



Act! Security Model

Understanding the Act! Security Model

A large, solid orange circle is positioned in the bottom right corner of the page, partially cut off by the edge.

sw!ftpage™

Table of Contents

Introduction	1
Security Overview	1
User Roles	1
Types of Security	3
Database Security	4
Database Users	4
Log-on Functionality	5
Feature Security	10
Permissions	10
Custom Permissions	19
Record Security	22
Cascading Access	23
Tools for Managing Record Security	24
Edit Contact or Opportunity Access	25
Lookup Contact or Opportunity by Access	26
Field-Level Security	27
Features Affected by Act! Security	29
Differences Between Act! and Act! Premium	29
Calendars	29
Data Exchange	30
Duplicate Checking	30
File Security	31
Companies and Groups	32
Shared Notes and Histories	33
Supporting Applications	34
Synchronization	34
Appendix A – Default Fields in Act!	34

Introduction

The Act! security model is designed to maximize flexibility and provide a variety of options for securing data. Managers and Administrators can leverage Act! security features to limit access to the database, records within the database, and fields related to those records. The entire Act! product family uses the same security model, ensuring consistent data protection across all applications.

This whitepaper explains the Act! security model, including descriptions of the key features, capabilities, and concepts. This document is intended for current Act! customers and potential customers performing functional and technical evaluations of the product, and is based on functionality available in Act! Premium.

Security Overview

The security model supports both stand-alone and workgroup implementations. Security in Act! can be scaled to suit your environment, whether you work alone, with a small team, or with a large workgroup¹. Security can be enforced at the database level, the feature level, the record level, and the field level.

User Roles

The five user roles in Act! are:

- **Administrator** – Administrator is the highest level role in Act!. Users with this role can access all features and all records that have public or limited access. Only private data owned by other users is inaccessible to the administrator. The administrator is the only role allowed to manage users, delete a database, and set the password policy. Users who are responsible for maintaining the database and who need access to most features and data, should be administrators.

Security in Act! can be scaled to suit your environment, whether you work alone, with a small team, or with a large workgroup.

¹ Published minimum system requirements are based on single user environments. Actual scalability and number of networked users supported will vary based on hardware and size and usage of your database. Scalability recommendations are based on in-house performance tests using the recommended server system requirements.

- **Manager** – Managers have access to all features except managing users, deleting a database, and setting the password policy. The manager role can be customized by granting or withholding four permissions. Managers have access to all public records. Users who need to manage teams, modify database schema, manage records owned by other users, create/edit layouts, import/export data, manage custom activity types, or update product information, should be managers.
- **Standard** – The standard role represents the typical user. Users with this role can access most areas of the application, create/edit any record to which they have access, and delete records that they own. Standard users can access only public records and their private records. The standard role can be customized by granting or withholding six permissions. Users who perform a variety of tasks, including creating/modifying word-processing and report templates, but who do not need to modify or maintain the database, should be standard users.
- **Restricted** – Restricted users can access only basic functionality. Users with this role can create/edit contacts, activities, notes, history, and opportunities, but cannot create/ edit groups or companies. Restricted users can run reports and write letters using existing templates, but they cannot modify templates. Restricted users can only access public records and their private records. In addition, users with this role cannot delete any records, even records they own. Typically, restricted users are assistants or others requiring only limited access to features in Act!.
- **Browse** – The browse role gives users read-only access to information in Act!. Browse users can perform lookups, run reports, and print information, but cannot create or modify any data in the Act! database. Temporary employees and users who only need to reference information should be browse users.

When assigning roles to users, make sure users can access all the records they need for any reports they are responsible for producing. If the user doesn't have access to a record, it won't show up in a report.

Types of Security

- **Database Security** – Controls who can use a database. Individuals access an Act! database using a unique user name. The database administrator can also implement a password policy to further restrict database access.
- **Feature Security** – Controls who can use specific features. Each Act! user is assigned a role. Each role dictates which features (permissions) a user can access. Act! also offers custom permissions which can be granted to or withheld from a user.
- **Record Security** – Controls who can see data and what data they can see. Every record has an owner known as a record manager. When a record is marked private, only the record manager can view it. Users can access all public data, their private data, and any limited access records to which they have been granted access. Administrators can access all records except private records owned by other users. A user must have access to a parent record (contact, company, group, or opportunity) to access any extended data (notes, history, activities, or secondary contacts) belonging to that parent record.
- **Field-Level Security** – Controls who can view and modify fields and what fields they can view and modify. Users who are assigned administrator or manager roles can secure fields, so that the information is available only to specific users and/or teams of users. Administrators or managers can give “full access,” “read only access,” or “no access” to fields on a user-by-user basis. A field can be given a default permission that applies to all users. Some core fields and system fields cannot be secured because they are required for basic functionality.



