

AES

Adaptive Enterprise Solutions

...unlocking the dawn of better results for your organization

AGENCY ADMINISTRATOR SECURITY MANAGER GUIDE



Adsystemtech Inc.

© 2010 Adsystem, Inc.
8401 Colesville Road Suite 450
Silver Spring, MD 20910
800.237.9785 Toll Free
301.589.3434 Voice
301.589.9254 Fax
www.adsystem.com

This document is not to be photocopied or used
without written permission of its copyright holder,
AdSystem Inc.

TABLE OF CONTENTS

OVERVIEW OF SECURITY MANAGER	1
GLOSSARY	1
THE BASIC PROCESS	1
SECURITY MANAGER STRUCTURE	2
ORGANIZATIONS MANAGED PAGE	3
NAVIGATING THE ORGANIZATIONS MANAGED PAGE	3
Select the Organization to manage	3
CREATE PROGRAM AREA (TAG)	4
NAVIGATING THE PROGRAM AREA (TAG) PAGE	4
Create New Program Areas (Tags)	5
Remove Program Area (Tags)	5
View existing Program Area (Tags)	5
CREATE PROGRAMS	6
NAVIGATING THE PROGRAMS PAGE	6
Create New Programs	7
Remove Program Area (Tags)	7
View existing Programs	7
CREATE USER GROUPS	8
NAVIGATING THE USER GROUP PAGE	8
Create New User Groups	9
Remove User Group	9
View existing User Groups	9
CREATE PERMISSIONS BETWEEN GROUPS	10
NAVIGATING THE PERMISSIONS PAGE	10
Assign Permission from Grantor to Grantee	11
Remove Permission from Grantee	11
View all Permissions assigned to a Group	11
CREATE USERS	12
NAVIGATING THE USER PAGE	12
Create new User	13
Reset User Password	13
Remove User (make invalid)	13
Unblock a User	13
Lock or Unlock a User from the System	13
View existing Users	14
ASSIGN PERMISSIONS TO USERS	15
NAVIGATING THE USER PERMISSION PAGE	15
Create a new User Permission	16
Remove User Permission	16
View all Permissions assigned to a User	16
ONLINE USERS PAGE	17
NAVIGATING THE ONLINE USERS PAGE	17
View User Information	17

CREATE TAB GROUPS FOR RESOURCE MANAGER	18
NAVIGATING THE TAB GROUPS PAGE	18
Create new Tab Group.....	19
Assign Users to Tab Group.....	19
Remove Users from Tab Group	19
Remove Tab Group	19
View all Members of Tab Group.....	19
CREATE REPORT PERMISSIONS	20
NAVIGATING THE REPORTS PAGE	20
Assign Report to User Group	21
Remove Report from Group	21
View all Reports assigned to a User Group.....	21
ASSIGN ADHOC REPORT VIEWS	22
NAVIGATING THE REPORTS PAGE	22
Assign Views to User Group.....	23
Remove View from Group	23
View all Reports assigned to a User Group.....	23
ASSIGN ADHOC REPORT QUERY.....	24
NAVIGATING THE ADHOC REPORT QUERY PAGE	24
View existing Queries	25
View all Reports assigned to a User Group.....	25
Add Queries to a Group	25
ASSIGN LISTING REPORT QUERY	26
NAVIGATING THE LISTING REPORT QUERY PAGE	26
View existing Queries	27
View all Queries assigned to a User Group.....	27
Add Queries to a Group	27
SUBSCRIBE REPORT.....	28
NAVIGATING THE SUBSCRIBE REPORT PAGE	28
Schedule Report Delivery to Groups or Users	29

Overview of Security Manager

Security Manager is a tool to be used by System and Local Administrators to create the security setup for the Organizations.

Local Administrators will create and manage Programs, User Groups, Users and their Permissions.

If the Program Development Web Tool is used to export a Program, the Program Area (Tag) and Program will be created there and appear in Security Manager automatically. The remaining security for that Program will be set up here.

Note that the Grid Titles tell which record is currently active and the total number of records in the grid.

Glossary

Domain is the physical instance of the software used for one collaborative; there may be a Production domain and a Training domain

Application is the designation given to the collection of pages in the system used for a specific type of program, i.e. HMIS, Head Start, CSBG, or Weatherization; only one Application can be used at a time

Application Roles (sometimes just called Roles) determine which pages in a specific Application a User can see and use; the name usually includes reference to both the application and the role, i.e. CSBGCM for Case Managers using CSBG or HMISPM for Program Managers using HMIS

Organization is an Agency set up to use the system

Org Code is a unique 3-digit code that identifies one Organization; all Program names, User Group names, User names begin with this code

Program is a program within the Organization; it will include one or more Program Components, Target Goals and Activities

Program Area is a grouping of Programs; each Program must be linked to a Program Area; a Program Area may have more than one Program linked to it; they are used primarily for reporting

User Group determines which Programs a User has access to; it will have permission to access one or more Programs

User is a Login ID created to log in to the system; it has permissions granted to it for various Groups and Roles

Active or **Valid** designates the item is currently being used in the system; since many items may not be deleted after they have been used, there is the option of making an item inactive

Grantor is the group granting rights to its data to a User Group

Grantee is the group receiving rights to the data of a Program or Group

The Basic Process

- 1 Select Organization to work with
- 2 Create Program Areas (or make sure they were exported correctly)
- 3 Create Programs (or make sure they were exported correctly)
- 4 Create User Groups
- 5 Assign Permission between Programs and User Groups
- 6 Create Users
- 7 Assign Permission to Users
- 8 Give Permission for Reports, Adhoc Views, Adhoc Queries and Listing Queries to User Groups
- 9 If using Resource Manager, create Tab Groups

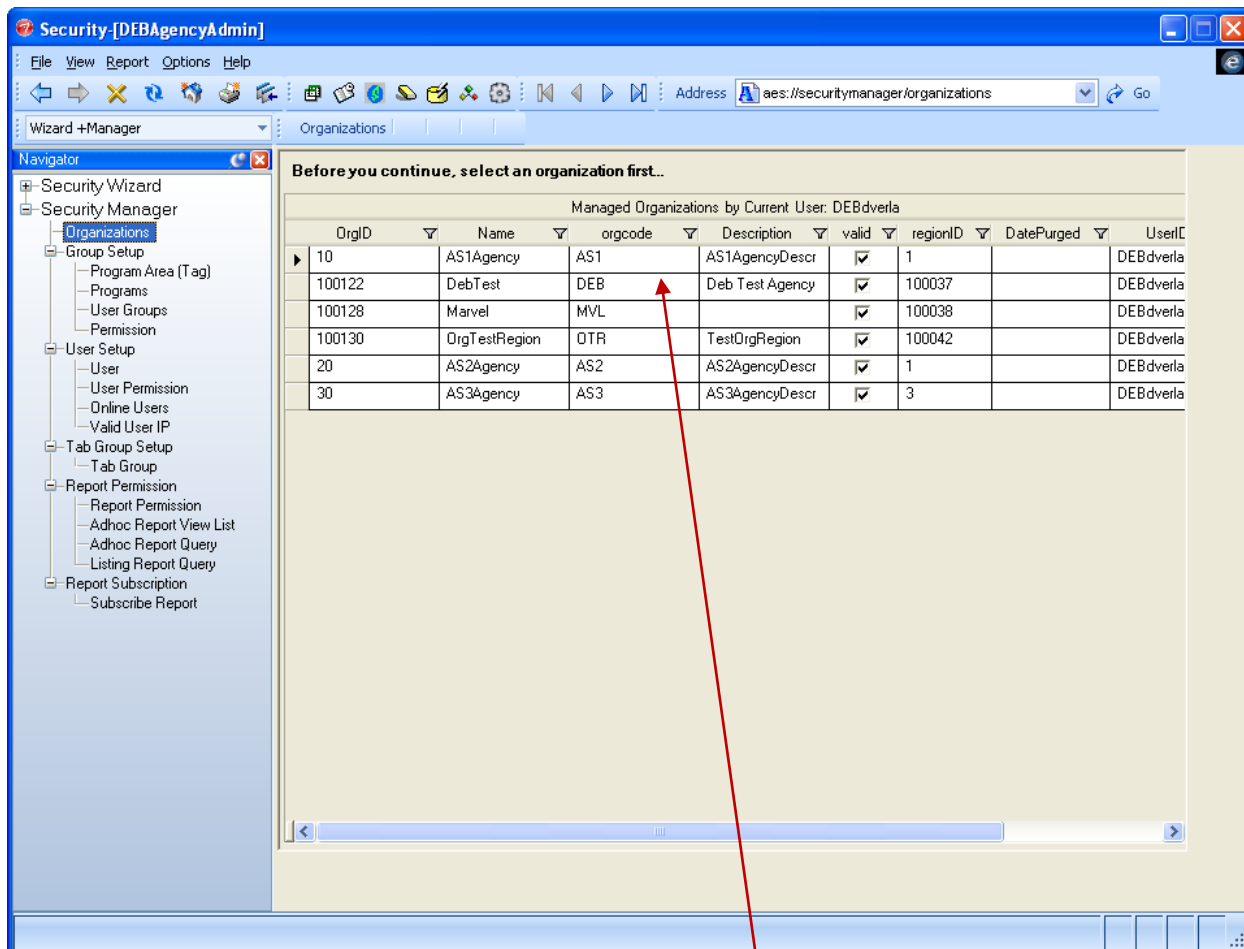
Security Manager Structure

There are several sections in Security Manager:

- 1 Group Setup section
 - a Program Areas (Tag) are used primarily to group Programs for reporting purposes
 - b Programs can be created here or exported from the Web Tool
 - c User Groups will be created here
 - d Program Areas, Programs, and User Group cannot be deleted, but may be made inactive
 - e Permission between the Program and one or more User Groups is granted on the Permission page
- 2 User Setup section
 - a Users can be created here or in the Security Wizard, Users are assigned a Role of User, Local Admin or System Admin; available Roles depend on the current User's permissions
 - b Users cannot be deleted, but may be made inactive
 - c Permissions to Groups and Roles are granted on the User Permission page
- 3 Tab Group Setup section
 - a Tab Groups are created for use in the Resource Manager
 - b Each Tab Group can have one or more Users assigned to it
 - c Tab Groups can be designated as Routes
- 4 Report Permissions section
 - a Report permissions are granted to User Groups for Application, General and Adhoc reports; reports must be assigned to an Application in Security Wizard to show up in Security Manager
 - b Views and Tables are made available for Adhoc Report types and Groups, these must also be made available in Security Wizard first
 - c Permissions are assigned to queries created in Adhoc Reports and on Listing pages; these can be made available to more than one Organization

Organizations Managed Page

Organizations are created in Security Wizard; security for the Organization is set up in Security Manager. An Organization must be selected here to work with on other Security Manager pages. Only those Organizations a User has permission to will be displayed here.



