



Security Levels in ACT!

There are 3 different types of Security in ACT!: Database Level, User Level and Record Level security.

Database Level Security:

Database Level Security is designed to only allow users with login access to open the database. Users must validate their login information through a currently active user name and password. Users can exist in the database but might be marked as Inactive, which would prevent them from opening the database. This also prevents users who are not members of the database from viewing the data, as they will not have a user name and password.

Single user databases do not require the user to log in. However, adding a password to the single user will then require the user to enter their user name and password when opening the database. Multi-user databases will always require each user to log in with their individual login information.

User Names:

By default, user names will match the Contact field of the 'My Record'. User names are not case sensitive. User names can be changed by Administrator level users only.

Passwords:

Passwords are not required and unless there are security reasons for using a password, it is recommended that a password not be created. When creating a user, or when changing the password on an existing user, the password field can be left blank. When a password is blank, typing anything into the password field will produce an **Invalid user name or password** error when logging into the database.



User Level Security:

There are 5 different User Security Levels in ACT!. Each of the 5 levels has different access rights, which are described below:

Administrator - The Administrator **Security Role** is designed for users who need to have access to all sections of the program. When a database is created, the first user is always an Administrator (this can be modified at a later time). Administrator is the highest level of access and is reserved for those users that are responsible for database maintenance, backup, restore and other general database management. The only information the Administrator does not have direct access to is the private data of other users. Administrators do have the ability to change the passwords of other users.

Manager - The Manager **Security Role** grants access to all primary functions within the program. Manager users have nearly the same access as the Administrator but are limited in some of the database management and maintenance tools. Managers have access to all things the Administrator does, EXCEPT for the following: Manage Users, Delete Database, Database Maintenance, Restore Database, Administer Custom Tables, or View/Archive Logs.

Standard - The Standard **Security Role** is designed for users who only create, and modify their own records, companies, and groups. Standard users do not need to manage the contacts of other users. Standard users can delete records only if they are the Record Manager. Standard users will also have the ability to modify

menus, toolbars, reports, and word templates but will not be able to add fields or modify the layout. In addition, Standard users are not able to setup synchronization.

Restricted - Restricted users have very limited access to the database. A user with the **Security Role** of **Restricted** will be able to add contacts, create activities, and create Sales opportunities. Restricted users also have the ability to create Activity series, and run Reports. However, a restricted user cannot add companies or groups and cannot delete data even if they are the owner. Furthermore, restricted users are not allowed to modify any portion of the database, including menus, tool bars, and layouts. Restricted users will still have access to E-mail and Fax features.

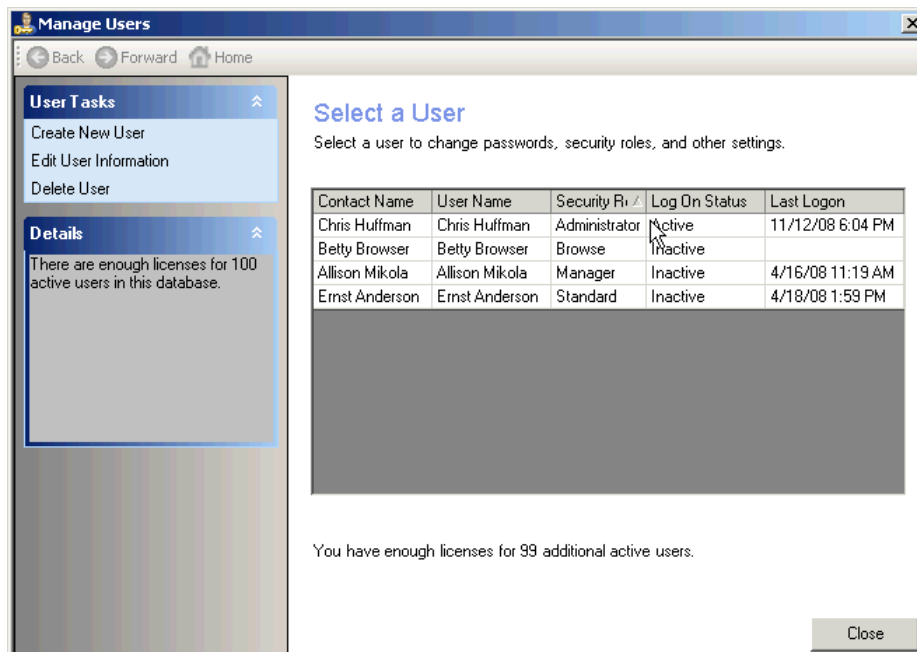
Browse - Browse users have the most limitations. Browse users are only able to view database information and cannot modify this information in any way. However, a user with the **Security Role** of Browse will still have access to Reports and Word Processing functions. All other functions are disabled for Browse users.