Figure 1: Act! security model

Database Security

Access to an Act! database is protected through the use of unique user names which grant users the right to open a database after logging on.

When a user tries to open an Act! database, he/she must enter a valid user name to access it. If the administrator has implemented a password policy, the user also needs to enter a valid password.

Database Users

Each person who can access an Act! database is a user of that database. Each user is assigned a user name. The user name is a unique identifier – only one user in any given Act! database can use that user name. Each user has a contact record (user record) referred to as “My Record” which represents the user in the database.

Any user with permission to edit contacts can change the name on their “My Record” record, but only an administrator can change the user name associated with that record.

A user’s log-on status must be active for them to access a database. An administrator can set a user’s log-on access to inactive to temporarily restrict that user from opening the database. For example, you may want to make a user inactive when he/she is on medical leave.

Log-on Functionality

General

- Act! remembers the last user name used to open an Act! database and populates the user name field in the Log on dialog box with that data.
- If a user selects the *Remember password* option when logging on to a database, then Act! remembers both the user name and password, and populates both fields in the Log on dialog box when opening that database. Act! maintains saved credentials for each database opened with the Remember password option checked. This information is saved for each local Microsoft® Windows® user.
- If a user does not select the Remember password option when opening a database, Act! only remembers the last user name, as described in the first bullet.

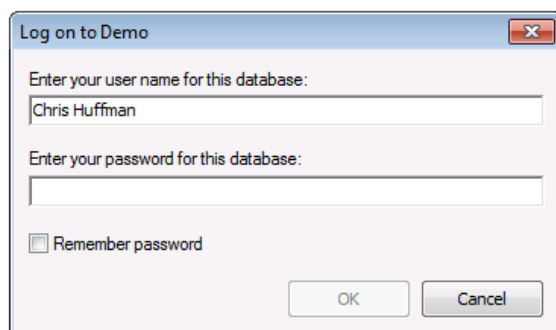


Figure 2: Log on dialog box

Single-User Databases

A single-user database has only one active user. The following log-on behaviors apply to a single-user database:

- If a database contains only one (active) user and no password, the Log on dialog box is bypassed, and the database opens.
- If a password exists for the database, the Log on dialog box appears as usual.
- Remember password functionality applies as described in the General section.

Multi-User Databases

A multi-user database is a database having more than one active user. The following log-on behaviors apply to a multi-user database:

- The Log on dialog box always appears.
- Remember password functionality applies as described in the General section.

External Applications

Act! requires log-on credentials when a user accesses the database through another application. This includes Act! Scheduler, Outlook®, and third-party add-on applications.

Password Policy

The administrator can decide whether passwords are optional or mandatory for users by establishing a password policy. The password policy dictates the parameters of password use for all Act! users. This functionality provides an additional level of protection for the database. By default, no password is required and no password parameters are defined. The administrator can allow users to choose whether or not they use a password, or set any combination of the five optional password settings. When a password policy is defined, it applies to all users. The administrator can also establish individual user password settings. Act! encrypts all passwords.

Password policy parameters are:

- **Re-use** – Restricts the use of recently used passwords. Example: Users cannot reuse their last two passwords.
- **Change interval** – Sets the maximum length of time a password can be used. Example: Users must reset passwords every 90 days.
- **Minimum duration between changes** – Sets the minimum length of time a password can be used. Example: Users cannot change their password every day.
- **Length** – Sets the minimum number of characters a password must contain.

