

Florida Department of Transportation

Trns•port

Security Coordinator Guide

PREPARED BY:
CAPSTONE ENGINEERING ASSOCIATES

SEPTEMBER 2005



Introduction

This User Guide describes the procedures involved in establishing and maintaining user security in the production environment of the Trns•port Cost Estimation System (CES), Trns•port Proposal and Estimate System (PES), the Trns•port Letting and Award System (LAS) and SiteManager the construction management system (S/M). It is intended to be used by both Central Office and District Office Security Coordinators.

There are two elements that control the security of the Department's data in the Trns•port database. These are the granting of access to individuals to particular Trns•port systems, and the granting of particular authority within each system. There are two processes that you will deal with in your capacity as a Security Coordinator – in CES/PES/LAS it is Roles and Users, in SiteManager it is User Groups and Users. As a Central Office Security Coordinator, you will have authority to create and modify Roles and User Groups, add users to the system, and assign security authority to them. As a District Security Coordinator, you will not be able to create or modify any Roles or User Groups, you will add users to the system, grant them security authority, and modify their authority as directed by managers.

The Trns•port Security Plan, as well as other Department documents, defines the responsibility of a Security Coordinator as “a Department employee responsible for monitoring and implementing security controls and procedures for a computer system. Computer Security Coordinators are only established by the Computer Security Administrator for a specific user and/or group of users.”

Central Office Security Coordinators have been appointed by appropriate managers to carry out their responsibilities in specific Trns•port systems, both within the Central Office and statewide, for users in their functional area of either production project management or maintenance project management. They have the responsibility of the Computer Security Administrator noted above. In a similar manner, District Office Security Coordinators have been appointed to carry out their responsibilities in Trns•port systems within their Districts.

The responsibility of both Central and District Office Security Coordinators is the same except for the ability to create, modify, and delete Security Roles. This authority to create or modify Security Roles has been given only to Central Office Security Coordinators.

Two things are required before granting access to new users. First, that the user has been assigned a Department UserIdentifier (USERID) in accordance with Resource Access Control Facility (RACF) procedures, and second, that an appropriate manager has indicated the responsibility that the new user is to be given.

Table of Contents

Introduction	2
1. CES/PES/LAS.....	5
1.1 Security Roles.....	5
1.1.1 Creating Security Roles	6
Assigning Tokens to a Role	7
1.1.2 Changing Security Roles	8
Adding Additional Tokens to a Role	9
Deleting Tokens from a Role.....	9
1.1.3 Copying Security Tokens from One Role to Another	9
1.2. Adding and Maintaining Users.....	11
1.2.1 Users	11
Adding a User	11
Deleting a User	13
Changing User Information	13
1.2.2 Systems and Users	13
Specifying a System Identifier.....	13
Adding a System Identifier	14
Changing a System Identifier.....	15
Deleting a System Identifier	16
1.2.3 Roles and Users	16
Assigning Roles to Users.....	16
Deleting Roles from Users.....	17
1.2.4 Listing Users.....	18
1.2.5 Users Changing Jobs or Leaving FDOT.....	18
2. SiteManager	21
2.1 Background.....	21
2.2 Security Hierarchy.....	21
2.3 Naming Conventions	22
2.5 Adding and Maintaining Users.....	22
2.5.1 Adding Users	23
User Data	23
Security Groups	24

2.5.2 Deleting a User	25
2.5.3 Changing User Information	25
User Data	25
Security Groups	27
Appendix A. Control Group.....	28

1. CES/PES/LAS

Having received direction from an appropriate manager, the Security Coordinator will proceed to add or change a user as specified by the manager.

If you are a LAS Security Coordinator, you should access LAS to transact all security functions. If you are a CES/PES Security Coordinator, you should access PES.

The figures that follow show PES screens, but the steps are the same in CES, PES, and LAS.

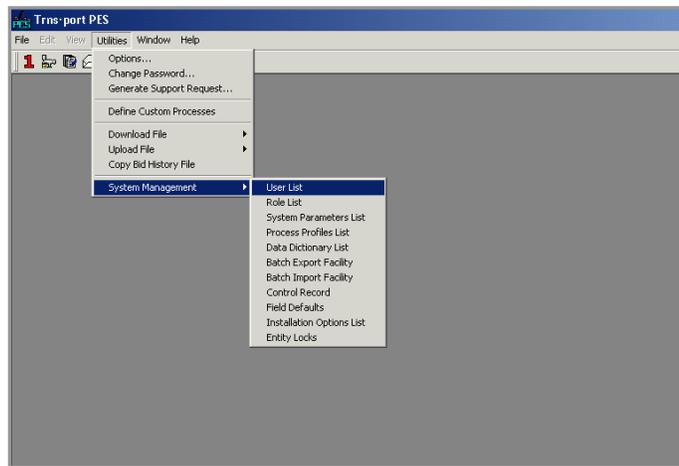
The User List utility allows you to maintain the list of authorized users, the systems they are authorized to use, their security role(s), and their Access Control Group information. Many Trns•port windows will indicate access to Contract Administration System (CAS). However, the Department does not use CAS.

To add, change, or list users, or to add, change, delete, or list Roles, begin on the main LAS screen.

- Click **Utilities** on the Menu Bar.
- Click **System Management**.
- Click **User List** if you are to add a user.

Or

- Click **Role List** if you are to add, change, or delete a Role.



1.1 Security Roles

A security Role is a name associated with a set of security tokens. PES and LAS each have over 300 security Tokens, each of which allows performance of a particular function. Examples are View Project Tabbed Folder, or Add Project, or Delete Project, etc.

The Role names used in CES, PES, and LAS are representative of typical users, and are divided by organizational function. An individual user must be assigned at least one security Role in order to perform functions within a system.

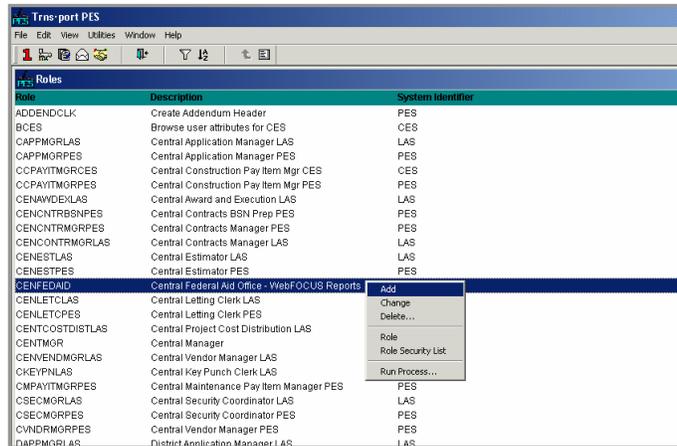
You can use security Roles to combine the tokens for several related tasks and to more efficiently provide users with access to the parts of the system they need. A user may be assigned any combination of security Roles and individual tokens. It is recommended that only Roles be used and that users not be given individual tokens in addition to those roles. If a particular Role does not meet the requirements for a task, you may create a new Role. By having all user access tied to security Roles, necessary changes to a Role will affect every user of that Role on his or her next log on. In this way, security requirements may be maintained in a consistent manner.

1.1.1 Creating Security Roles

To create a security Role, select System Management from the Utilities menu and choose Role List as seen above.

The Role List window will appear.

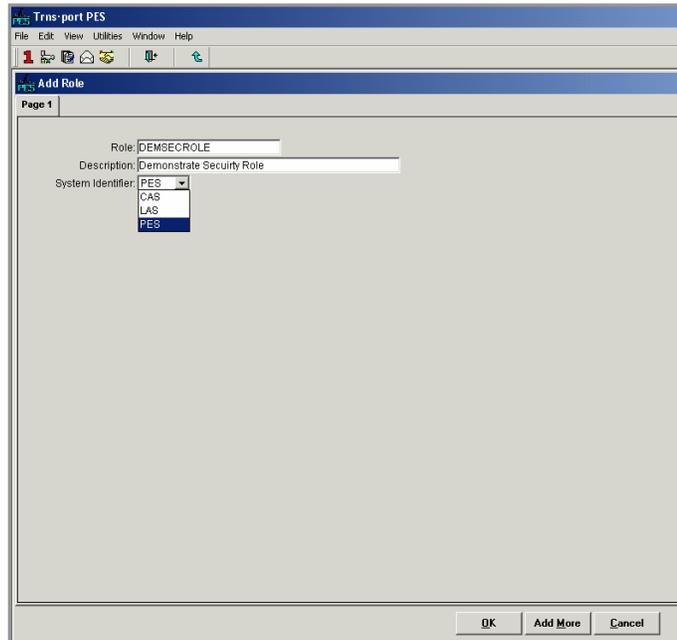
- Click **Add** from the right mouse button menu.



The Add Role detail window will appear.

- Enter the **Role** name in upper case letters.
- Enter a brief **Description** in upper and lower case letters.
- Click the **System Identifier** from the drop down list.
- Click **OK**.

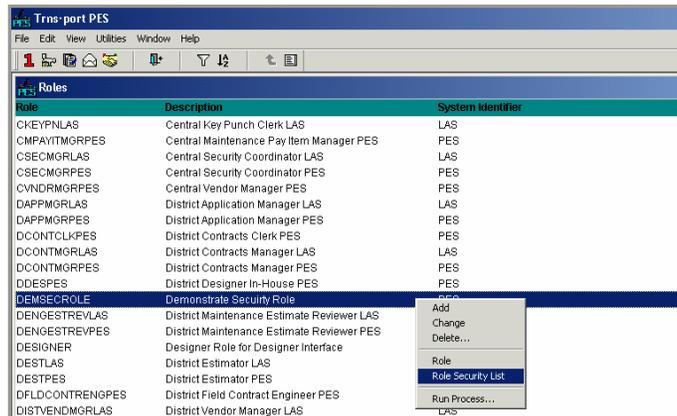
This will add the new Role to the Role List window.