Navigating the Organizations Managed Page

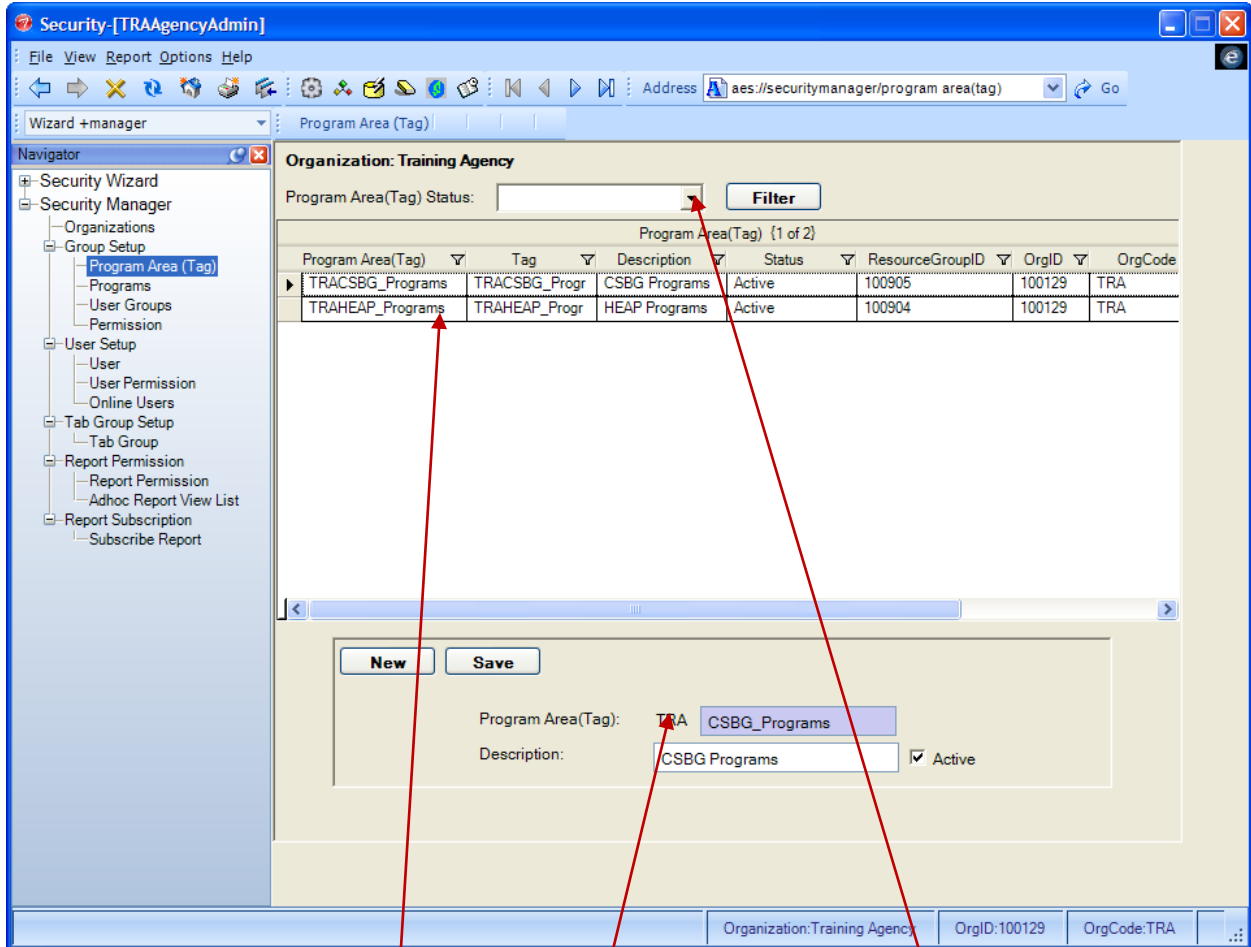
- All available Organization will appear in the MANAGED ORGANIZATION BY CURRENT USER GRID
- Select an Organization to work with on other Security Manager pages here

Select the Organization to manage

- 1 Click on Organization in MANAGED ORGANIZATION BY CURRENT USER GRID
 - a That Organization's information will be available now on all pages in Security Manager
 - b If no Organizations appear, check Security Wizard to make sure Organization setup is complete and that you have permission to manage the Organization
- 2 The Status Bar on other pages in Security Manager will reflect the active Organization and will show the name, ID and Org Code

Create Program Area (Tag)

Use this page to create new Program Areas. Each Program must be linked to one Program Area. If the Program Development Web Tool was used to export a Program, the Program Area will automatically be available on this page. Program Area names will automatically start with the Organization 3-digit Org Code; they cannot be changed once they are created!



Navigating the Program Area (Tag) Page

- All available Program Area (Tags) will be listed in the PROGRAM AREA (TAG) GRID
- Filter the list to see just Active or Deactivated Program Areas with the Program Area (Tag) Status dropdown
- Create new Program Areas in the bottom section

Create New Program Areas (Tags)

- 1 Click NEW button at bottom of page
- 2 Enter name for Program Area (Tag) (3-digit Org Code appears automatically)
- 3 Enter Description
- 4 Click to create checkmark in Active box
- 5 Click SAVE button
 - a Program Area will appear in PROGRAM AREA (TAG) GRID

Remove Program Area (Tags)

- 1 Program Areas cannot be removed or changed once they are created
- 2 They CAN be deactivated by un-checking the Active box

View existing Program Area (Tags)

- 1 All Program Areas will appear in the PROGRAM AREA (TAG) GRID
- 2 To view a filtered list of Program Areas:
 - a To view only Active Program Areas, select **Active** in the Program Area (Tag) Status dropdown
 - b To view only Deactivated Program Areas, select **Deactivated** in the Program Area (Tag) Status dropdown
 - c To view ALL Program Areas again, select % in the Program Area (Tag) Status dropdown
 - d If no filter is chosen, the default list is ALL Program Areas
- 3 All matching Program Areas will appear in PROGRAM AREA (TAG) GRID

Create Programs

Use this page to create new Programs. Each Program must be linked to one Program Area and one Application Type. If the Program Development Web Tool was used to export a Program, the Program will be displayed on this page. Program names will automatically start with the Organization 3-digit Org Code. Once a Program is created here, it will appear on the Program Setup page in the Organization library, as long as the User has correct permissions to use it.

The screenshot shows the Security Manager interface for the Training Agency organization. The main area displays a table of programs with columns for Program, Description, ResourceGroupID, Program Area(Tag), ApplicationType, Status, and O. The table contains 7 rows of data. Below the table is a form for creating a new program, with fields for Program, Description, Program Area(Tag), and ApplicationType. The form is currently filled with the following information:

Program	Description	ResourceGroupID	Program Area(Tag)	ApplicationType	Status	O
TRACentral Intak	Central Intake for	100918	TRACSBG_Programs	CSBG	Active	10
TRAHousing	Housing Counseli	100911	TRACSBG_Programs	CSBG	Active	10
TRAFamily Self S	Family Self Suffici	100910	TRACSBG_Programs	CSBG	Active	10
TRAWeather Rel	Weather Related_	100909	TRAHEAP_Programs	HEAP	Active	10
TRAHome Energ	Home Energy Pro	100908	TRAHEAP_Programs	HEAP	Active	10
TRAWinter Crisis	Winter Crisis Ener	100907	TRAHEAP_Programs	HEAP	Active	10
TRASummer Crisi	Summer Crisis En	100906	TRAHEAP_Programs	HEAP	Active	10

The form below the table is filled with the following information:

Program: TRA Family Self Sufficiency
Description: Family Self Sufficiency Program
Program Area(Tag): TRACSBG_Programs
ApplicationType: CSBG [Active]

Navigating the Programs Page

- All available Programs will be listed in the PROGRAM GRID
- Filter the list to see just Active or Deactivated Programs with the Program Status dropdown
- Create new Programs in the bottom section

Create New Programs

- 1 Click NEW button at bottom of page
- 2 Enter name for Program (3-digit Org Code appears automatically)
- 3 Enter Description
- 4 Select Program Area (Tag)
 - a All Program Areas created on the previous page will be available in the dropdown
- 5 Select Application Type
 - a All Applications with Roles assigned to this Organization in Security Wizard will appear here
- 6 Click to create checkmark in Active box
- 7 Click SAVE button
 - a Program will appear in PROGRAM GRID

Remove Program Area (Tags)

- 1 Programs cannot be removed once they are created
- 2 They CAN be deactivated by un-checking the Active box