- **Required number of character groups** – Specifies the number of character types the password must contain.
 - Lower-case (a-z)
 - Upper-case (A-Z)
 - Numeric (0-9)
 - Special Characters (printable extended ASCII set)

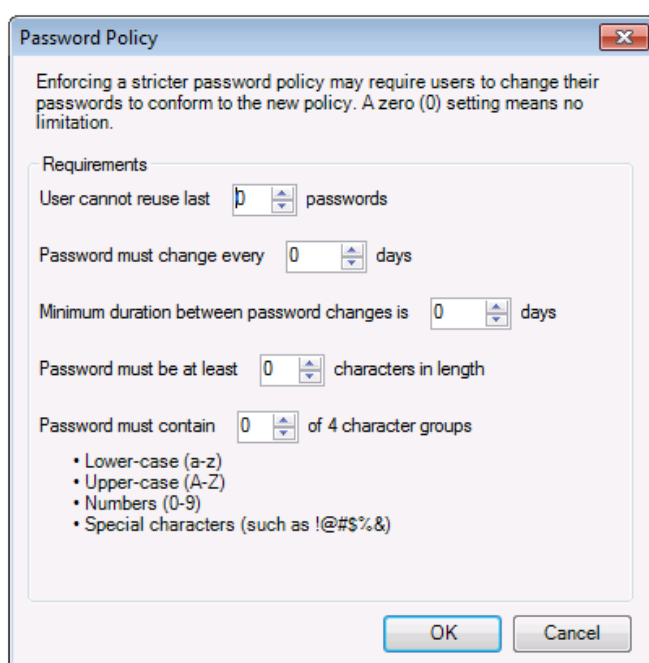


Figure 3: Password Policy dialog box

If a stricter password policy is implemented, users must change their passwords to conform to the new policy. Likewise, when a user's password expires, the user must change the password the next time he logs on to the database.

Note:

User password changes affect any third-party application that uses those log-on credentials to access the Act! database. The password change must be reflected in the log-on credentials entered for each third-party application the user utilizes in addition to Act!

The Set Password dialog box appears when a user is required to change her password. The dialog box informs the user of the current password policy.

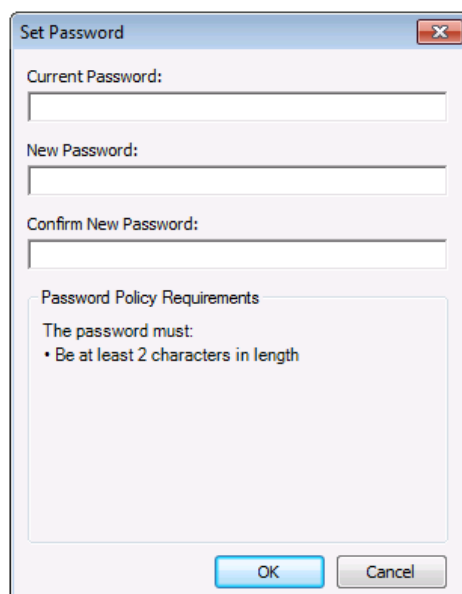
The image shows a 'Set Password' dialog box with a title bar containing a close button. It contains three text input fields labeled 'Current Password:', 'New Password:', and 'Confirm New Password:'. Below these fields is a section titled 'Password Policy Requirements' which contains the text 'The password must:' followed by a bulleted list item '• Be at least 2 characters in length'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 4: Set Password dialog box showing password policy requirements

User Management

Password use can also be managed with individual user settings. These settings can be used to:

- Force a user to change his password the next time he logs on to the database.
- Specify that a user cannot change his password.
- Specify that a user's password never expires.

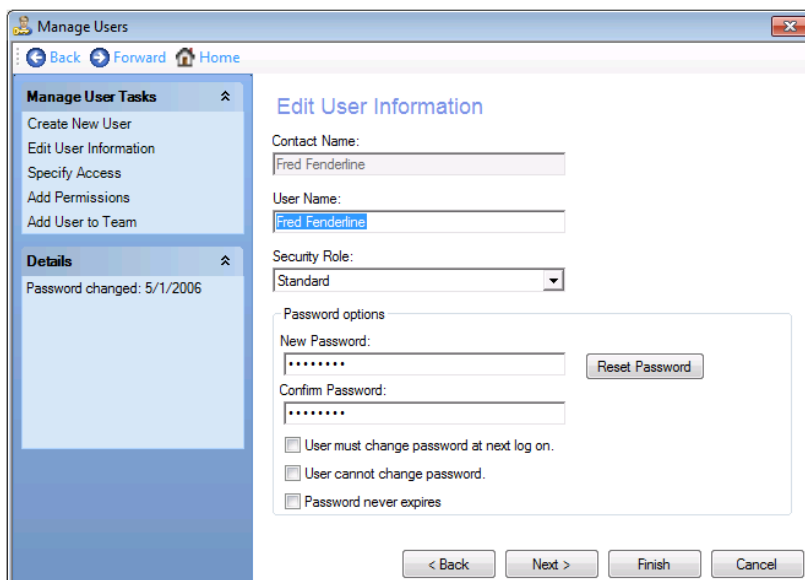


Figure 5: Manage Users screen with password information

Password settings defined in manage users take precedence over password policy settings. For example, if the password policy dictates a password change every 90 days, but a user's manage user settings indicate that the user cannot change a password, the manage user setting applies.