Assigning Tokens to a Role

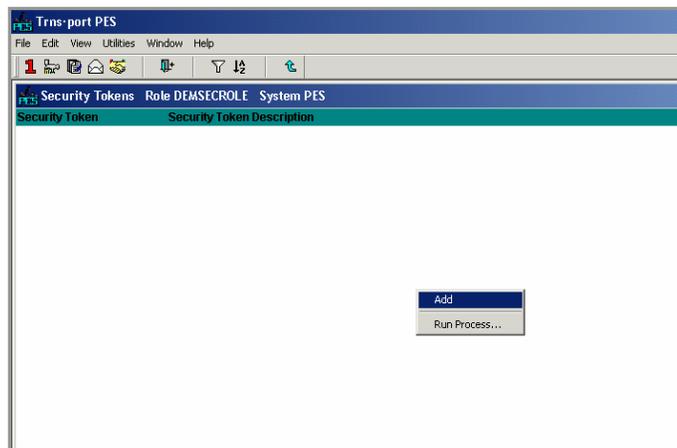
To assign security tokens to the new security Role,

- Click the new **Role** from the Role List.
- Click **Role Security List** from the right mouse button menu.



This will cause an empty Role Security List window to display. To assign tokens,

- Click **Add** from the right mouse button menu.



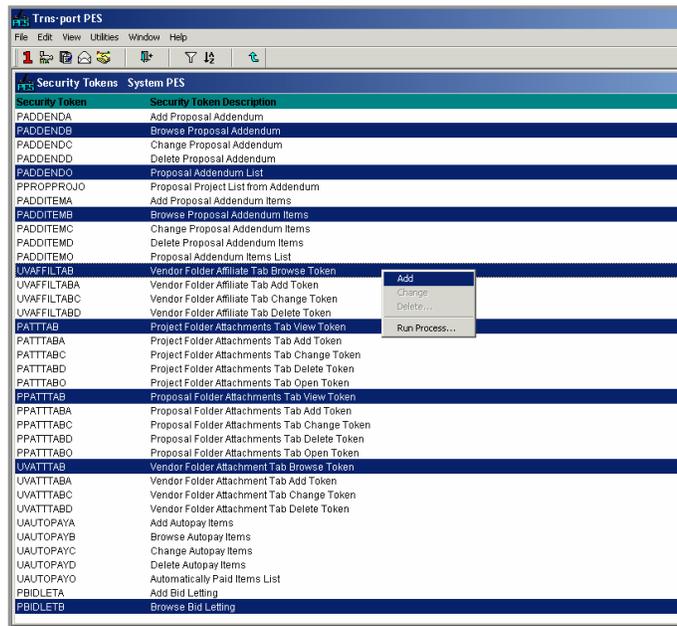
A window listing all the security tokens that exist for that System Identifier will be displayed.

- Click all the **tokens** you want to assign to the new Role.

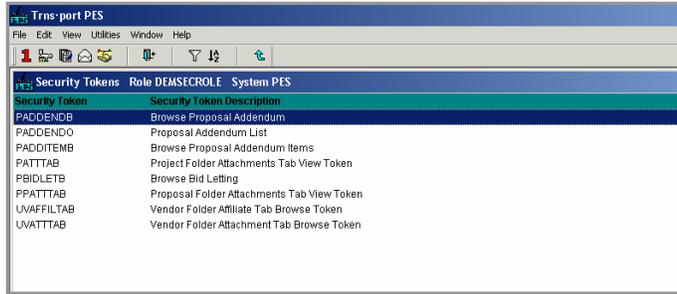
You can select more than one token by pressing and holding down the CTRL key until all desired tokens have been selected.

When you have selected all the tokens ensure that your cursor is on one of the blue bands and

- Click **Add** from the right mouse button menu.
- Click the **X** to close the Security Tokens list window.



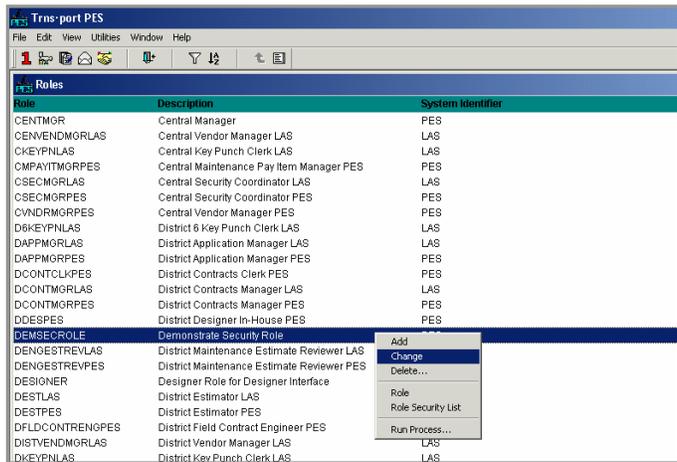
The tokens will be added to the new security Role and will be listed in the Role Security Tokens.



1.1.2 Changing Security Roles

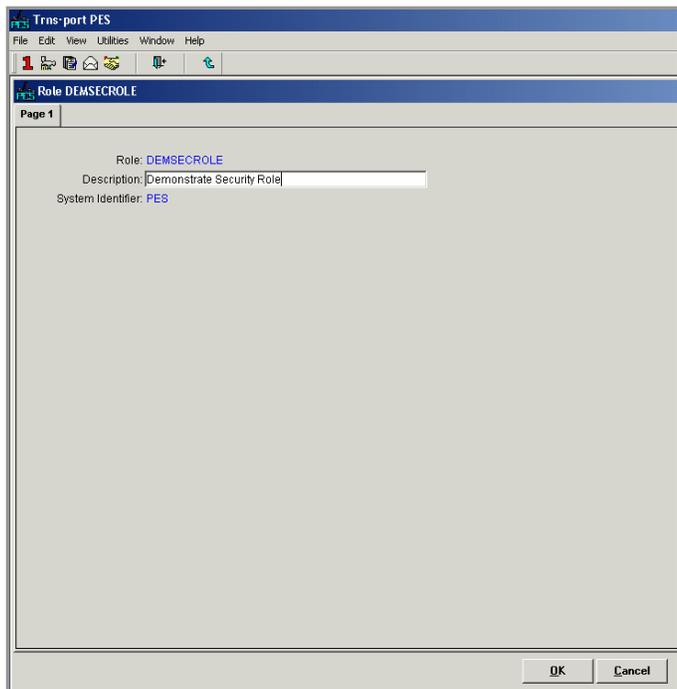
You can change the description of a security Role by selecting the Role in the Role List window and,

- Click **Change** from the right mouse button menu.



The Role detail window will be displayed.

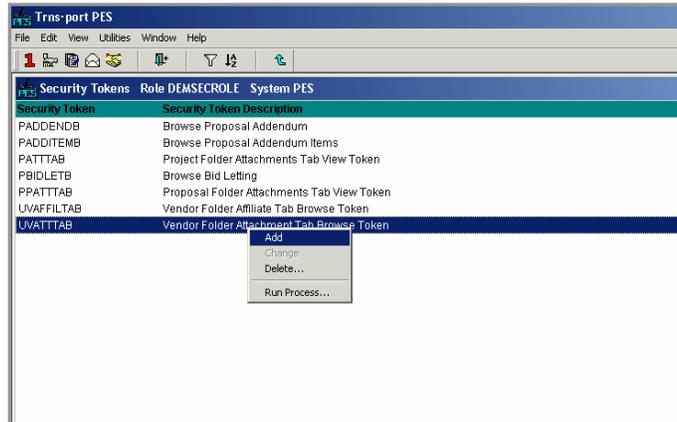
- Type the new information in the Description field.
- Click **OK** to save and close the window.



Adding Additional Tokens to a Role

To add to the tokens assigned to a security Role,

- Select the **Role** to change in the Roles List window.
- Choose **Role Security List** from the right mouse button menu.
- The Role Security Tokens List window will be displayed as seen here.
- Click **Add** from the right mouse button menu.



The System Security Tokens List window will be displayed. Select the token(s) you want as seen above in the process of creating the initial list of tokens.

- Close the System Token window by clicking the “X”.

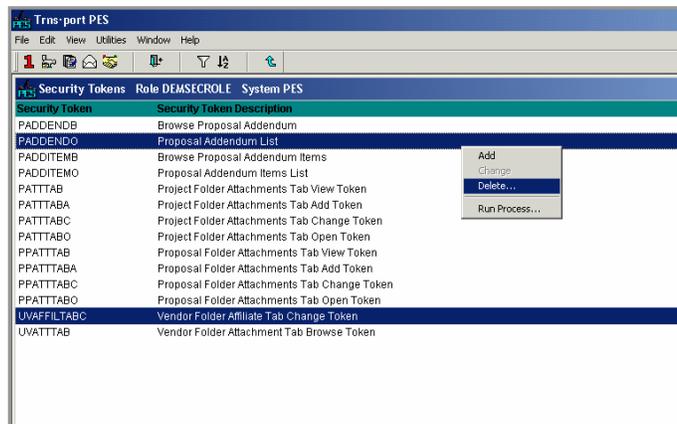
Deleting Tokens from a Role

To remove one or more tokens from a security Role,

- Click the **Role** to change in the Roles List window.
- Click **Role Security List** from the right mouse button menu.

The Role Security Tokens List window will be displayed.

- Click the **token(s)** to be removed.
- With the cursor on a blue band, Rclick the mouse and Click **Delete**.



1.1.3 Copying Security Tokens from One Role to Another

If a new Role has similar security requirements to an existing Role, you can copy the tokens of the existing Role into the new Role and then modify the new Role by either adding or deleting individual tokens. This is a fast, easy way to create a new Role.

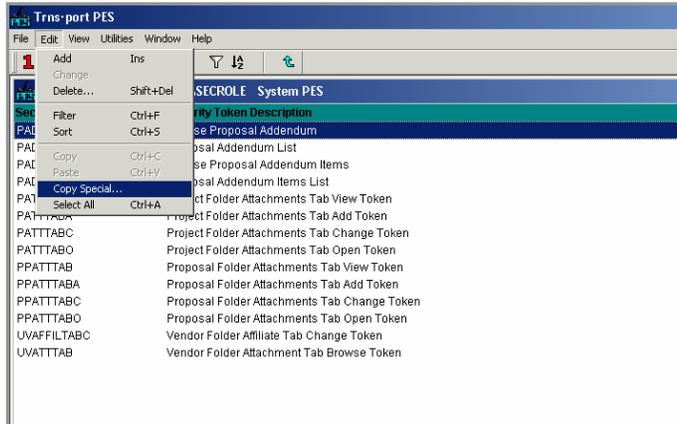
The Copy Special feature of Trns•port usually begins by selecting an existing entity and creating a duplicate from it. In this case, the logic is changed.