View existing Programs

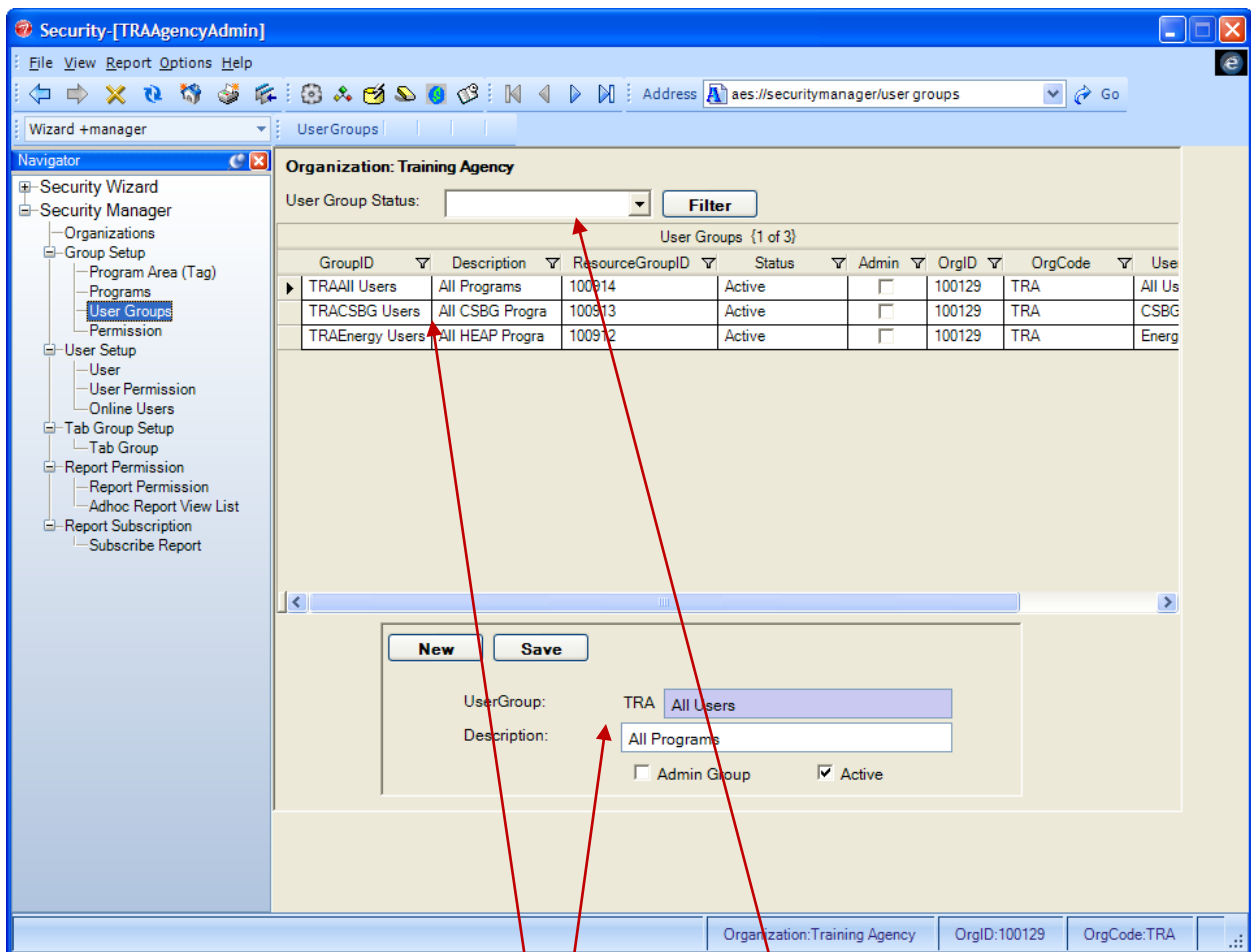
- 1 All Program will appear in the PROGRAM GRID
- 2 To view a filtered list of Programs:
 - a To view only Active Programs, select **Active** in the Program Status dropdown
 - b To view only Deactivated Programs, select **Deactivated** in the Program Status dropdown
 - c To view ALL Programs again, select % in the Program Status dropdown
 - d If no filter is chosen, the default list is ALL Programs
- 3 All matching Programs will appear in PROGRAM S GRID

Create User Groups

Use this page to create User Groups. USER GROUPS determine what DATA a User sees, while the ROLE determines which PAGES a user sees. Note that no Program is selected on this page – Permissions for the User Groups will be set on the Permission page. All User Group names automatically start with the 3-digit Org Code.

Create a User Group for each Program and/or for each Group of Programs and Reports that any User will need to access. For example, an organization has three Programs – A, B and C; they have users who access only their own program, and other users who access all three programs. They would need four User Groups: User Group A, User Group B, User Group C and User Group ABC.

An Agency Admin group is created automatically by Security Wizard; it is the Admin group for the Organization and has access to all data for that Organization. It will not appear on this page to avoid changing or deleting it by mistake.



Navigating the User Group Page

- All available User Groups will be listed in the USER GROUP GRID
- Filter the list to see just Active or Deactivated User Groups with the User Group Status dropdown
- Create new User Groups in the bottom section

Create New User Groups

- 1 Click NEW button at bottom of page
- 2 Enter name for User Group (3-digit Org Code appears automatically)
 - a It can be helpful to use the word user in the User Group name so it is not confused with a Program
- 3 Enter Description
- 4 Click to add checkmark in Admin Group checkbox if this User Group is an Admin Group
 - a If a Group is marked as an Admin Group and has rights to another Group (*see Group Permissions page*), they will be able to see data marked with a *Private* consent by a User in that Group
- 5 Click to create checkmark in Active box
- 6 Click SAVE button
 - a User Group will appear in USER GROUP GRID

► It can be helpful to use the word *User* in the User Group name so it is not confused with a Program name

Remove User Group

- 1 User Groups cannot be removed once they are created
- 2 They CAN be deactivated by un-checking the Active box

View existing User Groups

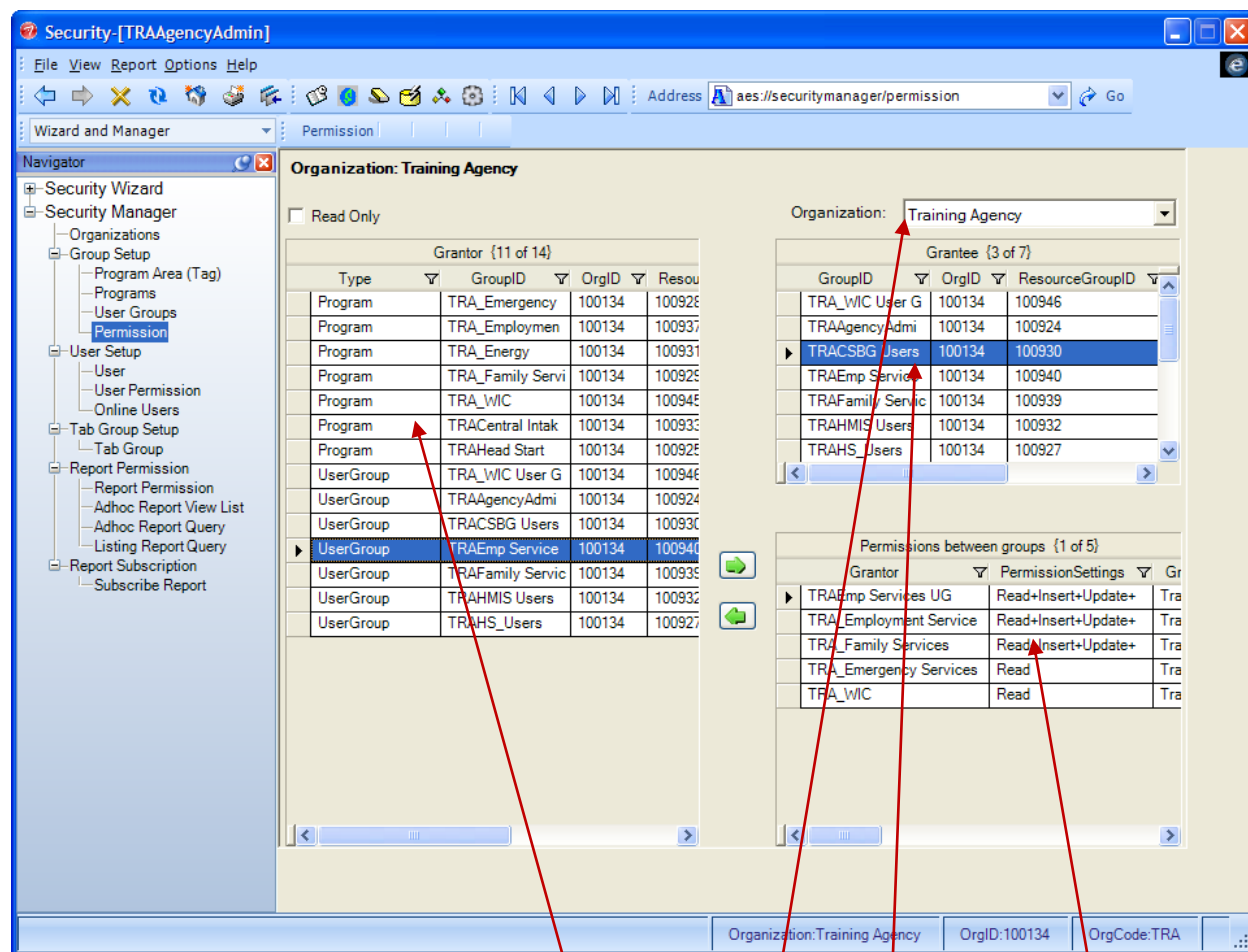
- 1 All User Groups will appear in the USER GROUP GRID
- 2 To view a filtered list of User Groups:
 - a To view only Active User Groups, select **Active** in the User Group Status dropdown
 - b To view only Deactivated User Groups, select **Deactivated** in the User Group Status dropdown
 - c To view ALL User Groups again, select % in the User Group Status dropdown
 - d If no filter is chosen, the default list is ALL User Groups
- 3 All matching User Groups will appear in USER GROUPS GRID

Create Permissions between Groups

Use this page to assign permission from Programs and user Groups to a User Group. The Group selected as the GRANTOR grants permission TO the group selected as the GRANTEE, so the Grantee will have access to the Grantor's data.