User Reset of Password

Users receive an alert when they attempt to open the database if any of the following has occurred:

- The password policy has changed,
- An administrator has indicated that the user must change her password.
- The user's password has expired,
- Users are required to change their passwords.

A user can also change her password by selecting *Set Password* from the File menu. In all cases, the user is informed of the current password policy.

Feature Security

Each Act! user is assigned one of 5 roles in the database, and each role has different access to features (permissions) within the application. Additionally, custom permissions can be individually granted to or withheld from a user.

Permissions

A permission lets a user or role perform a specific action or use a specific feature. The ability to perform these actions and use these features is managed through granting and/or limiting permissions through role assignment and through the use of custom permissions.

Default permissions are granted to each user based on role. Administrators have the most permissions, and browse users have the fewest.

The following table lists the major permissions in Act! and which permission is assigned to each of the five roles. Default permissions are inherent to the role. Custom permissions can also be granted to managers and standard users.

Permission	Administrator	Manager	Standard	Restricted	Browse
All Records					
Manage Other Users' Records - User can modify the record manager and the access of contacts, companies, groups, opportunities, notes, and histories that other users own (are the record manager for).	x	x			
Delete Records - User can delete contacts, companies, groups, opportunities, notes, and histories which he owns (this user is the record manager).	x	x	<i>Default custom permission</i>		

Permission	Administrator	Manager	Standard	Restricted	Browse
Delete Other Users' Records - User can delete contacts, companies, groups, opportunities, notes, and histories that other users own (are the record manager for).	x	x			
Activities					
Manage Activities - User can schedule, edit, delete, and clear activities.	x	x	x	x	
Activity Delegate for all users – User has permanent ability to schedule, edit, delete, and clear activities for all other users and resources.	x	x			
Manage Custom Activities - User can create, edit, and delete custom activities, priorities, and resources. ²	x	x			
Manage Custom Priorities - User can create, edit, and delete custom priorities.	x	x			
Manage Resources - User can create, edit, and delete resources.	x	x			
Manage Events - User can create, edit, and delete events.	x	x			
Activity Series					
Activity Series – User can schedule activity series.	x	x	x	x	
Manage Activity Series – User can create and edit activity series.	x	x	x		
Manage Other Users' Activity Series – User can edit activity series that	x	x			

² In Act! Premium (access via web), some administrative functions must be performed on the Web server.

Permission	Administrator	Manager	Standard	Restricted	Browse
other users own.					
Delete Activity Series – User can delete activity series that he owns.	x	x	Default custom permission		
Delete Other Users' Activity Series - User can delete activity series that other users own.	x	x			
Contacts					
Manage Contacts - User can create and edit contact records.	x	x	x	x	
Manage Other User's Contacts - User can change record manager and/or modify access to other users' contacts.	x	x			
Delete Contacts - User can delete contacts which he owns.	x	x	Default custom permission		
Delete Other Users' Contacts - User can delete Contacts owned by other users.	x	x			
Manage Notes and Histories - User can create and edit notes and histories. NOTE: Administrators can restrict editing of notes and histories for a database by setting a preference. This preference lets users create notes and histories but disallows editing.	x	x	x	x	
Unlink My Contacts – User can unlink contacts they own (are the record manager for) from linked companies.	x	x	x		
Unlink Other Users' Contacts - User can unlink contacts that other users own (are the record manager for) from linked companies.	x	x			