- Begin by adding a new Role header as illustrated above.

Or

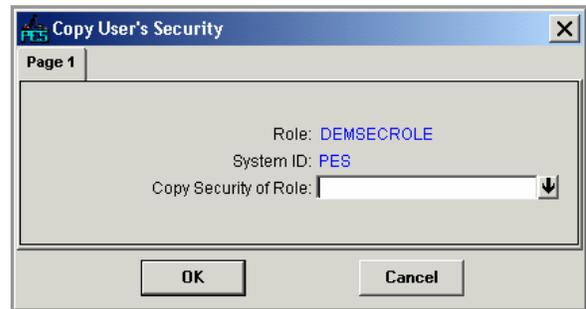
- Click an existing Role Header to which you want to add tokens.

Once the Role header is highlighted, open the Role Security List from the right mouse button menu. The List may be a blank screen, or may contain tokens.



- Click **Edit > Copy Special** from the Menu Bar.

A Role Security Transfer window will be displayed as seen here. The system automatically enters values in the Role and System ID fields.

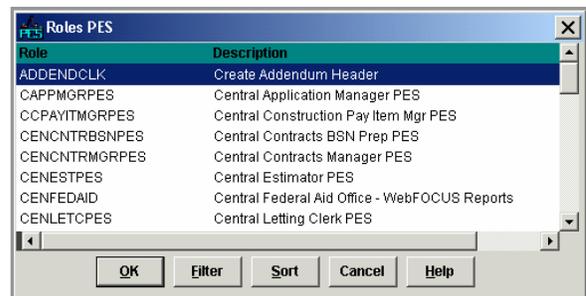


- Click the **down arrow** to display a list of all existing Roles for the selected system identifier.

- Click the **Role** from which you want to copy tokens and click OK.

Trns•port enters the Role in the Copy Security of Role field.

- Click **OK** in the Copy Security User's window.



The copy is now completed, and the token(s) have been added to the Role.

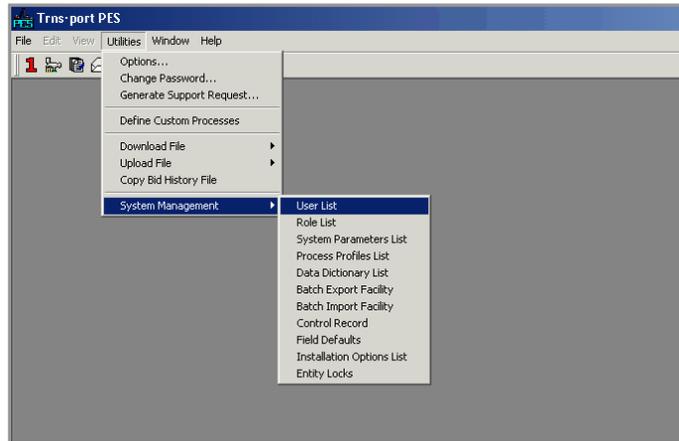
1.2. Adding and Maintaining Users

1.2.1 Users

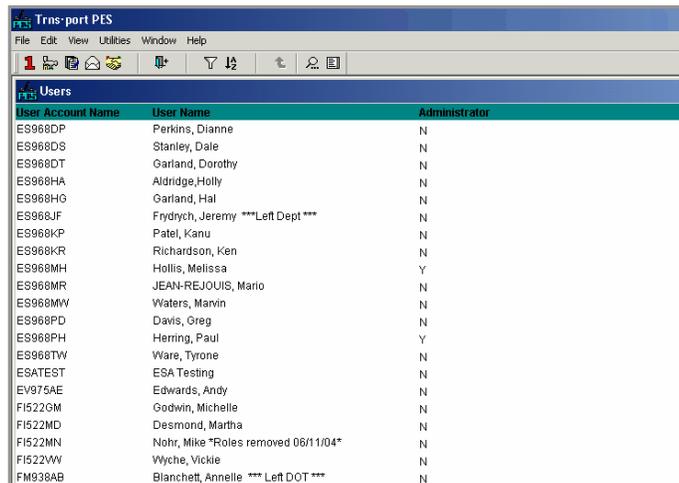
Adding a User

To add a user,

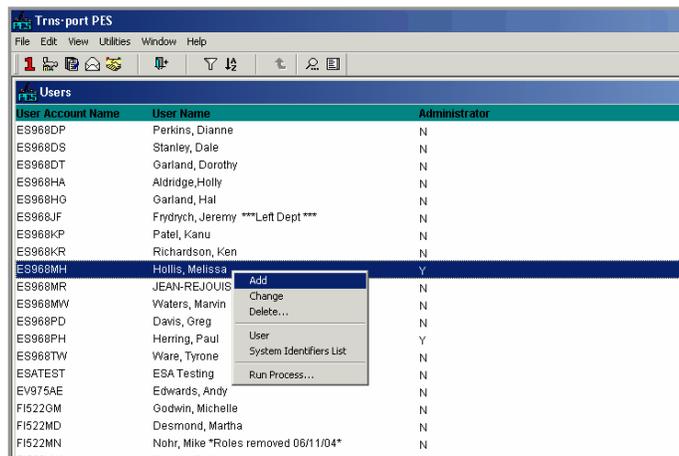
- Click **Utilities > System Management > User List** from the Menu Bar.



The User List window will appear.



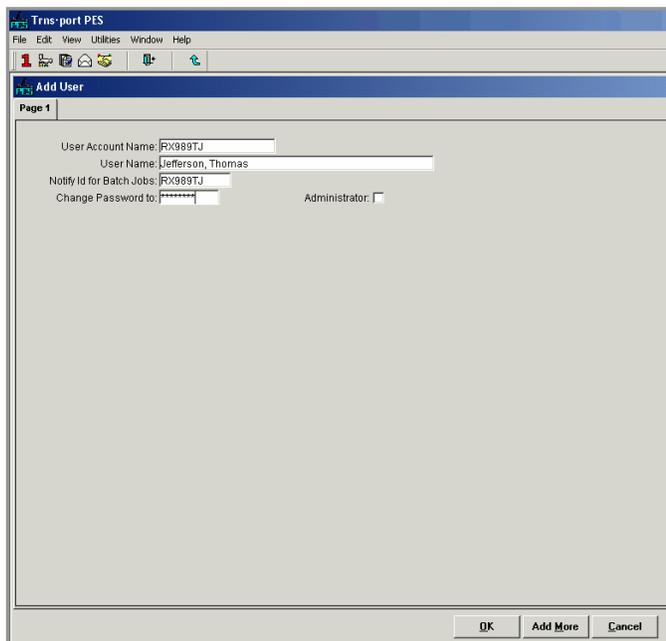
- Place the cursor anywhere in the window.
- Rclick and select **Add** from the right mouse button.



The Add User Detail Window will appear.

Enter data in the following fields.

- Enter *User Account Name* in **upper case letters**.
- Enter *User Name* in format of **Last Name, First Name** using standard capitalization.
- *Notify Id for batch Jobs* will fill automatically.
- *Change Password to*. Assign a temporary password having at least six but no more than 13 characters. Instruct the new user to change this temporary password the first time he or she logs on.



Administrator will only appear if the user that opens this window is an authorized System Administrator. If the Security Coordinator places a check in this box, the user that the record represents will also become a System Administrator. If it is cleared, the user will not have System Administrator authority. A System Administrator has access privileges above and beyond other users. An Administrator may open any window, regardless of what security Role or security tokens the Administrator has been assigned, and may set or clear another Administrator's flag. It is not expected that this authority will be granted to anyone outside of the Central Office.

- Click **OK** to add the new user, **Add More** to add another user, or **Cancel** to return to the User List window without adding a new user.
- ❖ ***User Account Name* is a required field, and is to contain the assigned Department RACF UserId. All Trns•port users must have a User Account Name to sign on to authorized systems. RACF UserIds are purged monthly and as a consequence UserIds can be and are reused. This leads to a problem in all Trns•port systems because UserIds are not deleted from any Trns•port system when a user leaves but all authority is removed. The UserIds remain tagged to historical transactions in the data bases. In instances where a new user is assigned a RACF UserId that duplicates a former Trns•port UserId, prior to continuing with the new user, the old Trns•port UserId is to be modified by appending the numeral 1 (or 2 or 3 if necessary) to the UserId. This is to be done by data base change so that all history is modified uniformly. Submit an email request to the Trns•port Coordinator to have this change made. After this change is made, the new user may be entered.**

Deleting a User

- ❖ While all Trns•port modules have a Delete capability for users, deletions are not to be made. SiteManager maintains transaction history by UserId, and PES/LAS are expected to do so in future releases. The maintenance of transaction history by UserId is desired.

Changing User Information

To change information about a user,

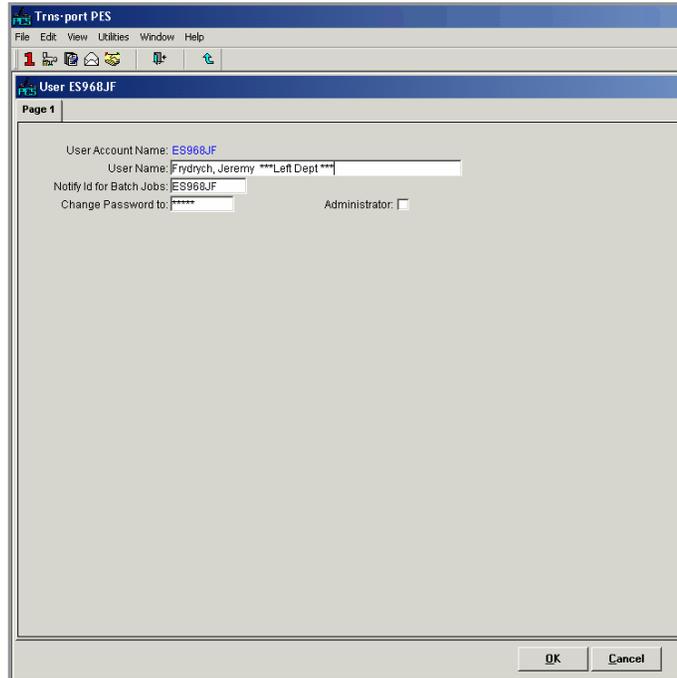
- Click the **user** in the User List window.
- Click **Change** from the right mouse button menu.