Rights should be assigned from each Program to each User Group who will need access to it; these rights can be assigned as Read Only when needed. If using Group Consent Levels, permission needs to be assigned from User Group to User Group as needed.


An Agency Admin User Group is created automatically, although it does not appear on the User Group page. It will appear here and will have rights automatically assigned to it from all Programs and User Groups.



Navigating the Permissions Page

- All User Groups and Programs will be listed in the GRANTOR GRID
- All Organizations that User has access to will be listed in Organization dropdown
- All User Groups in the selected Organization will be listed in the GRANTEE GRID
- All Permissions linked to the selected *Grantee* will be listed in the PERMISSIONS BETWEEN GROUPS GRID

Assign Permission from Grantor to Grantee

- 1 Select Organization in Organization dropdown on right side of page
 - a This is the Organization that will be receiving access to the data; it may be the same Organization showing in the GRANTOR GRID or it may be a different one
- 2 If the Grantor will be a Program, and the User Group receiving access should be able to view the data but not edit it, click to create a checkmark in the Read Only checkbox
- 3 Select Grantor in the GRANTOR GRID - this is the Group GRANTING the rights TO another group
- 4 Select the Grantee in the GRANTEE GRID - this is the Group RECEIVING the rights FROM the other group
- 5 Click the right arrow button 
 - a The Permissions will appear in the PERMISSIONS BETWEEN GROUPS GRID
 - b Use the left arrow button to remove a Permission

➤ Permissions are granted from left to right: FROM the Grantor TO the Grantee so the Grantee will have access to the Grantor's data


➤ All Programs and User Groups will be displayed in the GRANTOR GRID

➤ Select the Organization in the dropdown to see all User Groups in the GRANTEE GRID

In the simplest scenario, each Program should be selected as a Grantor and all User Groups who need access to that Program should be selected as the Grantee(s).

Note that Permissions to all Programs and User Groups have been assigned automatically to the Agency Admin User Group.

Remove Permission from Grantee

- 1 Select Grantee in GRANTEE GRID in upper right section
 - a Linked Permissions will appear in the PERMISSIONS BETWEEN GROUPS GRID
- 2 Select the Permission to remove 
- 3 Click the left arrow button
- 4 Permission will disappear from the PERMISSIONS BETWEEN GROUPS GRID

View all Permissions assigned to a Group

- 1 Select Grantee in GRANTEE GRID in upper right section
 - a The choice of a Grantor in the GRANTOR GRID will not affect the Permissions that appear
- 2 All linked Permissions will appear in PERMISSIONS BETWEEN GROUPS GRID on lower right side of page
 - a Any permissions that were assigned with Read Only permission will show READ in the Permissions Setting column

Example

Organization has Program A and Program B

User Group 1 should have all access to A and to B

User Group 2 should have all access to B, but should only be able to view A

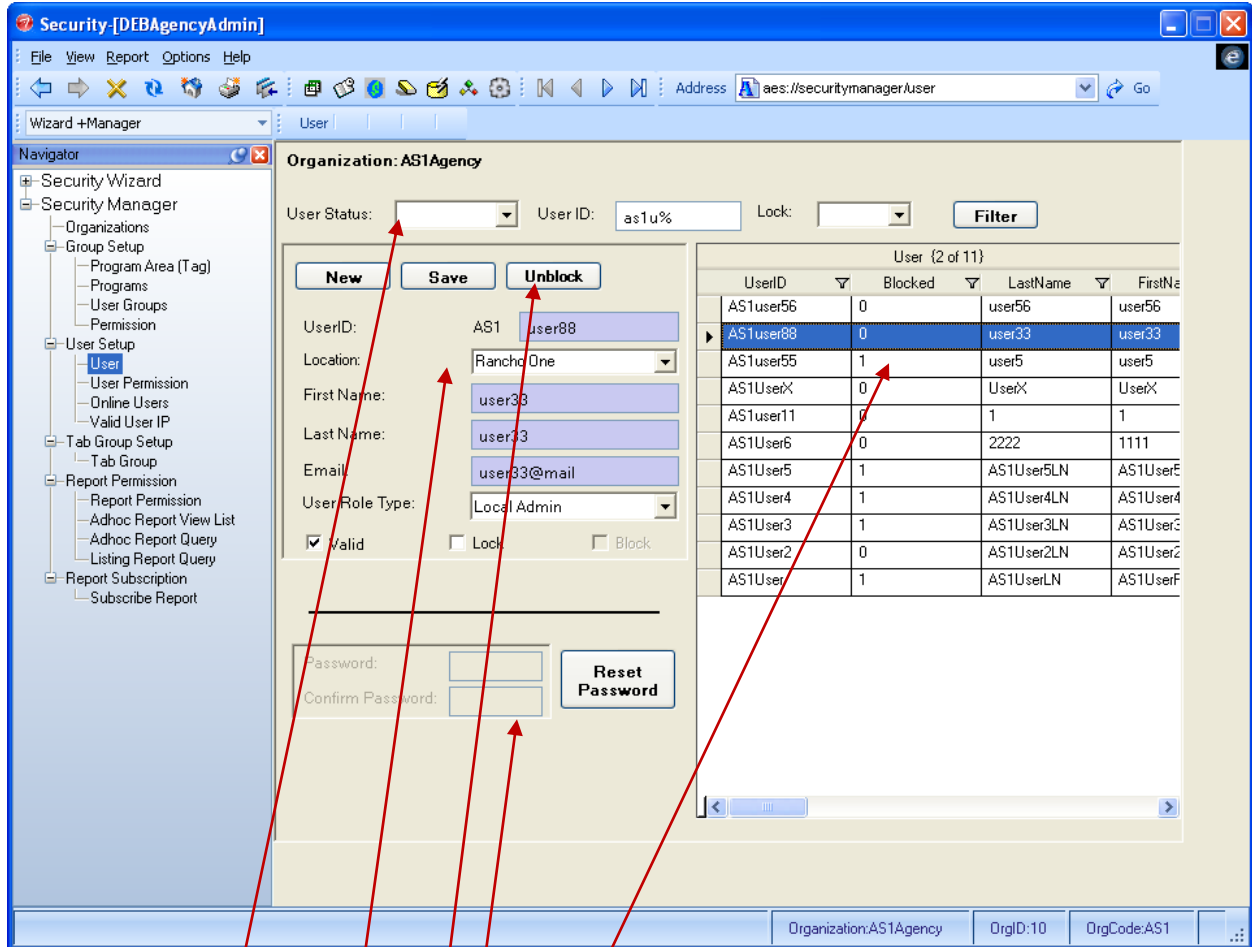
- 1 Select Group 1 in GRANTEE GRID
- 2 Select Program A, Program B and User Group 2 in GRANTOR GRID
- 3 Click right arrow button
- 4 Select Group 2 in GRANTEE GRID
- 5 Select Program B and User Group 1 in GRANTOR GRID
- 6 Click right arrow button
- 7 Click to create checkmark in Read Only checkbox
- 8 Select Program A in GRANTOR GRID
- 9 Click right arrow button

Create Users

Use this page to create Users within the Organization; Users created in Security Wizard will automatically appear here. All User IDs will automatically begin with the 3-digit Org Code.

Passwords can be changed here; they cannot be looked up, but can be reset.

Users have a set number of tries to log into the system, if they fail the system blocks them out from that IP Address; they can be unblocked on this page. Users cannot be deleted, but may be made Invalid or their access may be locked temporarily.



Navigating the User Page

- Filter the list of Users by Status, User ID or Lock Status
- Create new Users in the left section
- Unblock a User's access with the Unblock button
- Reset a User Password in the bottom section
- All available Users appear in the USER GRID

Create new User

- 1 Click NEW button
- 2 Enter User ID (3-digit Org Code appears automatically)
- 3 Select a default Location
- 4 Enter First Name
- 5 Enter Last Name
- 6 Enter User Email address
- 7 Select User Role Type
 - a User or Local Admin
- 8 Click to create checkmark in Valid box
- 9 Make sure Lock checkbox does NOT have checkmark
- 10 Click SAVE
 - a User will appear in USER GRID

A message will appear recommending that you reset the password for the new User.

- 11 Click OK in the message popup
- 12 Select User in User Grid
- 13 Click RESET PASSWORD button
- 14 Enter Password
- 15 Confirm Password
- 16 Click SAVE PASSWORD button

➤ Users are created here, but before the User can log in to the system, Permissions must be granted to the User on the User Permission page

➤ Local Admins created here will not have permission to Security Manager until an organization is added to them on the Security Wizard User Admin page

➤ Local Admins created here will not have roles automatically assigned; they will have those roles when created in Security Wizard; other roles may be assigned on the User Permission page



Reset User Password

- 1 Select User in USER GRID
- 2 Enter Password
- 3 Confirm Password
- 4 Click RESET PASSWORD button

➤ An Admin cannot look up a User's password but may reset it here

Remove User (make invalid)

- 1 Users cannot be deleted but may be made inactive
- 2 Select User in USER GRID in upper right section
- 3 Click in Valid checkbox to remove checkmark
 - a User record still exists, but is no longer active and valid

Unblock a User

Users are blocked from the current IP Address after entering their password incorrectly three times. Users who are currently blocked will have 1 displayed in the Blocked column

- 1 Select User in USER GRID
- 2 Click UNBLOCK button at top of page
 - a This will unblock the User's access so they will be able to log in again

Lock or Unlock a User from the System

- 1 Select User in USER GRID
- 2 Click to create checkmark in Lock checkbox
 - a User will not be able to log in to system until their account is unlocked
- 3 Click to remove checkmark in Lock checkbox
 - a User will now be able to log in to system