Permission	Administrator	Manager	Standard	Restricted	Browse
vCard – Send Act! contacts in vCard format to non-Act! users.	x	x			
Companies					
Manage Companies - User can create and edit companies.	x	x	x		
Manage Other User's Companies - User can change the record manager and/or modify access to other users' companies.	x	x			
Delete Companies - User can delete companies which he owns.	x	x	<i>Default custom permission</i>		
Delete Other Users' Companies - User can delete companies owned by other users.	x	x			
Communications					
Manage Email - User can enable email for use with Act! and can transfer/restore the email database.	x	x	x	x	x
Enable Dialer - User can enable and set up telephone dialing.	x	x	x	x	
Manage Default Word Processor - User can select the default word processor used by Act!.	x	x	x	x	x
Manage Word Processing Templates - User can create and edit word-processing templates.	x	x	x		
Write Letters - User can generate letters using word-processing templates.	x	x	x	x	

Permission	Administrator	Manager	Standard	Restricted	Browse
Customization³					
Manage Layouts (Layout Editor) - User can create and edit layout templates.	x	x			
Customize Menus⁴/Toolbars -User can modify menus and toolbars. NOTE: Menu/toolbar customizations apply only to the local copy of Act!. The global toolbar cannot be customized at this time.	x	x	x		
Customize Columns -User can customize columns in list views. Applies to the local Windows user only.	x	x	x	x	x
Customize Navigation Bar -User can customize the appearance of the navigation bar. Applies to local Windows user only.	x	x	x	x	x
Data Exchange					
Import/Export Data - User can import data to and export data from the database.	x	x			
Import/Export Records via Email - User can attach a contact, company, or group to an email and can import such records received as an email attachment.	x	x	x		
Export to Microsoft Excel® -User can export data from designated views to Excel.	x	x	Default custom permission		

³ In Act! Premium (access via web), some administrative functions must be performed on the Web server.

⁴ This feature is not available in Act! Premium (access via web).

Permission	Administrator	Manager	Standard	Restricted	Browse
Database Management⁵					
Back up Database - User can back up the database (does not include backing up personal files).	x	x			
Copy Database - User can save a copy of the database.	x	x			
Copy/Move Contact Data - User can copy or move data from one contact to another using the Copy/Move feature.	x	x			
Database Maintenance - User can perform database Check and Repair and Remove Old Data.	x				
Define Fields - User can modify the database schema (create, edit, and delete fields), rename fields, manage drop-down lists, and set up fields linked to companies.	x	x			
Delete Database – User can delete the database.	x				
Lock Database – User can lock the database.	x	x			
Manage Database Preferences - User can edit global database preferences such as Duplicate Checking, Name Preferences, Allow Editing of Notes or Histories, or Company Linking.	x	x			
Password Policy - User can define and modify the password policy.	x				

⁵ In Act! Premium (access via web), some administrative functions must be performed on the Web server.

Permission	Administrator	Manager	Standard	Restricted	Browse
Remote Administration - Non-administrator user in a remote database can back up the database, restore a database back-up file, and perform database maintenance (Check and Repair only).	X	<i>Available custom permission</i>	<i>Available custom permission</i>		
Restore Database - User can restore a database backup file.	X				
Scan for Duplicates - User can scan the database for duplicate records.	X	X	X	X	X
Share Database - User can share the database for use by multiple users.	X				
General Features					
Backup/Restore Personal Files - User can back up and restore personal supplemental files (documents, Internet links, dictionaries, and menu/toolbar customizations). NOTE: Applies only to the local Act! installation.	X	X	X	X	X
Perform Lookups - User can perform lookups and advanced queries on data in Act!.	X	X	X	X	X
Printing - User can print Act! address books, calendars, email, envelopes, labels, lists, reports, and documents.	X	X	X	X	X
Run Act! Update - User can update the Act! application (does not include database upgrade).	<i>Not governed by security or permissions.</i>				

Permission	Administrator	Manager	Standard	Restricted	Browse
Upgrade Database - User can upgrade the database to work with a newer version of Act!.	X	X	Default permission granted to "Lone Standard User"		
Groups					
Manage Groups – User can create and edit groups.	X	X	X		
Manage Other User's Groups - User can change the record manager and/or modify access to other users' groups.	X	X			
Delete Groups - User can delete groups which he owns.	X	X	Default custom permission		
Delete Other Users' Groups - User can delete groups owned by other users.	X	X			
Opportunities					
Manage Opportunities - User can create and edit opportunities.	X	X	X	X	
Manage Other User's Opportunities - User can change the record manager and/or modify access to other users' opportunities.	X	X			
Delete Opportunities - User can delete opportunities which he owns.	X	X	Default custom permission		
Delete Other Users' Opportunities – User can delete opportunities owned by other users.	X	X			
Manage Opportunity Processes - User can create and edit opportunity processes.	X	X			