The User Detail window will be displayed.

You will notice that the *User Account Name* field is highlighted in blue. This means that it is not available to be changed by you. Throughout CES, PES, and LAS, when you encounter a field in blue, it may not be changed from that screen. In this example the *User Name* was modified to show *****Left Dept*****.

When you finish making your changes.

- Click **OK** to save the changes or **Cancel** to return to the User List window without saving changes. Changes in the database will only be made if you click **OK**.

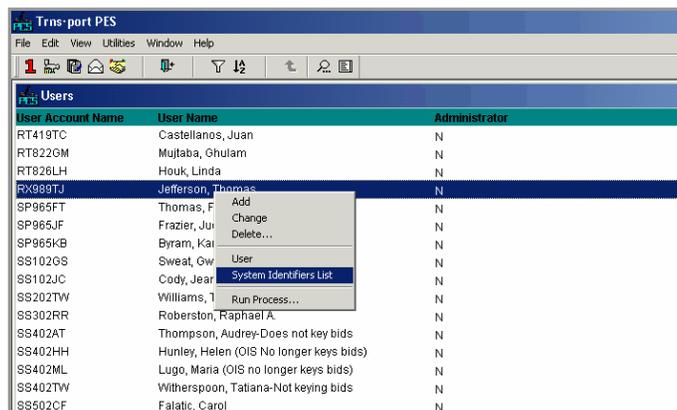


1.2.2 Systems and Users

Specifying a System Identifier

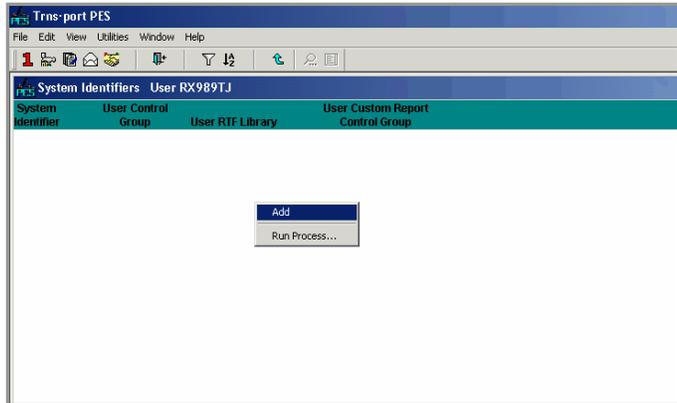
To specify the systems that users may access; the user Control Group that they are a part of; and other information to control system security; select the user in the User List window.

- Click **System Identifiers List**.



The System Identifiers List window for the selected user will be displayed. It may be blank as seen here or it may contain Systems if the user is not new.

- Rclick in the white space.
- Click **Add**.



Adding a System Identifier

To allow access to CES, PES, or LAS,

- Click **Add** from the right mouse button menu.

This will display the Add System Identifier window for the selected user.

- Enter data in the following fields.

System Identifier is a required field. It specifies which Trns•port system a user has access to. Type in CES, PES, or LAS as appropriate.

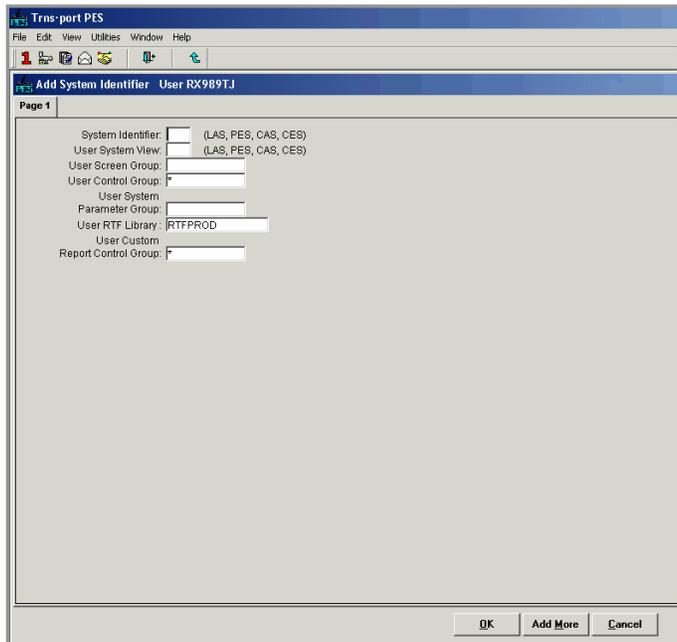
User System View is a required field. It defaults to the System Identifier you typed in, but is not currently used by Trns•port. You do not need to add anything to this field.

User Screen Group is not a required field and is not currently used.

User Control Group is a required field. It controls which group of projects or proposals a user may access. The information in this field must be entered in all capital letters (CAPS). Control Groups assigned to users may contain letters and numerals, or * and ? as wild cards. Control Groups assigned to projects or proposals may contain only letters and numerals. For further information on Control Groups, see Appendix A. Enter a Control Group for the new user.

User System Parameter Group is not a required field and is not currently used.

User RTF Library is a required field. It specifies the library for RTF templates used by batch processes. The default value is RTFPROD. You do not need to change it.



User Custom Report Control Group is a required field. It controls which group of custom reports a user may access with regard to viewing, adding, changing, or deleting. At present, all users are to be assigned the default value of “*.” You should not change it.

When you finish adding information,

- Click **OK** to allow the user to access the Trns•port system, **Add More** to allow the user to access another Trns•port system, or **Cancel** to return to the System Identifier List window without allowing the user to access another Trns•port system.

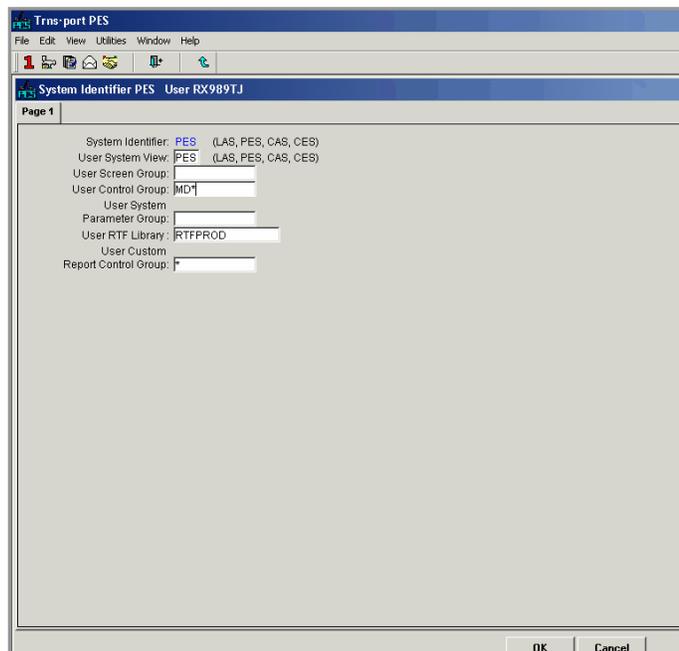
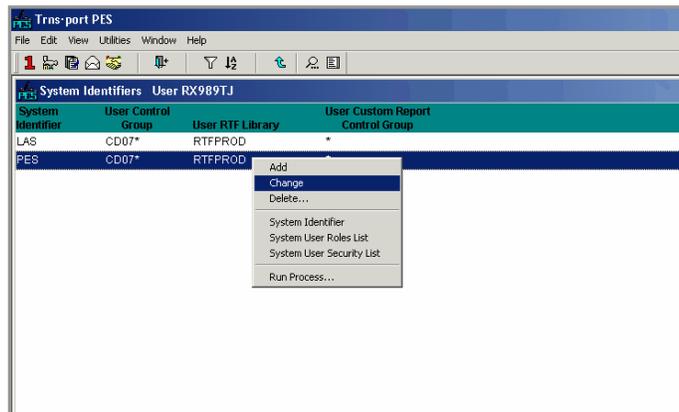
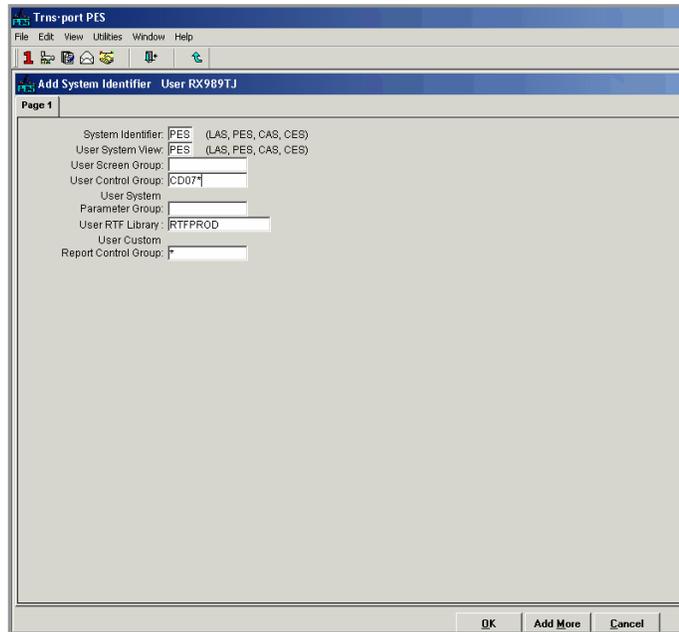
Changing a System Identifier

To change information concerning a Trns•port system for a user,

- Click the desired **system**.
- Click **Change** from the right mouse button menu.

The System Identifier window will be displayed as seen here. You may change any information except the System ID, which appears in blue. In this example, the Control Group was changed to *MD. When you finish making changes in the window,

- Click **OK** to save the changes to the database. Click **Cancel** to close the window without saving the changes.