Note: Restricted or **Browse** users may not initiate synchronization.

Additionally, custom permissions may be granted by the Administrator to Manager and Standard users to allow them to perform additional tasks within ACT!. These custom permissions are:

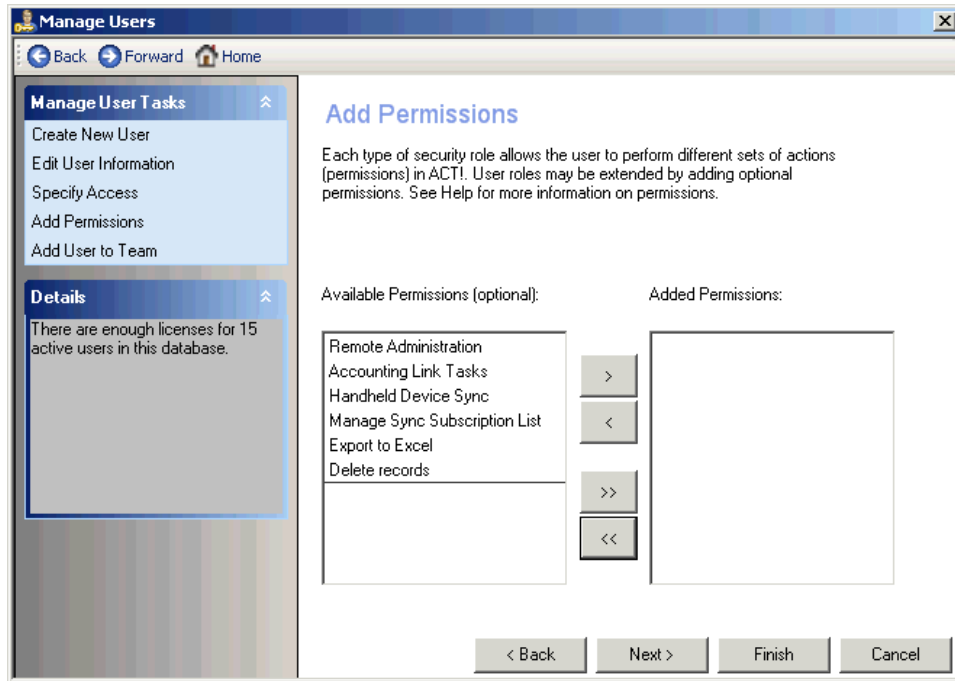
- **Accounting link tasks** - Lets the user install and use an Accounting/back-office link.
- **Handheld device sync** - Lets the user synchronize ACT! with handheld devices.
- **Remote administration** - Lets the user back up, restore, and check and repair a remote database they belong to.
- **Manage Sync Subscription List** (ACT! 2009 and higher) - Lets a remote database user add and remove contacts from their sync set
- **Export to Excel®** - Lets the user export data in a list view to Excel. (*Premium versions only*)
- **Delete records** - Lets the user delete contacts, companies, groups, activity series, notes, histories, opportunities, and secondary contacts the user owns. (*Premium versions only*)

These permissions are set in the **Manage Users - Add Permissions** dialog box (as illustrated below):