Permission	Administrator	Manager	Standard	Restricted	Browse
Manage Opportunity Products - User can create and edit opportunity products.	x	x			
Reporting					
Run Reports - User can run reports using report templates.	x	x	x	x	x
Manage Report Templates (Report Designer) – User can create, edit, and delete report templates.	x	x	x		
Synchronization, Database⁶					
Enable Synchronization – User can get the database ready for synchronization.	x	x	x		
Manage Synchronization Setup - User can set up database synchronization.	x	x			
Manage Subscription List - User can modify the synchronization subscription list.	x	Default custom permission	Default custom permission		
Restore Remote Database – User can unpack and restore a remote database for synchronization.	Not governed by security or permissions.				
Initiate Database Synchronization - User can initiate database synchronization.	x	x	x		
Synchronization, Other					
Accounting Link Tasks – User can set up and perform accounting link synchronization.	x	Default custom permission	Available custom permission		

⁶ In Act! Premium (access via web), some administrative functions must be performed on the Web server.

Permission	Administrator	Manager	Standard	Restricted	Browse
Handheld Device Sync⁷ - User can set up and perform handheld device synchronization.	x	<i>Default custom permission</i>	<i>Available custom permission</i>		
Outlook Activity Sync⁸ - User can update the Act! calendar with activities from Microsoft Outlook.	x	x	x	x	
User/Team Management					
Manage Users - User can create, edit, and delete users. Modifications include custom permissions, password settings, or role assignment.	x				
Manage Teams - User can create, edit, and delete teams.	x	x			

Custom Permissions

A custom permission is an optional permission which can be granted to, or restricted from, an individual who has a manager or standard role. Administrators are irrevocably granted all permissions in the database. No custom permissions are available to restricted and browse users.

The six custom permissions available in Act! Premium are:

- **Accounting link tasks** - Ability to perform Accounting Link tasks.
- **Delete records** - Ability to delete contacts, companies, groups, opportunities, notes, and histories which the user owns (is the record manager for).
- **Export to Excel** - Ability to export list view data to Microsoft Excel.
- **Handheld device sync⁹** – Ability to set up and perform handheld device synchronization.

⁷ This feature is not available in Act Premium (access via web).

⁸ This feature is not available in Act Premium (access via web).

- **Remote administration** – Ability of a non-administrator in a remote database to perform database maintenance, back up a database, and restore a database backup file. This permission does not include the ability to remove old data.
- **Manage subscription list** – Ability to modify the database synchronization subscription list. In a remote database, the subscription list displays the contacts currently included in the sync set. Users with this permission can add or remove contacts from the sync set.

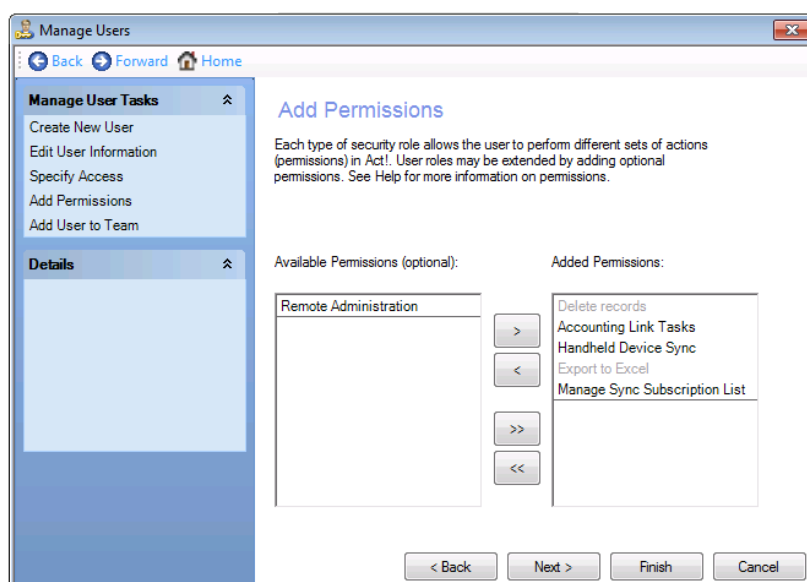


Figure 6: Manage Users dialog box showing available user preferences

Manager and Standard Roles

An administrator can grant or restrict any of four custom permissions to users with a manager role:

- *Accounting Link Tasks* - granted by default, but can be removed
- *Handheld Device Sync*¹⁰ - granted by default, but can be removed

⁹ This feature is not available in Act! Premium (access via web).