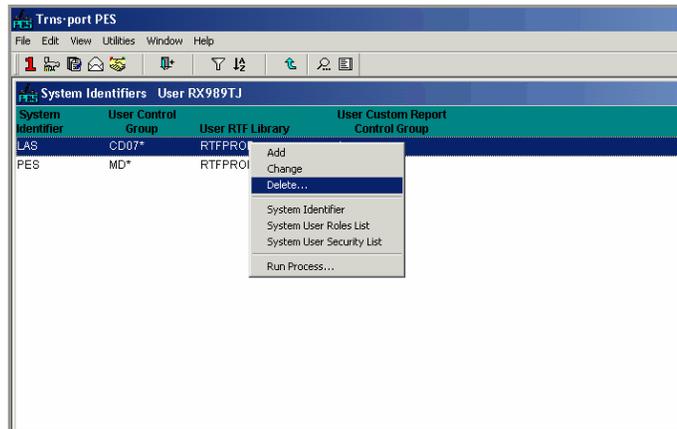


Deleting a System Identifier

To delete an existing System Identifier record for the user,

- Click the desired system(s)
- Click **Delete** from the right mouse button menu

A series of Delete warning windows will be displayed. Acknowledge each one.



1.2.3 Roles and Users

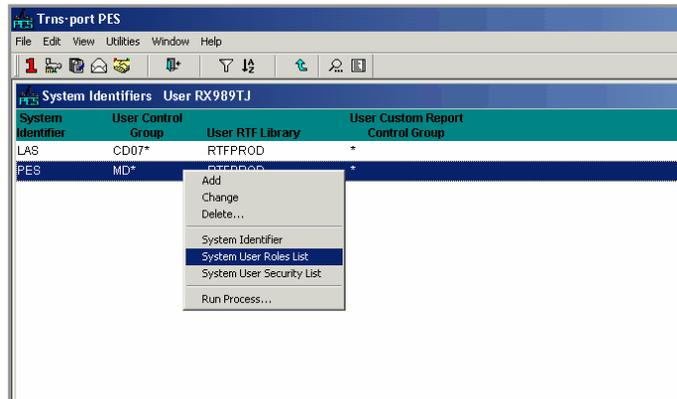
Assigning Roles to Users

To assign a security Role to a user,

- Click the **user** in the User List window.
- Click **System Identifier List** from the right mouse button menu.

The System Identifier List window will be displayed.

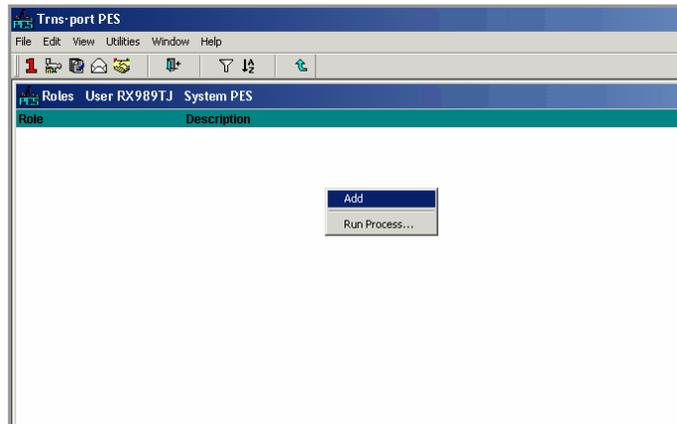
- Click the system for which you want to add a Role
- Click **System User Roles List** from the right mouse button menu.



The list window for security Roles assigned to that user for the system will be displayed. For a new user the screen may be blank.

To add security Roles for the user,

- Click **Add** from the right mouse button menu.

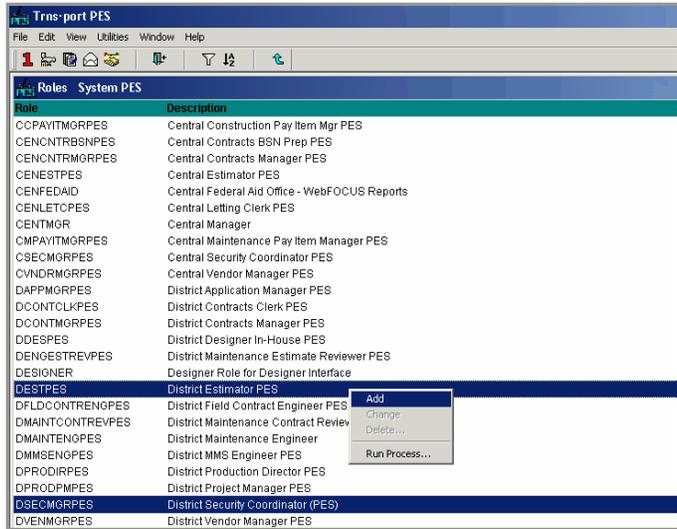


This will display a window listing all the Security Roles for the system.

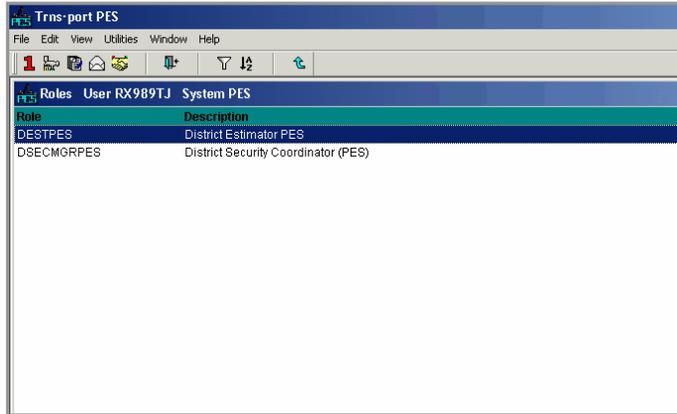
- Click a **Role** or **Roles** from the list and.
- Put the cursor on a blue band and click **Add** from the right mouse button menu.

When you finish adding Roles,

- Close the window by clicking the “X”.



The new Roles will be added to the user.



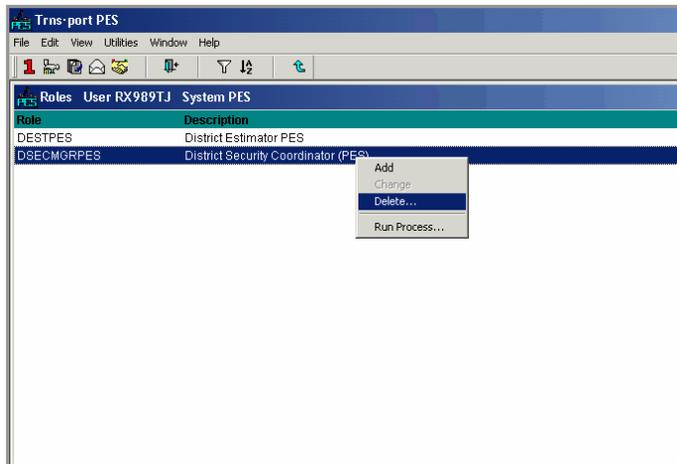
Deleting Roles from Users

To delete one or more Roles for a user,

- Click a **Role** or **Roles** in the Security Roles List window for the user.
- Click **Delete** from the right mouse button menu

A Delete warning window will be displayed.

- Click **YES** to complete the delete or **NO** to cancel it.



1.2.4 Listing Users

The List Users process produces a printed listing of selected user information, with which to review current user security.

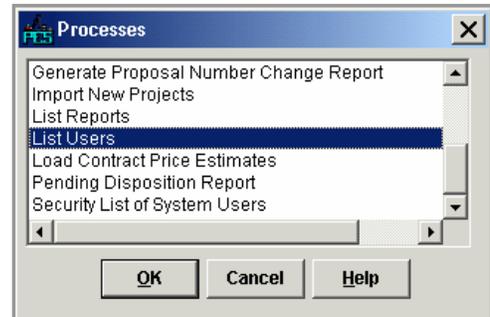
To produce a list of users,

- Click a **user** or **users** from the User List window.
- Click **Run Process** from the right mouse button menu.

User Account Name	User Name	Administrator
ES968AI	Ney, Allison	N
ES968DP	Perkins, Dianne	N
ES968DS	Stanley, Dale	N
ES968DT	Garland, Dorothy	N
ES968HA	Aldridge, Holly	N
ES968HG	Garland, Hal	N
ES968JF	Frydrych, Jeremy ***Left Dept***	N
ES968KP	Patel, Kanu	N
ES968KR	Richardson, Ken	N
ES968MH	Hollie, Melissa	Y
ES968MR	JEAN-REJOUIS, Mario	N
ES968MW	Waters, Marvin	N
ES968PD	Davis, Greg	N
ES968PH	Herring, Paul	N
ES968TW	Ware, Tyrone	N
ESATEST	ESA Testing	N
EV975AE	Edwards, Andy	N
FI522OM	Godwin, Michelle	N
FI522MD	Desmond, Martha	N
FI522MN	Nohr, Mike *Roles removed 06/11/04*	N
FI522VW	Wyche, Vickie	N

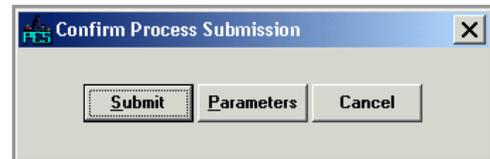
This will open the Run Processes window.

- Click **List Users**.
- Click **OK**.



This will display the Confirm Process Submission window.

- To submit the batch process, Click **Submit**.
- To change process submission parameters, click **Parameters**.
- To return to the User List window without submitting the batch process, click **Cancel**.

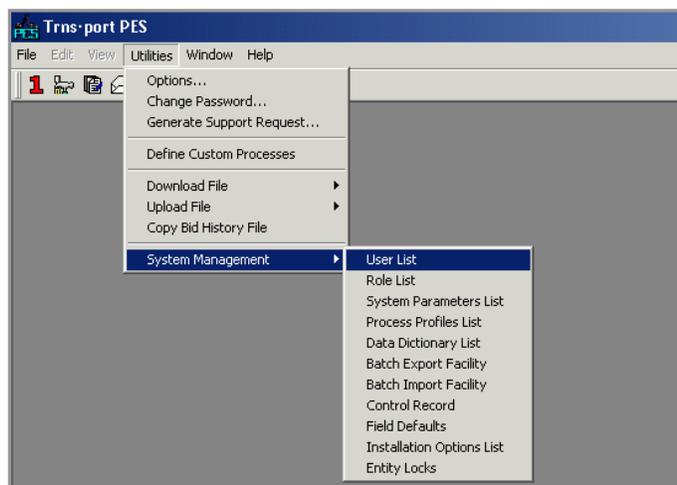


1.2.5 Users Changing Jobs or Leaving FDOT

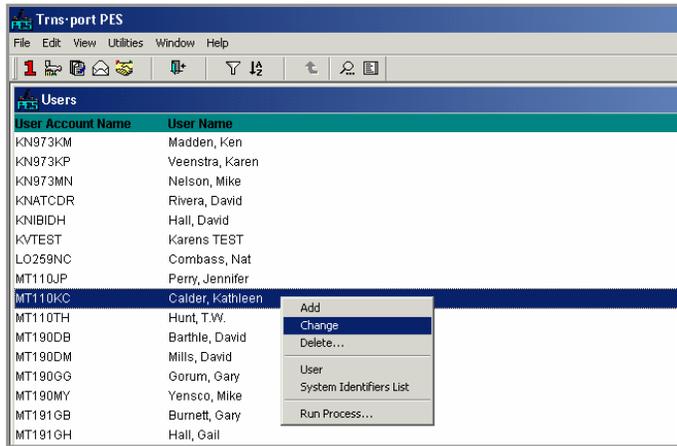
In this circumstance the purpose of the change is to leave the UserId intact but remove all authority.