View existing Users

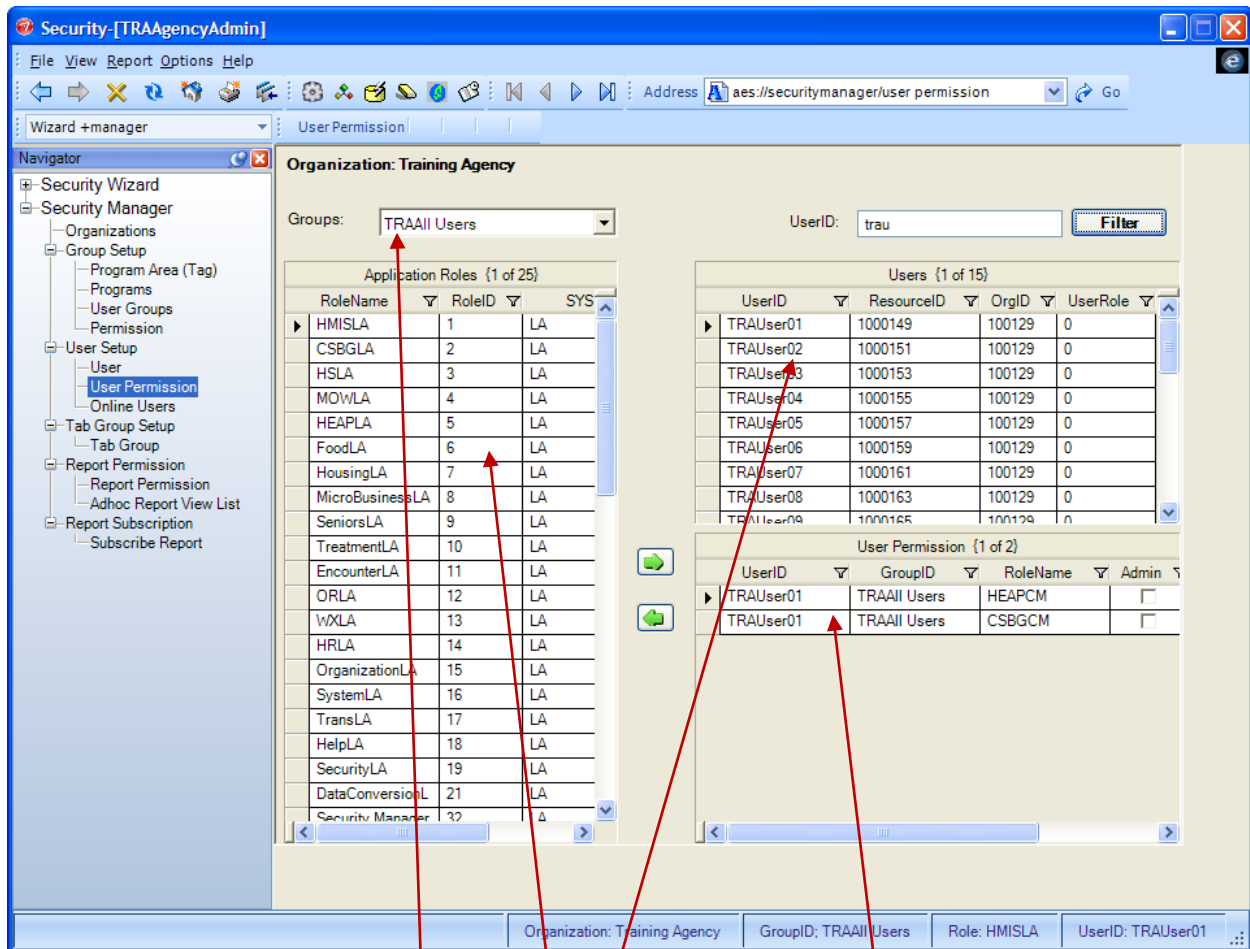
- 1 All Users will appear in the USER GRID
- 2 To view a filtered list of Users:
 - a To view only Active Users, select **Active** in the User Status dropdown
 - b To view only Deactivated Users, select **Deactivated** in the User Status dropdown
 - c To view ALL Users again, select % in the User Status dropdown
 - d If no filter is chosen, the default list is ALL Users
- 3 All matching User Groups will appear in USER GRID

Assign Permissions to Users

Use this page to assign Permission for Users to specific User Groups and Roles. Remember, Groups give the users access to see data in the system; Roles give the Users access to see pages in the system.

A User may have Permission to more than one Group and more than one Role; a User will not be able to log into the system until they are assigned a Group and Role.


Users with Local Administrator as their User Role Type will have all Roles with SYS = LA automatically assigned whether they were created in Security Wizard or Security Manager.



Navigating the User Permission Page

- All User Groups will appear in the Group dropdown
- All available Application roles will appear in the APPLICATION ROLES GRID
- All Available Users will be listed in the USERS GRID
- All Permissions assigned to the selected User will appear in the USER PERMISSION GRID

Create a new User Permission

- 1 Select the User Group in the Groups dropdown
- 2 Select a role in the APPLICATION ROLES GRID on the left side
 - a To select more than one Role in the grid, click and drag down to select all rows
 - b Or click on the first Role, press CTRL and click on each additional record to add
- 3 Select the User in the USER GRID on top right
 - a To select more than one User in the grid, click and drag down to select all rows
 - b Or click on the first User, press CTRL and click on each additional record to add
- 4 Click the right arrow button 
 - a User Permission will appear in the USER PERMISSION GRID on the lower right side


➤ *User Groups are created on the User Groups page in Security Manager*

➤ *Application Roles are created and assigned to an Organization in Security Wizard; Roles will not appear here unless they have been assigned to the Organization*

➤ *Users are created on the User page in Security Manager or Security Wizard*

➤ *Users will not be able to log into the system until they have Permissions granted to one or more Groups and Roles on this page*

Remove User Permission

- 1 Select the User in the USER GRID
- 2 Select the Permission to remove in the USER PERMISSION GRID in the bottom right section of the screen
- 3 Click the left arrow button 
 - a User Permission will disappear from USER PERMISSION GRID

View all Permissions assigned to a User

- 1 Select User in USER GRID
- 2 All assigned Permissions will appear in the USER PERMISSION GRID

Online Users Page

Use this page to view online activities of Users, including last logon time, IP address of that computer and their lock status.

Organization: AAAAgency

Online Users (1 of 2)							
UserID	LogonTime	IP	LastName	FirstName	OrgID	OrgName	ResourceID
AAAUser	06/25/2008	12.173.57.57	Last	First	100077	AAAAgency	100274
AAAUser2	06/25/2008	12.173.57.57	Last2	First2	100077	AAAAgency	100274

User ID: AAAUser
Resource ID: 100274
LastName: Last
FirstName: First
Organization Name: AAAAgency
Logon Time: 6/25/2008 2:38:08 PM
LogOn IP: 12.173.57.57
Status: unlocked

Organization: AAAAgency OrgID: 100077 OrgCode: AAA

Navigating the Online Users Page

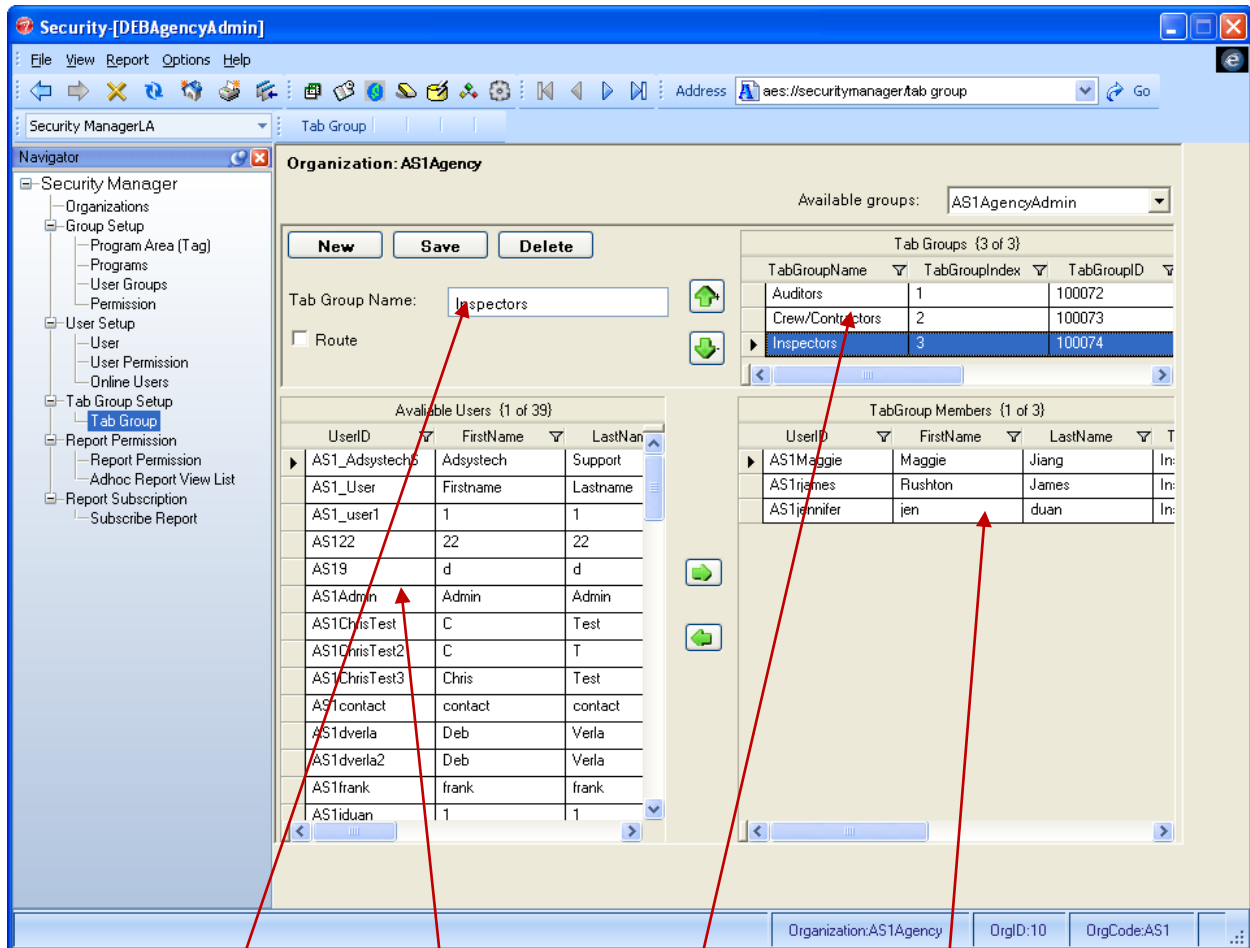
- All Users who are currently logged in will appear in the ONLINE USERS GRID
- Information about the selected User will appear in the bottom section