¹⁰ This feature is not available in Act Premium (access via web).

- *Manage Subscription List* - granted by default to managers of a synchronizing database, but can be removed
- *Remote Administration* - available to managers of a synchronizing database

An administrator can grant or restrict any of six custom permissions to standard role users

- *Export to Excel* - granted by default, but can be removed
- *Delete Records* - granted by default, but can be removed
- *Accounting Link Tasks* - available to standard users
- *Handheld Device Sync*¹¹ - available to standard users
- *Manage Subscription List* - available to standard users of a synchronizing database
- *Remote Administration* - available to standard users of a synchronizing database

Available Custom Permissions by Role

Permission	Administrator	Manager	Standard	Restricted	Browse
Accounting link tasks	n/a	x	x		
Export to Excel	n/a	n/a	x		
Delete records	n/a	n/a	x		
Handheld device sync ¹²	n/a	x	x		
Manage subscription list	n/a	x	x		
Remote administration	n/a	x	x		

n/a – base permission granted as part of the designated role.

¹¹ This feature is not available in Act Premium (access via web).

¹² This feature is not available in Act Premium (access via web).

Default Custom Permissions by Role

Permission	Administrator	Manager	Standard	Restricted	Browse
Accounting link tasks	n/a	x			
Export to Excel	n/a	n/a	x		
Delete records	n/a	n/a	x		
Handheld device sync ¹³	n/a	x			
Manage subscription list	n/a	x	x		
Remote administration	n/a				

n/a – base permission granted as part of the designated role.

Record Security

Record security in Act! is determined by ownership, by role, and by the access list. The access list lists users and/or teams who can access a record. Administrators can assign user access to individual contacts, companies, groups, or opportunities using the access list.

Each record in Act! has an owner known as the record manager. A record manager can change the ownership and modify the access list of records which he owns. This permission does not extend to Browse users, who are not allowed to modify the database in any way.

Administrators and Managers can also modify ownership or the access list of any records they can access. Standard and Restricted users can modify the ownership and access list of only those records they own. The record manager (owner) is always included in the access list for that record.

A user must have access to a record to view it in any way. If a user does not have access to a record, he will not be able to find it using lookups, include it in reports,

¹³ This feature is not available in Act Premium (access via web).

print its information, or include it in mail merges. Inaccessible records do not appear in any views or lists.

The three access types are:

- **Public access** – All users in the database can access a public record. Contacts, companies, groups, opportunities, and all extended data record types can be public access. Extended data records are explained in the following Cascading Access section. All user records (contacts) are public.
- **Private access** – Only the owner (record manager) can access a private record. Contacts, companies, groups, opportunities, and all extended data record types can be marked as private.
- **Limited Access** – Allows access to a contact, company, group, or opportunity record¹⁴ by designated users and/or teams. Record managers can always access contacts they own. All users with administrator roles can also access all limited access records by default.

When a record is designated as “private,” only the record manager can view it. An administrator can access all records except private records owned by other users.

Note:

Users can modify preferences to set the default access list of newly created records. For example, a salesperson may want all new contact records to be limited access, accessible only by the “Sales Team.” This setting is on the Startup tab of the Preferences panel.

Cascading Access

Record security is further limited by “cascading access,” which means that the record security of certain types of records (parent records) affects the security of other types of records (extended data records).

A parent record is a contact, company, group, or opportunity. These four top-level record types can exist independently of any other type of record in Act! and can own extended data. Extended data refers to record types which cannot exist

¹⁴ Only certain fields can be designated as read-only or no access. Limited access is only available to Act! Premium and Act! Premium (access via web) only.

independently, such as notes, histories, activities, and secondary contacts. Extended data always belongs to one or more parent records.

Notes and histories can belong to contacts, companies, groups, opportunities, and/or any combination of those. Activities can belong only to one or more contacts. Secondary contacts can belong only to one parent contact record.

A user must have access to a parent record (contact, company, group, or opportunity) to access any extended data (notes, history, activities, or secondary contacts) belonging to that parent record.