In this example a person moves from one official position to another wherein a new UserId is to be assigned.

- Click **Utilities > System Management > User List** from the Menu Bar.

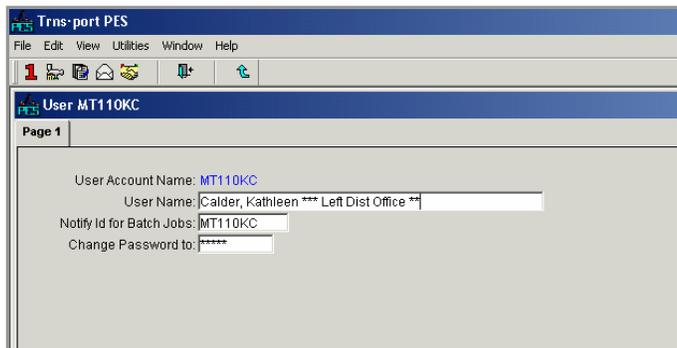


- Click the particular **User**.
- Rclick **Change** from the right mouse button menu.

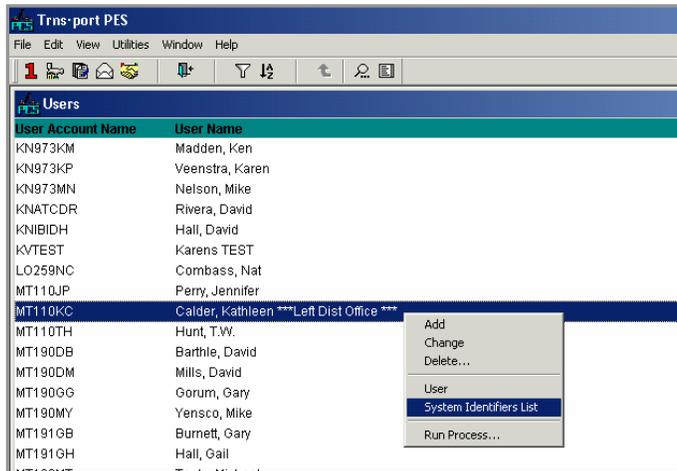


- Change the text in the *Use Name* field.
- Click **OK**.

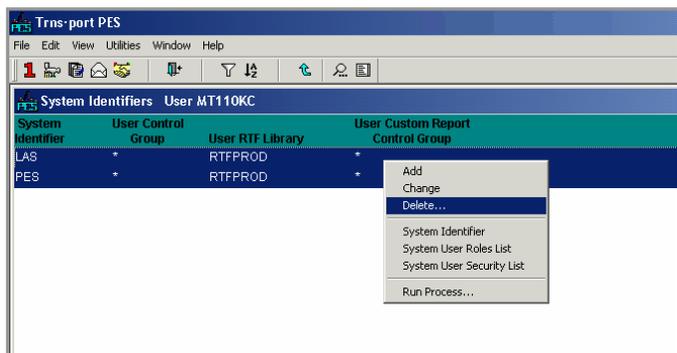
In this example the text change added the phrase *****Left Dist Office*****.



- Rclick **System Identifiers List** from the right mouse button menu.

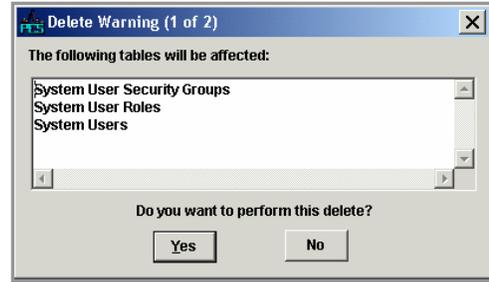


- Highlight all rows
- Click **Delete** from the right mouse button menu.



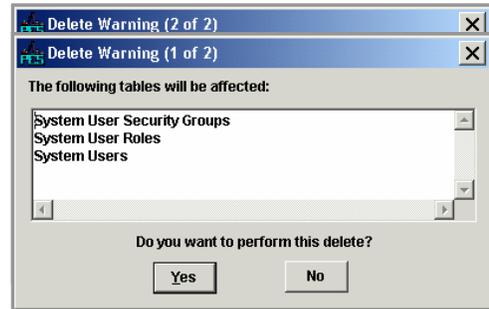
A Delete Warning window will open.

- Click **Yes**.



A second Delete Warning window will open.

- Click **Yes**.



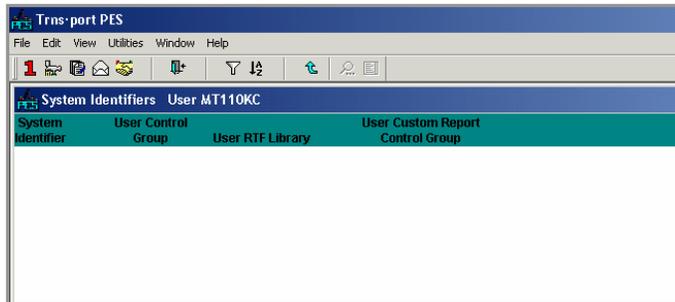
A Confirm Delete window will open.

- Click **Yes to All**.

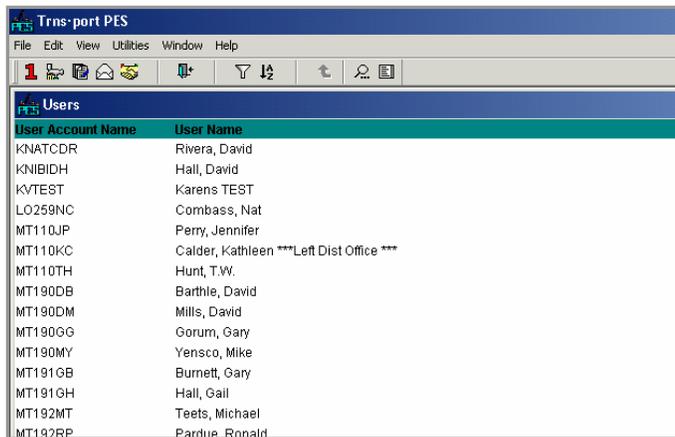


The rows will have been removed.

- Close the window.



All necessary changes have been completed.



2. SiteManager

2.1 Background

SiteManager has extensive methods to control access to all of the program functions as well as to make changes to the database based on contract authority, even if a user has the update authority under the function.

SiteManager approaches security from all of the following avenues.

- **User Login** - User must have a valid UserId to access the application. The security table is checked at each logon attempt to verify user is a valid user.
- **User Group** – User is assigned to a specific security group. This provides the user access to all functions with appropriate operation capability as defined for that group. At logon user must select a group under which the user will be working during that logon session. Group security can be defined at the highest window level, at a specific function level, at a specific tab within a function or in some cases even at a data element on the window tab within the function. Operation capability can be defined as *Inquiry, Update, or No Rights*.
- **Contract Authority** – Even if user has the Update access to a specific program function such as Contract Records, the user may be prevented from doing any updates to those contract records without specific authority to that contract.
- **Process Authority** – For some of the functions such as Payment Approval and Contract Change Order Approval even if all of the above provide update access and user is not specifically shown as the appropriate individual for this approval then the user will not have this authority.

2.2 Security Hierarchy

Since the Department has two distinct set of users, Maintenance and Construction, it is necessary that a security hierarchy function to ensure proper compliance with the security roles within SiteManager.

- Level 1 – SM Creator** – This is the highest level of security within SiteManager and is the one that is used to install initial application and database as well as updates to application and database. This level should reside within the OIS area.
- Level 2 – SM Administrator** – This is the highest user level and is responsible for establishing Operational Parameters, and Code Table Maintenance. This level is the responsibility of the user community. A limited number of individuals will have this authority.
- Level 3 – Central Office User Administrator** – This level will be assigned by Level 2 to be able to assign new users to SiteManager, create new groups as needed, and have access to all of the functions with update capability and Office Wide contract authority. This will allow these level 3 users to assign limited security to level 4 users.

Level 4 – District User Administrator – Level 3 users will assign this level and users in this level will be able to assign new users to existing **Security Groups**. User will have Office Wide Contract Authority only for their district.

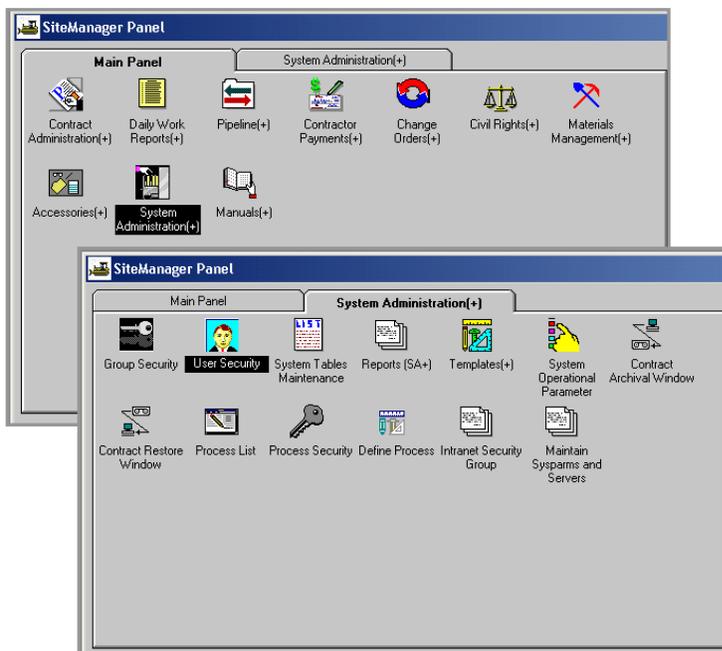
Level 5 – SiteManager Users – This level will be made up of all SiteManager users as defined by user id, security group, and contract authority.

