looks similar to the others we were just working with, except it is for fields and there are no check boxes. There is also a special Notes category at the bottom, which lists the note fields. You can easily secure one or all of those note fields for the current module. The Notes screen itself can be secured in Security Setup, and if the Notes screen is visible to a user, secured categories of notes are not.

5. In the **Personal** category, look for the **First Name** field.

   Note that the First Name field currently is set to Full Access.

6. Click anywhere in the row that includes the **First Name** field, which will highlight that row, and then click there again.

   This changed the access to Display Only.

7. Click anywhere in that row again.

   Now the access is No Access.

8. Click again to toggle the **First Name** field access back to **Display Only**.

9. Still in the **Personal** category, find the **Last Name** field and toggle that field's access until it is **No Access**.

10. Close the **Security Setup for Personnel Management** screen, saving your changes.

11. Click the **Open Employee** button on the Shortcut Bar.

    The Lookup screen is displayed. One of the lookup fields is Last Name. Any field that you select as a lookup field will be viewable by all users because Lookup ignores field security. You should never include a field in the Lookup that cannot be viewed by all users. We have restricted Last Name access for our demonstration but it would be highly unusual to ever restrict access to a field that is used as a lookup field.

12. Open **Donald Stern's** record.

13. In the **First Name** field, try to enter something.

You can't because this field was set to Display Only status. You can put the cursor in the field, but you cannot edit the field.

14. Now click in the **Last Name** field.

    Whoops, it's not there. We set this field to No Access and thus the field cannot be seen or edited. If a report has the Last Name field on it, you will not be allowed to run that report.

15. Close **Donald's** record.

16. Create an **Adhoc Report**. On the **Report Definition** tab, use the popup in the **Field Name** field. In the **Personal** category, look for the **First Name** and **Last Name** fields.

    The First Name field is there because it is set to Display Only, so you can still see the field's data. The Last Name is not there because it is set to No Access. When a field is set to No Access, it cannot be seen anywhere. If you tried to create a Custom Screen, it would not be available in that Select Field popup either.

17. Use the **Security Setup - Module** process to set the **First Name** and **Last Name** fields back to **Full Access**.

18. Close the **Security Setup for Personnel Management** screen, saving your changes.

    We have now concluded our training on security setup, so we need to become all powerful again. Let's set the DEMO user back to Administrator so we can have full access to the Setup and Administration menus in order to be able to do the rest of the lessons.

19. On the **Setup** menu, select **Security Setup.** Select the **Administrator** check box.

    Ahh, that feels much better. We now have complete control again!

20. Close the **Security Setup** screen, saving your changes.

21. Exit **People-Trak**.

22. This concludes this tutorial and lesson.