Additional Permissions for Manager and Standard User Roles



The following charts show specifically what features that each different **Security Role** has access to:

Contacts:

	Administrator	Manager	Standard	Restricted	Browse
Create/Edit Contacts	X	X	X	X	
Delete "My Contacts"	X	X	X		
Delete Other User's Contacts	X	X			
Move Contact Data	X	X			
Manage Other User's Contacts (change Record Manager and control access)	X	X			
Promote Secondary Contacts ¹	X	X	X		

Opportunities:

	Administrator	Manager	Standard	Restricted	Browse
Create / Edit Opportunities	X	X	X	X	
Delete "My Opportunities"	X	X	X		



Delete Other User's Opportunities	X	X			
Manage Opportunity Process	X	X			
Manage Opportunity Products	X	X			
Manage Other User's Opportunities (change Record Manager and control access)	X	X			

Companies:

	Administrator	Manager	Standard	Restricted	Browse
Create / Edit Companies	X	X	X		
Delete "My Companies"	X	X	X		
Delete Other User's Companies	X	X			
Manage Other User's Companies (Change Record Manager)	X	X			

Groups:

	Administrator	Manager	Standard	Restricted	Browse
Create / Edit Groups	X	X	X		
Delete "My Groups"	X	X	X		
Delete Other User's Group	X	X			
Manage Other User's Groups (Change Record Manager and control access)	X	X			

Activities:

	Administrator	Manager	Standard	Restricted	Browse
Create / Edit / Delete "My Activities"	X	X	X	X	
Manage Custom Activity Types List	X	X			
Manage Priorities List	X	X			
Manage Resources	X	X			
Update Activities with Outlook	X	X	X	X	



Create / Edit Events	X	X			
Edit Delegate for All User's and Resources (cannot be removed)	X	X			
Schedule For (any users)	X	X			
Schedule For (when granted specific access)	X	X	X	X	

Activity Series:

	Administrator	Manager	Standard	Restricted	Browse
Run Activity Series	X	X	X	X	
Create / Edit Activity Series	X	X	X		
Delete My Activity Series	X	X	X		
Delete Other User's Activity Series	X	X			
Manage Other User's Activity Series (Change Record Manager)	X	X			

Reporting:

	Administrator	Manager	Standard	Restricted	Browse
Run Reports	X	X	X	X	X
Create / Edit Reports	X	X	X		
Delete Reports	X	X	X		
Delete Other User's Reports	X	X			

Communications:

	Administrator	Manager	Standard	Restricted	Browse
Enable Email	X	X	X	X	
Enable Telephony	X	X	X	X	
Enable Word Processing	X	X	X	X	
Create / Edit Word Processor Templates	X	X	X		



Data Exchange:

	Administrator	Manager	Standard	Restricted	Browse
Import Data	X	X			
Export Data	X	X			
Export to Excel®	X	X	X		

Customization:

	Administrator	Manager	Standard	Restricted	Browse
Access Layout Editor	X	X			
Customize Menus / Tool bars	X	X	X		

User Management:

	Administrator	Manager	Standard	Restricted	Browse
Manage User's	X				
Reassign Contacts / Activities / Opportunities	X	X			
Manage Teams	X	X			

Database Management:

	Administrator	Manager	Standard	Restricted	Browse
Run ACT! Update	X	X	X		
Access All Non-Private Data	X				
Lock/Unlock Database	X	X			
Delete Database	X				
Database Maintenance	X				
View / Archive Logs	X				
Customize Fields	X	X			
Administer Custom Tables	X				



Backup Database (Does not include Backup Remote Database)	X	X			
Restore Database (Does not include Restore Remote Database)	X				
Edit Duplicate Checking Settings	X	X			
Enable/Disable Allow Files/E-mails Attachment to Database	X				
Enable/Disable Allow History/Notes Editing	X	X			
Set Contact Name Preferences	X	X			
Set Company Creation Preferences	X	X			

Synchronization:

	Administrator	Manager	Standard	Restricted	Browse
Enable Synchronization	X	X			
Initiate synchronization (remote database only)	X	X	X		
Manage Synchronization Setup	X	X			
Manage Subscription List	X	X	X		
Manage Other User's Device Sync Setup	X	X	X		

Online Access

	Administrator	Manager	Standard	Restricted	Browse
Run ACT! Update	X				
Internet Access	X	X	X	X	X

¹ Standard users may only promote Secondary Contacts where the user is the Record Manager for the primary contact

Record Level Security:

Record level security controls access to records in the ACT! database. The record manager has the ability to mark records as **Private** and therefore make these records unavailable to other users. Private data is only visible to the owner. Even users with an administrator role cannot view private data.



Contacts:

Contacts are unique, they have three security options: **Public**, **Private** and **Limited Access**.

- **Public** - Public contacts can be seen by all users.
- **Private** - Private Contacts can only be seen by the Record Manager assigned to that contact record. Administrators do not have the ability to view other users' private contacts. A private contact will, by default, have private notes, histories, activities, and opportunities. A User's 'My Record' cannot be made private, but may contain private notes, histories, activities, and opportunities.
- **Limited Access** - Limited access allows the record manager to identify certain users/teams and give access to these Contacts. When a user is removed from the Limited Access list, the user will continue to have open activities and opportunities with that contact. However, when they clear that activity or change the opportunity in a way to generate a history, they will be notified that they are creating a history for a contact they no longer can access. Once a user is removed from the ACL (Access Control List), they cannot create new activities or opportunities with that Contact.

Note: Limited Access is only available in ACT! Premium for Workgroups.

Notes, Histories, and Opportunities:

If a user has access to a contact; notes, histories, and opportunities can be created and designated as private. Private items/records are not viewable by other users in the database, even if the other users can view the contact record. When a contact is deleted, all notes, histories, and opportunities are deleted, even if they are private.

Activities:

ACT! users will have the ability to view the details of another user's calendar unless the other user's activity is private. In this case, the calendar will reflect busy time for this user, with no reference to any activity details. If an activity is public, but the contact is private, the activity will display but the contact name will not. You cannot add an activity to another user's calendar; unless you have been given delegate permission's to do so. By default, all administrator users will have edit permission. Any user involved in the activity can modify the alarm settings, priority and activity color. However, unless you are a delegate or an organizer for an activity, you cannot modify any other property of the activity.

Groups and Companies:

Standard, Manager, and Administrators can create companies and groups. By default, the creator of the company or group is the Record Manager. The Record Manager can make the group private to other users. Making a company or group private, does not make the contacts and other entities of that company or group private.

Reassigning records:

An administrator or manager can reassign ownership of non-private contacts, activities, opportunities, groups, and companies from one user to another user. Items that cannot be reassigned are Activity series, and History records. Historical fields, such as "Created By" will be unaffected by reassignment. An administrator or manager can reassign records to any user in the database with the exception of Browse users. Records can be reassigned to a user that is not on a contact's Access Control List (ACL). If the designated user is not on the contact's ACL, a notification will be displayed telling the administrator or manager that the user does not have access to that contact. However, the administrator or manager can still reassign the contact to that user.

Mass Reassigning:

Reassignment can be done on a per record basis (per activity, opportunity, etc) or on a per user basis where every record associated with one user may be reassigned to another user. When a record is reassigned, the designated user becomes the record manager of that item.



Mandatory Reassignment:

In the case of mandatory reassignment (deleting a user from the database), private records will be deleted from the database.

User Preferences (under the Tools menu)

Administrator and **Manager** level users have access to all options under Preferences.

Standard and **Restricted** users do not have access to following Preference options:

- Allow history editing (General)
- Allow notes editing (General)
- Names Preferences (General)
- Duplicate Checking options (General)
- Company Preferences (Startup)
- Automatically check for updates (Startup)

Browse users do not have access to the following Preference options in addition to the ones listed for Standard and Restricted:

- Salutation preferences (General)
- Dialer preferences (Communication)