2.3 Naming Conventions

Because of the differing needs of Maintenance and Construction users, it is necessary to have a consistent naming convention for all Security Groups. The following format has been adopted for this eight character field. The general code structure will be **XXYYAAAA** where;

1. **XX** - Will indicate whether Maintenance (MT) or Construction (CN)
2. **YY** - Will indicate whether Central Office (CO), District Office (DO), Resident Office (RO), Maintenance Yard (MY) or Field Office (FO). In the event a group is needed specifically for a District then the second character will be replaced with the District number (example D1, R1, F1 etc)
3. **AAAA** – Will indicate the functions such as Lead Inspector (LEAD), Inspector (INSP), Project Manager (PMAN), Project Engineer (PENG), Office Engineer (OENG), Final Estimates (FINL), etc in Construction. For Maintenance this will designate Application Managers and Security Coordinators (AMSC), Application Managers (AM), Security Coordinators (SC), and Maintenance Users (USER).

2.5 Adding and Maintaining Users



The SiteManager security process begins by adding an individual to the User List. At the Main Panel

- Click the **System Administrator** icon.
- Click the **User Security** icon.

2.5.1 Adding Users

User Data

The User Security detail window will open.

- Click the **New Sheet**  icon to create a black window.
- Enter **User Id** in lower case letters. This value is to match the assigned RACF UserId identically.
- Enter **User Name** in the form of **Last name, First Name (Middle Initial optional)**, using lower case letters, and standard capitalization.
- ❖ **User Id** is a required field, and is to contain the assigned Department RACF UserId. All Trns•port users must have a UserId to sign on to authorized systems. RACF UserIds are purged monthly and as a consequence UserIds can be and are reused. This leads to a problem in all Trns•port systems because UserIds are not deleted from any Trns•port system when a user leaves but all authority is removed. The UserIds remain tagged to historical transactions in the data bases. In instances where a new user is assigned a RACF UserId that duplicates a former Trns•port UserId, prior to continuing with the new user, the old Trns•port UserId is to be modified by appending the numeral 1 (or 2 or 3 if necessary) to the UserId. This is to be done by data base change so that all history is modified uniformly. Submit an email request to the Trns•port Coordinator to have this change made. After this change is made, the new user may be entered.
- ❖ Note In the SSN field, **do not enter** a real SSN. However, this must be a unique number that is entered in the same form as a Social Security Number to uniquely identify the individual. The following format can be used to help keep unique numbers within a District and Office.
Use the first 3 digits as the district number. Example: **001**
Use the 4th and 5th digits to record the last 2 digits of the office cost center number.
Example: **06**
Use the last 4 digits to record a unique sequential number. Example: **0003**
The completed number from this example would be **001-06-0003**
- **Active** –This is a check to indicate the user is currently a valid user under SiteManager.
- **Database Login ID** and **Database Password**, will remain **blank**. These fields are set by the Database Administration and remain invisible to all users.

For a person in the **Central Office**,

- Click the **Central** field.

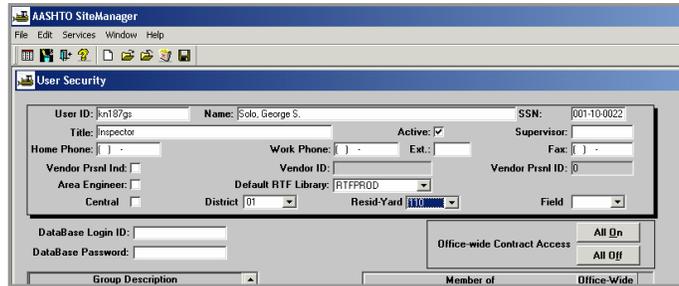
For a person in a **District Office**,

- Click the down arrow in the **District** field.

- Click the appropriate **District Number**.

For a person in a **Resident Engineer Office, or Maintenance Yard**

- Click the down arrow in the **District** field.
- Click the appropriate **District Number**
- Click the down arrow in the **Resid-Yard** field.
- Click the appropriate **Cost center**



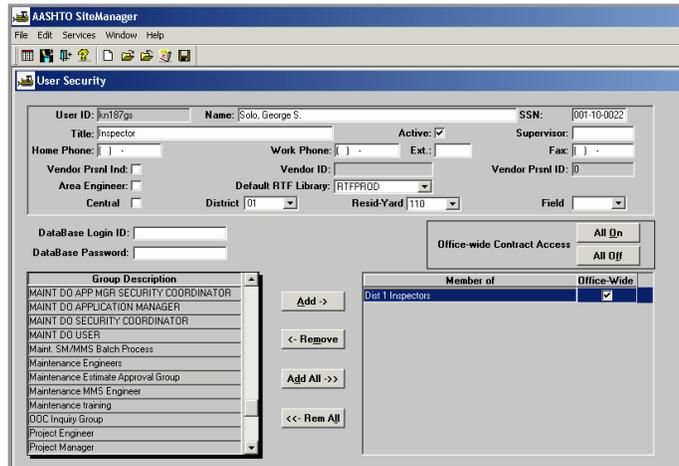
Field is reserved for future use.

Security Groups

Once the UserId has been entered the list of **Security Groups** in the lower left panel will activate.

Member of is a listing of the groups to which this user is authorized. The available groups will be shown on the left

- Click the label **Group Description** and the list will sort alphabetically.
- Click appropriate groups.
- Click **Add**.



The selected group(s) will be assigned into the lower right panel

In this example an inspector has been added.

The following fields will have to be determined for the specific user as they relate to the functions that the user will perform.

- ❖ **Office Wide Contract Authority** – This is to be checked if user is to have access to all contracts within the area as indicated by the office location for which the user is assigned. For example:
 - If a user is assigned to District 1 and they have Office Wide Contract Authority then they will be able to see and update contract information for contracts in District 1.
 - If they were assigned to Resid-Yard 110 then the user would be able to see and update only the contract assigned to Resid-Yard 110.

- ❖ **Area Engineer** – This is used to indicate whether this user can be assigned as an Engineer for one of the Office Location identified below. In the Contract Administration Reference Table for Administrative Offices, those individuals that are to be entered as Engineer for office location must be identified with this flag.

The following fields are optional and may be entered as desired.

- **Title** – This could be the working title for the user’s position.
- **Supervisor** – This is a 7-character field that could contain the UserId, Initials, or Name for this user’s current Supervisor.
- **Home Phone** – This would be the User’s current home phone number.
- **Work Phone** – This would be the User’s current work number including the Area Code. If it is a Suncom number do not include the Area Code.
- **Ext.** – This would be the user’s Extension to the Work Phone number entered.
- **Fax** – This would be the user’s current FAX number including Area Code. If a Suncom number, do not enter the Area Code

The following fields will not be used by FDOT at this time.

- **Vendor Prsnl Ind** – This would be checked if user were a Contractor or material supplier. Currently there are not plans to provide access to SiteManager to individuals not on the Department’s computer network. Checking this would make the other fields available.
- **Vendor Id** – This would be a unique identifier for vendor where user is employed. This is a searchable field of valid vendors within the Department’s Vendor Database.
- **Vendor Prsnl Id** – This would be a unique identifier for the user employed by the vendor already entered. This is a searchable field from the Department’s Vendor Database.

2.5.2 Deleting a User

- ❖ While all Trns•port modules have a Delete capability for users, deletions are not to be made. SiteManager maintains transaction history by UserId, and PES/LAS are expected to do so in future releases. The maintenance of transaction history by UserId is desired.

2.5.3 Changing User Information

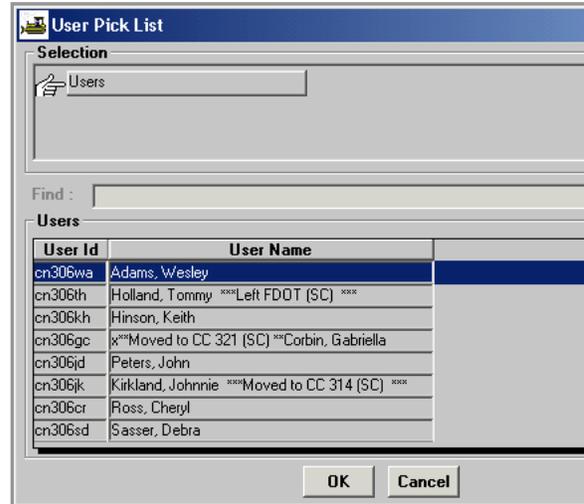
User Data

The User Security detail window will open.

- Click the **Open Folder**  icon.

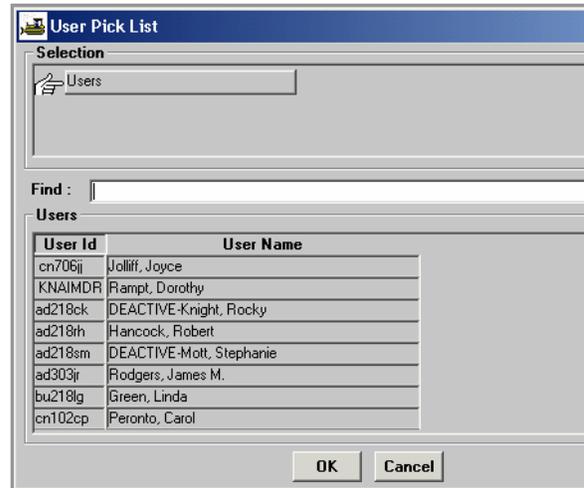
The User Pick List will open.

- Click the label **User Id** to sort the list alphabetically.