View User Information

- 1 Select User in ONLINE USERS GRID
- 2 Information about that User will appear in bottom section of page

Create Tab Groups for Resource Manager

Use this page to manage the Users and Groups that will be using Resource Manager. Create Tab Groups and add Users to the Tab Group as members, anyone needing to have appointments scheduled needs to be a member of a Tab Group (see Resource Manager Guide for more information about Tab Groups). Tab Groups need to be created only if the Organization is using Resource Manager.



Navigating the Tab Groups Page

- Create new Tab Groups in the top left section of the page
- All existing Tab Groups will appear in the TAB GROUPS GRID
- All Available Users will be listed in the AVAILABLE USERS GRID
- All Users who are members of the selected Tab Group will appear in the TAB GROUP MEMBERS GRID

Create new Tab Group

- 1 Select User Group in Available Groups dropdown
 - a This determines which Users will be displayed in the AVAILABLE USERS GRID
- 2 Click NEW button
- 3 Enter Tab Group Name
- 4 If this Tab Group is a Route, click to create checkmark in Route checkbox
- 5 Click SAVE button

Assign Users to Tab Group

- 1 Select User Group in Available Groups dropdown
 - a This determines which Users will be displayed in the AVAILABLE USERS GRID
- 2 Select Tab Group in TAB GROUPS GRID
- 3 Select User(s) in AVAILABLE USERS GRID on lower left section of page
- 4 Click right arrow button
 - a Users will appear in TAB GROUP MEMBERS GRID on right side of page

Remove Users from Tab Group

- 1 Select User Group in Available Groups dropdown
- 2 Select Tab Group in TAB GROUPS GRID
- 3 Select User(s) in TAB GROUP MEMBERS GRID on lower right section of page
- 4 Click left arrow button
 - a Users will disappear in TAB GROUP MEMBERS GRID on right side of page

Remove Tab Group

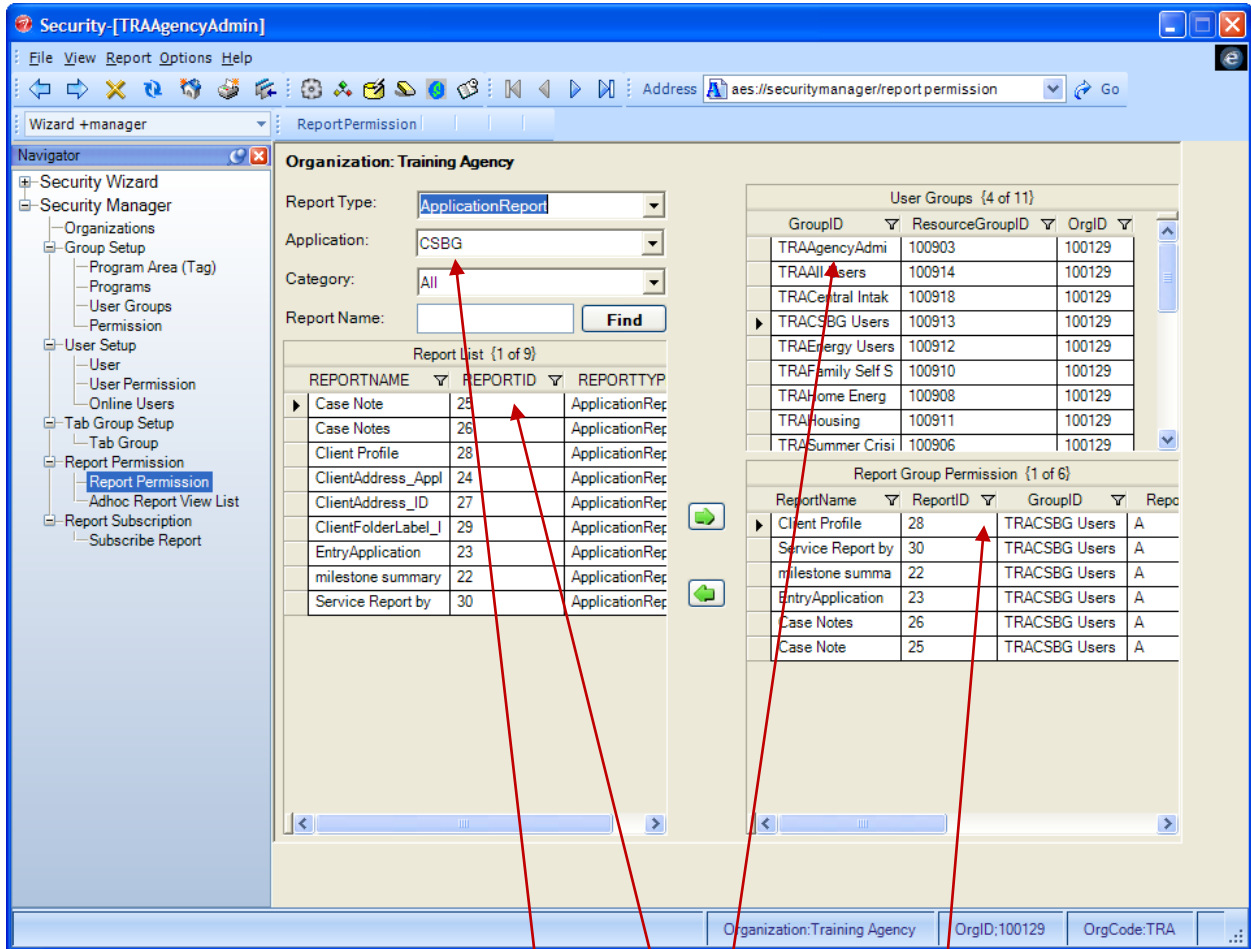
- 1 Select User Group in Available Groups dropdown
- 2 Select Tab Group in TAB GROUPS GRID
- 3 Click DELETE button
 - a Tab Group will disappear in TAB GROUP GRID on upper right side of page

View all Members of Tab Group

- 1 Select User Group in Available Groups dropdown
- 2 Select Tab Group in TAB GROUPS GRID
- 3 Users will appear in TAB GROUP MEMBERS GRID on lower right section of page

Create Report Permissions

Use this page to give permission for Reports to the User Groups. Reports that were assigned to Applications in Security Wizard will appear here.




Navigating the Reports Page

- Report Types will be listed in the Report Type dropdowns
- All available Reports of the selected type will appear in the REPORT LIST GRID
- All Available Applications will be listed in the APPLICATIONS GRID
- All Reports available in the selected Application will appear in the REPORTS AND APPLICATION ROLE GRID

Assign Report to User Group

- 1 Select Report type in Report Type Dropdown at the top of page
 - a Ad Hoc, Application and General are the three Report types
- 2 Select Application in Application dropdown
- 3 Select Category in Category dropdown
- 4 If searching for specific Report, enter name in Report Name Field
- 5 Click FIND button


Available Reports will appear in REPORTS LIST GRID.

- 6 Select Report(s) in REPORTS LIST GRID on left side of page
 - a To select more than one Report in the grid, click and drag down to select multiple rows
 - b Or click on the first Report, press CTRL and click on each additional Report to add
 - c If no Reports appear, there are no available Reports of the selected type for the selected Application
- 7 Select User Group in USER GROUP GRID on right side of page
 - a To select more than one User Group in the grid, click and drag down to select multiple rows
 - b Or click on the first User Group, press CTRL and click on each additional record to add
- 8 Click -> right arrow button 
 - a Report will appear in REPORT GROUP PERMISSION GRID

➤ Reports will appear here only if they were assigned to the Application in Security Wizard

➤ If a report is used by multiple applications, it will need to be assigned for each application

Remove Report from Group

- 1 Select User Group in USER GROUP GRID in upper right section
- 2 Select Report in REPORT GROUP PERMISSION GRID in lower right section
- 3 Click <- left arrow button 
 - a Report will disappear from REPORT GROUP PERMISSION GRID

View all Reports assigned to a User Group

- 1 Select User Group in USER GROUP GRID in upper right section
- 2 All linked Reports will appear in the in REPORT GROUP PERMISSION GRID in lower right section
 - a The report will only appear in the Grid once, no matter how many application versions have been assigned

Assign Adhoc Report Views

Use this page to manage the Views that will be available for Adhoc Reports. The Views that were assigned to an Application in Security Wizard will be available here.