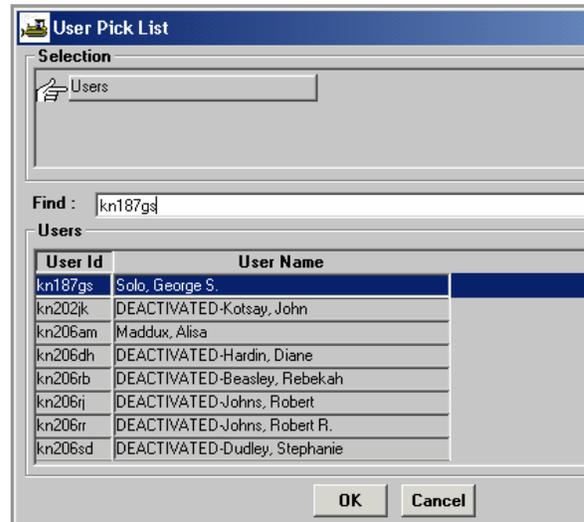
- Enter the UserId in the **Find** window.

In this example enter kn187gs

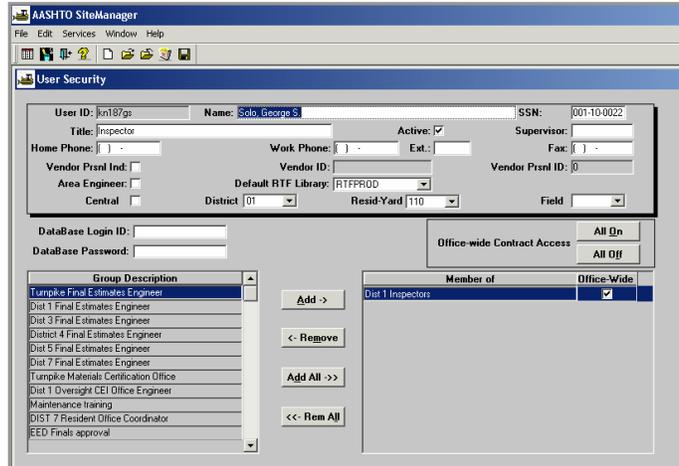


The record for George S. Solo kn187gs will be highlighted.

- Click **OK**.



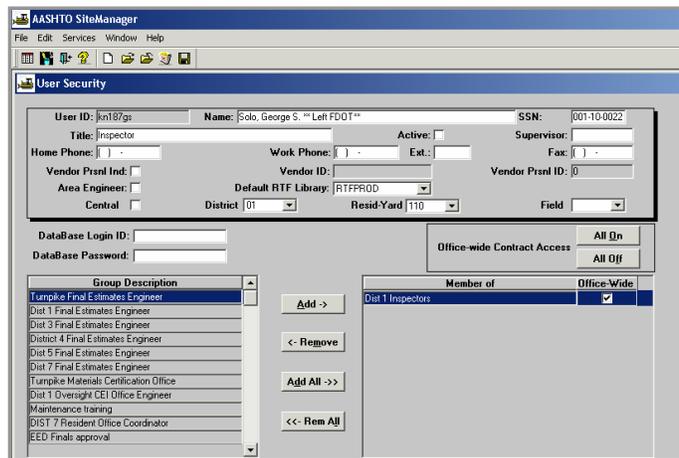
The detail record will open. Note that the UserId field is grayed out, but that all other fields are available for change.



In this example the User has left the Department.

In the User data panel

- At the end of the **Name** field add the phrase ****Left FDOT****
- Click the **Active** flag to the off mode

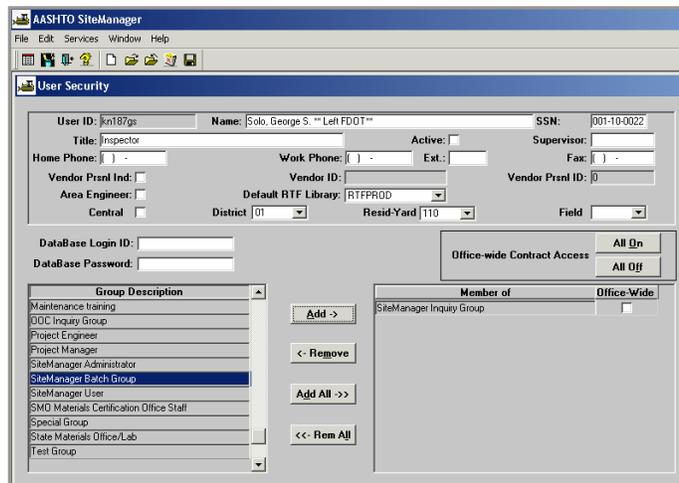


Security Groups

- Highlight all entries in the **Members of** panel.
- Click **Remove** to remove all Security Groups.
- In the **Group Description** panel, click the **label** to sort the list.
- Click **SiteManager Inquiry Group**.
- Click the **Add** button.

The SiteManager Inquiry Group will now appear in the **Member of** panel as seen here.

- Click **Save**.
- Close the window.



All necessary changes for this particular example are complete.

Appendix A. Control Group

The assignment of Access Control Groups is one of the principal tools available to the Department to control access to project data. Through the plan outlined here, a hierarchy can be established where data may be compartmentalized to restrict access to a set of people who need visibility of a particular project and to deny visibility to those who don't.

The use of Control Groups satisfies two concerns. The first is to reduce the volume of information that will appear on Project List screens, and second to secure information during the bidding and award process. The use of Control Groups allows the visibility projects to be moved from one person to another. An example would be a project in District 2 that might have a Control Group of CD02PMA. With this Control Group assigned to the project, the District Estimator(s), having a personal Access Control Group of CD02*, would always have visibility of the project. Similarly, any person having an Access Control Group that is less restrictive would also be able to see the project on his or her project list screen. For example, a user with an Access Control Group of C* would have access to every project in the Production organization statewide.

For the management of projects for Central Office letting, the sequence of Control Groups assigned to the Project, and the Proposal header when it is created, would be as follows:

- CD02PMA: When under the control of a District Project Manager.
- CD02: When control of the project shifts from the Project Manager to the District Estimator.
- CC02: When the District Estimator transfers the proposal to the Central Office for letting. A further refinement here will be decisions in the Central Office Estimates Office about compartmentalizing within itself. For example, a particular estimator may use CC02TW (initials) to assign the access to another estimator, or CC02A to have proposals shared by two or more Estimators as a group within the overall estimates office.
- CT02: When the proposal is ready for processing by the Central Contracts Administration Office. It is necessary that the proposal Control Group remain unchanged while the project is in LAS and the Contracts Administration Office in order to ensure that the Engineer's estimate is always under the control of only the estimator.

The following table illustrates how visibility of projects to a community (Maintenance or Production) for oversight is granted, and then to a smaller group of project or maintenance staff for the control and management of project detail.

	PES	LAS
District Contracts Manager	?L##*	?L##*
District Contracts Assistant A	?L##A*	?L##A*
District Contracts Assistant B	?L##B*	?L##B*
District Production Director	CD##PM*	None
District Production Project Manager A	CD##PMA*	None
District Production Project Manager B	CD##PMB*	None
District Project designed by Consultant Firm	CD##T###	None
District Estimator	CD##*	CD##*
Assistant District Estimator	CD##A*	CD##A*
District Maintenance Engineer	MD##*	None
Assistant District Maintenance Engineer A	MD##A*	None
District Maintenance Contract Estimator	MD##*	MD##*
Assistant District Maintenance Contract Estimator	MD##A*	MD##A*
District Work Program Manager	?D##*	None
Central Maintenance Manager	M*	None
Central Estimator	CC*	CC*
Central Office Production Manager	CC*	None
Central Office Contracts Manager	CT*	CT*

Control Group Structure:

Character position 1: M = Maintenance Project

 C = Construction Project

Other characters may be assigned if desired to segment project development to other specialty areas.

Character position 2: D = District Office processing
 C = Central Office processing
 T = Central Contracts Administration Office
 L = District Contracts Administration Office

Character positions 3 & 4: ## = District Number
 And where * and ? may be used as traditional wild cards.

Character position 5: The letters T, U, V, W, X, Y, and Z are reserved for Central Office and statewide use. When a consultant firm is the designer of a project, the last four characters of the control group will identify the consultant firm. The letters T, U, V, W, X, and Y identify consultant firms.

A project created in the Central Office could be assigned an office code.

Character positions 6/7/8: Organizational or subordinate breakout where desired. For consultant firms, these three characters, in conjunction with a letter in character position 5, identify the firm.

For those projects let through the DCP system today, Central Office staff would rarely require access to them for control or change purposes, but may have visibility of them depending on the Control Group structure finally developed.

The Control Group feature is a very important tool, but it has limitations:

- It is not a code table and, therefore, will require a thorough understanding of the structure by Application Managers and Security Coordinators.
- Control Group is not available to Letting Headers.
- When transferring a project or proposal to another user, take care to ensure that all letters in the new Control Group are capitalized, and that a valid Control Group has been used. If these precautions are not taken, a project or proposal will be removed from the project or proposal list screen of the previous user and will be available to no one. Under this circumstance, a user with high-level authority such as a Security Coordinator or Application Manager will have to find the errant project or proposal and assign a valid Control Group.

Control Group Life Cycle

A Control Group assigned to a project/proposal might evolve in the following manner:

Maintenance Contract

Receive Maintenance Project from FM	MD##
District reassigns project internally	MD##A (or other subset)
Create Proposal Header	MD##A
Pass to Contracts Office	ML##
Contracts Administration Office activity	ML## (or subset if desired)
Pass to "estimator" for Bid Analysis	MD## (or other person)
Return record to Contracts Office	ML##
Complete award and execute phases	ML##

Construction Project

Receive Production Project from FM	CD##
District reassigns project internally	CD##A (or other subset)
Or	
District reassigns to consultant firm	CD##T365 (or other subset)
Pass file to District Estimator	CD##
Create Proposal Header	CD##
Pass to District Contracts Office	CL##
Contracts Administration Office activity	CL## (or subset if desired)
Pass to Distr Estimator for Bid Analysis	CD##
Return record to Contracts Office	CL##
Complete award and execute phases	CL##

Or for Class 1 Contract

Pass file to District Estimator	CD##
Create Proposal Header & Price Job	CD##
Pass to Central Estimator	CC##
Pass to Central Contracts Admin. Office	CT## (or subset if desired)
Pass to Central Estimator for Bid Analysis	CC##
Return record to Contracts Office	CT##
Complete award and execute phases	CT##