Organization: Training Agency

Application: CSBG

Table Name	Table List ID	
vADHOC_Utilization_	41	
vADHOC_Utilization_	42	
vADHOC_Utilization_	43	
vADHOC_Utilization_	44	
vADHOC_Utilization_	45	
vAdhocActivities	181	
vADHOCDemographi	182	
vADHOCActivitiesInA	183	
vADHOCActivitiesInA	184	
vADHOCFlatEntryExt	185	
vADHOCIncomeDem	186	
vADHOCMilestoneSt	187	
vAdhocProfileQuestio	188	
vAdhocQuestions	189	
vADHOCReferral	190	
vAdhocServices	191	
vADHOCSnapshotInc	192	

GroupID	ResourceGroupID	OrgID
TRAgencyAdmi	100903	100129
TRAAI Users	100914	100129
TRACentral Intak	100918	100129
TRACSBG Users	100913	100129
TRAEnergy Users	100912	100129
TRAFamily SelfS	100910	100129
TRAHome Energ	100908	100129
TRAHousing	100911	100129
TRASummer Crisi	100906	100129

Table Name	GroupID	Table List ID	OrgID	
vADHOCIncome	TRACSBG Users	186	100129	5
vADHOCReferral	TRACSBG Users	190	100129	5
vADHOCDemogr	TRACSBG Users	182	100129	5

Organization: Training Agency OrgID: 100129 OrgCode: TRA


Navigating the Reports Page

- All available Views will appear in the VIEW LIST GRID
- All Available User Groups will be listed in the GROUPS GRID
- All Views assigned to the selected User Group will appear in the CONTEXT ADHOC REPORT TABLE LIST GRID

Assign Views to User Group


- 1 Select Application in dropdown

Views assigned to that application in Security Wizard will appear in the VIEW LIST GRID.

- 2 Select View(s) in VIEW LIST GRID on left side of page
 - a To select more than one View in the grid, click and drag down to select multiple rows
 - b Or click on the first View, press CTRL and click on each additional record to add
- 3 Select User Group in GROUP GRID on right side of page
 - a To select more than one User Group in the grid, click and drag down to select all rows
 - b Or click on the first User Group, press CTRL and click on each additional record to add
- 4 Click -> right arrow button
 - a Report will appear in CONTEXT ADHOC REPORT TABLE LIST GRID 

► Views will appear here only if they were assigned to the Application in Security Wizard

Remove View from Group

- 1 Select User Group in USER GROUP GRID in upper right section
- 2 Select View in CONTEXT ADHOC REPORT TABLE LIST GRID in lower right section
- 3 Click <- left arrow button
 - a View will disappear from CONTEXT ADHOC REPORT TABLE LIST GRID 

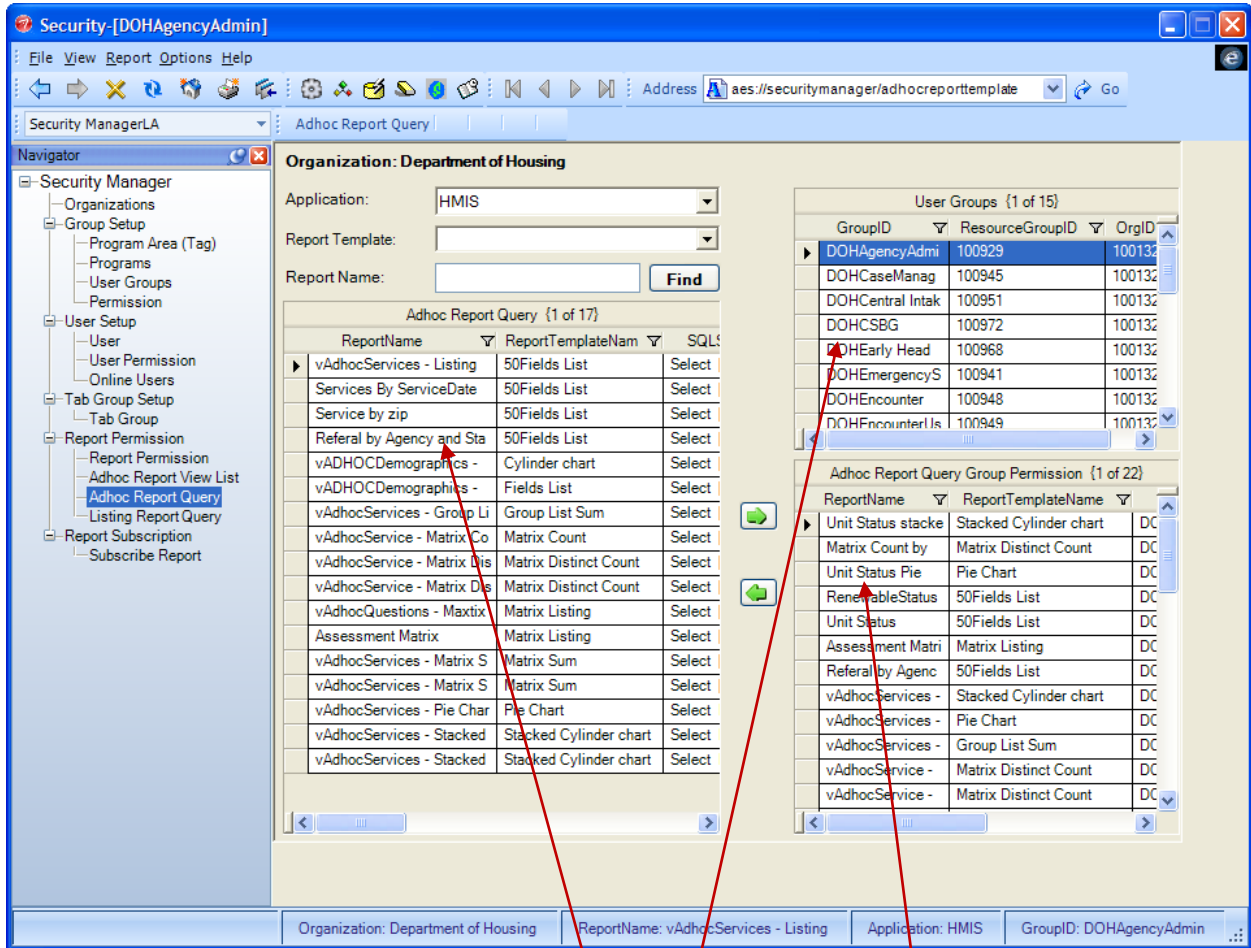
View all Reports assigned to a User Group

- 1 Select User Group in USER GROUP GRID in upper right section
- 2 All linked Views will appear in the in CONTEXT ADHOC REPORT TABLE LIST GRID in lower right section

Note that some views may appear to be listed multiple times in the Grid, which is because each one is linked to a different application. Each view has a Table List ID listed next to it and you will see that same number in the VIEW LIST GRID and in the CONTEXT ADHOC REPORT TABLE LIST GRID.

Assign Adhoc Report Query

Once Adhoc Queries are saved by Administrators and users, use this page to manage the Queries and assign permissions. The Program or User Group must have rights to the Report Type assigned on the Report Permission page and to the View assigned on the Adhoc Report View List page. If sharing Queries between Organizations, remember to select the desired Organization first on the Organizations page.



Navigating the Adhoc Report Query Page

- Limit the list of Queries by selecting an Application and/or Report Template in the dropdowns
- All available Adhoc Report Queries will appear in the ADHOC REPORT QUERY GRID
- All Available User Groups will be listed in the GROUPS GRID
- All Queries assigned to the selected User Group will appear in the ADHOC REPORT QUERY GROUP PERMISSION GRID

View existing Queries

- 1 Select parameters of Query search:
 - a Select Application in dropdown to limit search to one application
 - b Select Report Template to limit search to one template type
 - c Enter Report Name to find one specific Query
 - d Make no selections to find ALL existing Queries
- 2 Click FIND

All matching Queries will appear IN ADHOC REPORT QUERY GRID. Note the Grid shows the Query name, the Report Template used to create the Query and the SQL String; if cursor is paused over SQL String, a tool tip will show the entire string.

View all Reports assigned to a User Group

- 1 Select User Group in USER GROUP GRID in upper right section

All assigned Queries will appear in the in ADHOC REPORT QUERY GROUP PERMISSION GRID in lower right section.

Add Queries to a Group

- 1 Select Query(s) in ADHOC REPORT QUERY GRID on left (see *View existing Queries* above)
- 2 Select User Group(s) in USER GROUP GRID in upper right section
- 3 Click the -> Right Arrow button



The Query will appear in the ADHOC REPORT QUERY GROUP PERMISSION GRID in the lower right section

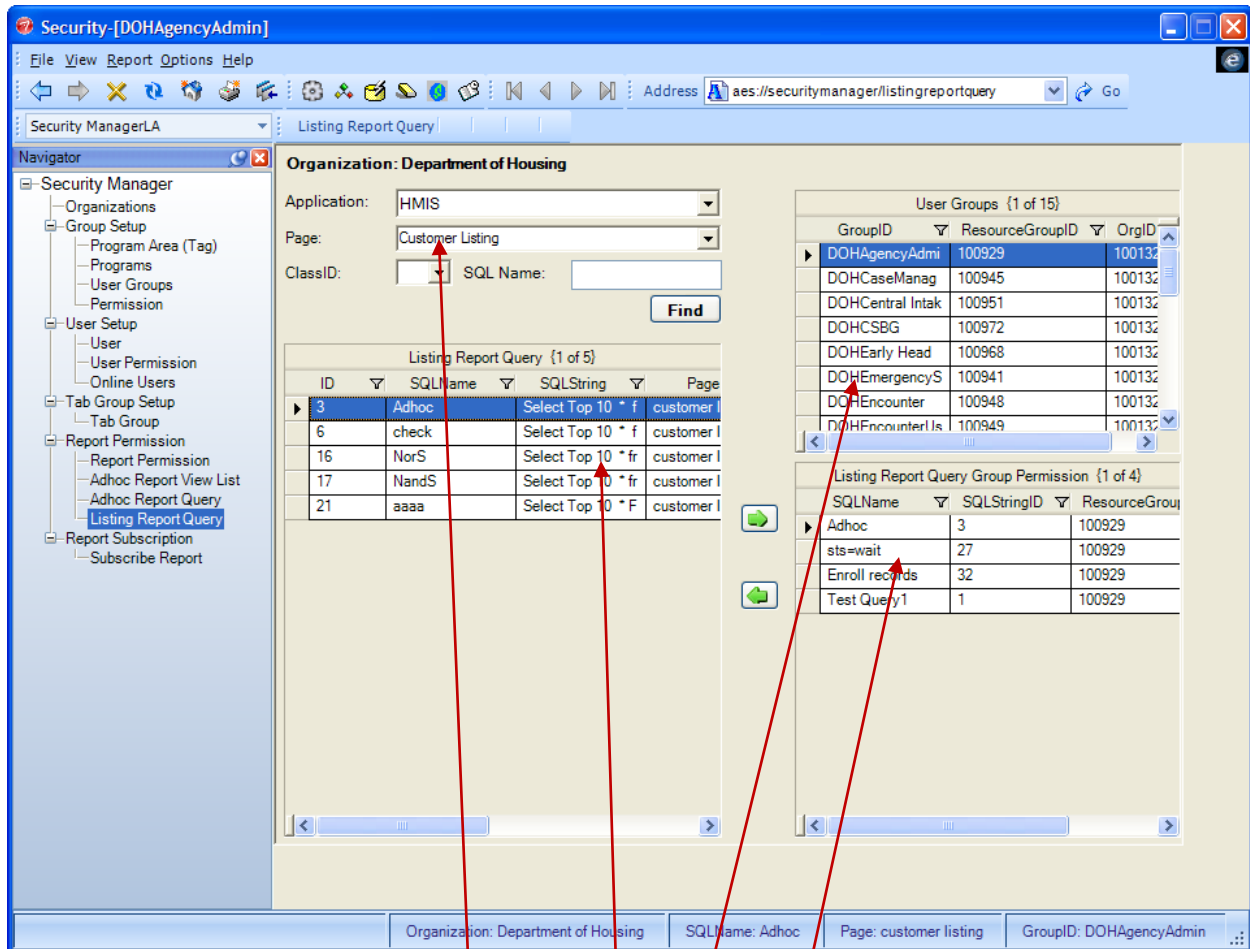
- 4 To remove a Query permission, select it in the and click the <- Left Arrow button



If the Group has not been assigned permission to both the Report Template on the Report Permission page and the Report View used on the Adhoc Report View List page, an error will appear stating the necessary permissions need to be assigned first.

Assign Listing Report Query

Use this page to manage the Queries created on pages in the system and assign Permissions to them; many Queries will be created on the Listing and Customer Listing pages. If sharing Queries between Organizations, remember to select the desired Organization first on the Organizations page.



Navigating the Listing Report Query Page

- Limit the list of Queries by selecting an Application and/or Page in the dropdowns
- All available Listing Report Queries will appear in the LISTING REPORT QUERY GRID
- All Available User Groups will be listed in the GROUPS GRID
- All Queries assigned to the selected User Group will appear in the LISTING REPORT QUERY GROUP PERMISSION GRID

View existing Queries

- 1 Select parameters of Query search:
 - a Select Application in dropdown to limit search to one application
 - b Select page to limit search to just queries created on that page
 - c Enter SQL Name to find one specific Query
 - d Make no selections to find ALL existing Queries
- 2 Click FIND


All matching Queries will appear IN LISTING REPORT QUERY GRID. Note the Grid shows the SQL name, but if the cursor is paused over SQL String, a tool tip will show the entire string.

View all Queries assigned to a User Group


- 1 Select User Group in USER GROUP GRID in upper right section

All assigned Queries will appear in the in LISTING REPORT QUERY GROUP PERMISSION GRID in lower right section.

Add Queries to a Group

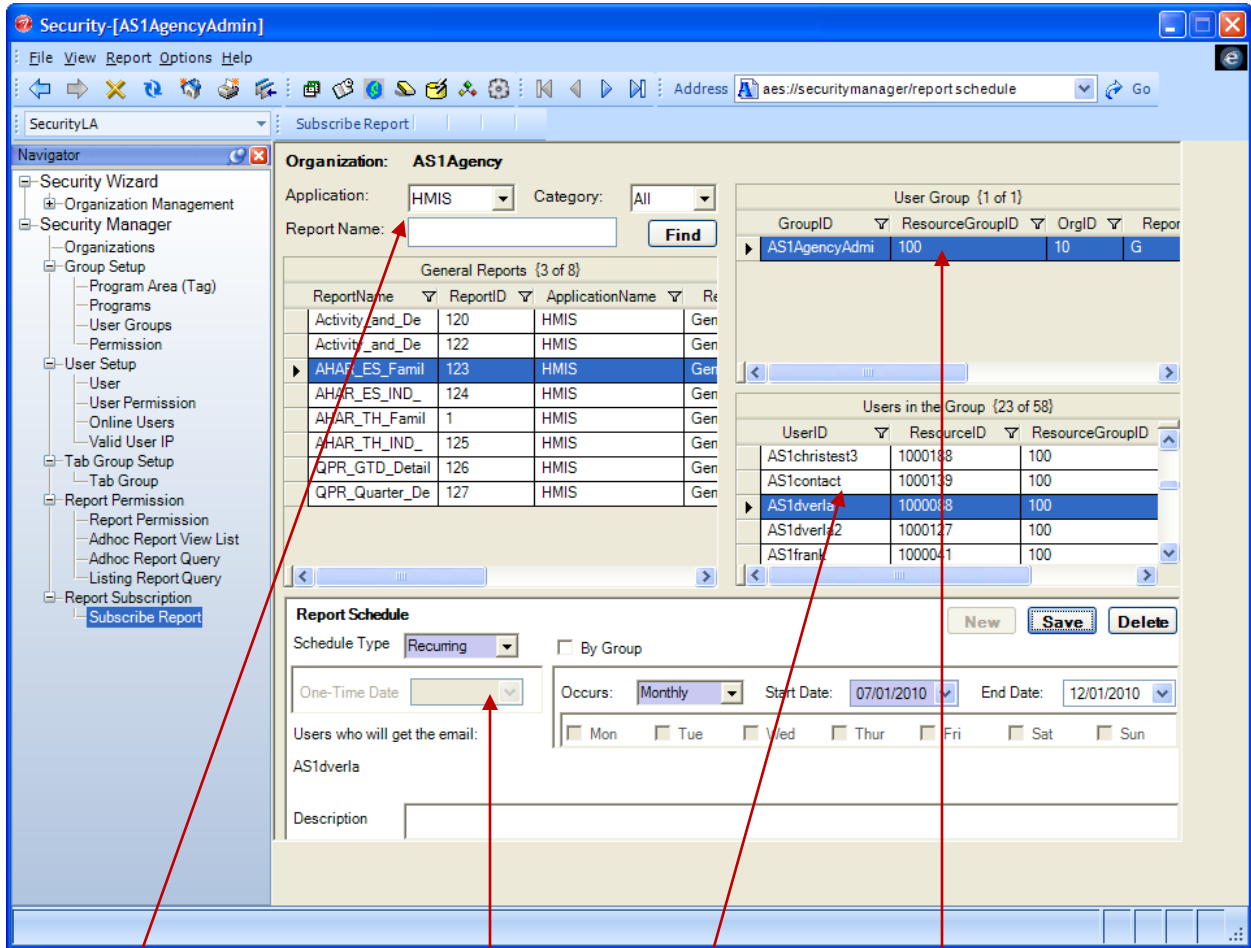
- 1 Select Query(s) in LISTING REPORT QUERY GRID on left (see *View existing Queries* above)
- 2 Select User Group(s) in USER GROUP GRID in upper right section
- 3 Click the -> Right Arrow button 

The Query will appear in the LISTING REPORT QUERY GROUP PERMISSION GRID in the lower right section

- 4 To remove a Query permission, select it in the and click the <- Left Arrow button 

Subscribe Report

Use this page to set up jobs that will automatically execute a management report and email it to select users or to an entire group. The page is agency specific, so you can select any Application and Report that is currently available for that Agency, and then select a User Group and users within that group. The job can be set up to be a onetime occurrence or to be recurring. The report will be emailed to the email addresses of the Users selected.



Navigating the Subscribe Report Page

- Select Management Reports in top left section; matching reports will be displayed in GENERAL REPORT GRID
- All User Groups with permission to that Report will be displayed in USER GROUP GRID
- All Users of selected User Group will be displayed in USERS IN THE GROUP GRID
- Schedule the delivery of Report in bottom section

Schedule Report Delivery to Groups or Users

- 1 Select an Application (HMIS, Head Start, CSBG, etc.)
- 2 Select a Category if needed
- 3 If looking for one report, enter name of report
- 4 Click FIND

All matching reports will appear in GENERAL REPORT GRID.

- 5 Select Report to use in GENERAL REPORT GRID
- 6 Select User Group in USER GROUP GRID on right side of page
 - a All Groups who have permission to selected report will be displayed
- 7 If selecting specific Users, select them in the USER IN THE GROUP GRID
 - a All members of selected User Group will be displayed
- 8 Click NEW button in bottom section

- 1 Select Schedule Type
 - a One Time
 - b Recurring
- 2 If One time
 - a Select Date
 - i) Date must be future date
- 3 If Recurring
 - a Select Occurs:
 - i) Daily
 - ii) Weekly
 - iii) Monthly
 - b Select Start Date and end Date
 - i) Dates must be future dates
 - c Click to create checkmark in Day of week if Weekly
- 4 If sending to entire Group, click to create checkmark in By Group checkbox
- 5 Enter Description
- 6 Click SAVE
- 7 Parameter Popup window will appear
- 8 Click on each item in REPORT PARAMETERS GRID
- 9 Enter Parameter Values
- 10 Click SAVE button
- 11 Repeat for each record in Grid
- 12 Click CLOSE when finished

► It is helpful to run the report once and note the Values for each Parameter; the popup Parameter window will not have dropdowns and you will need to enter a value for each parameter