Example: A user who cannot access a contact also cannot access a note belonging to that contact, regardless of the access list or record manager of the note.

If an extended data record belongs to (is shared by) two or more parent records of any type, accessibility to the extended data record is limited to those users with access to at least one of the parent records.

Cascading access does not grant any more access to an extended data record than the user has to the extended data record itself. For example, User A has access to a contact, Joe Smith, but cannot access a private note owned by User B (record manager) for Joe Smith.

Tools for Managing Record Security

A variety of tools are available for managing record security.

Access Level

Access Level information is found on the Contact Access, Company Info, Group Info, and Opportunity Info tabs on the contact, company, group, and opportunity detail views and lets the user change access to the current record.

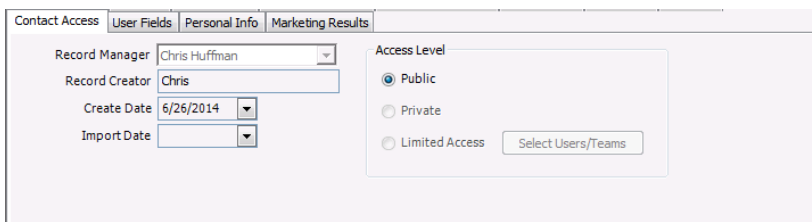


Figure 7: Contact Access tab showing access level information

Users set access to extended data by selecting or clearing the private check box found in the lower left corner of create/edit dialog boxes for each extended data type (activities, notes, history, and secondary contacts).

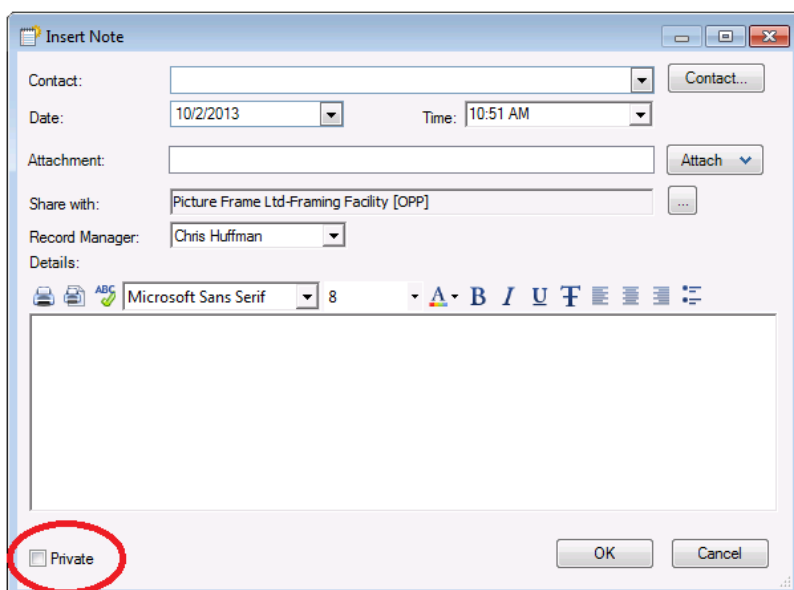


Figure 8: Insert Note dialog box with Private check box

Edit Contact or Opportunity Access

Users with the appropriate access role can change the access level of contacts or opportunities en masse, by selecting a bulk update function from the *Contacts*> *Edit Contact Access* menu when the Contact List view is displayed, or from the *Opportunities*> *Edit Opportunity Access* menu when the Opportunities List view is displayed. The commands operate on the selected contacts or opportunities in the list.

The available functions include:

- *Make Contact (or Opportunity) Private* – changes the selected contacts records to private access.
- *Make Contact (or Opportunity) Public* – changes the selected records to public access.
- *Add Users/Teams* – adds one or more users and/or teams to the access lists of the selected records.
- *Remove Users/Teams* – removes one or more users and/or teams from the access lists of the selected records.
- *Create New Access List* – creates a new access list for the selected records.
- *Edit Access List* – allows you to edit an existing access list for the selected records.

To change access, the user must be an administrator, manager, or the record manager of all the selected contacts (or opportunities).

Lookup Contact or Opportunity by Access

Users can perform contact lookups by access type, record manager, or the users/teams who can access the records. Users can find contact (or opportunity) records using criteria related to access by clicking **Lookup> By Access**.

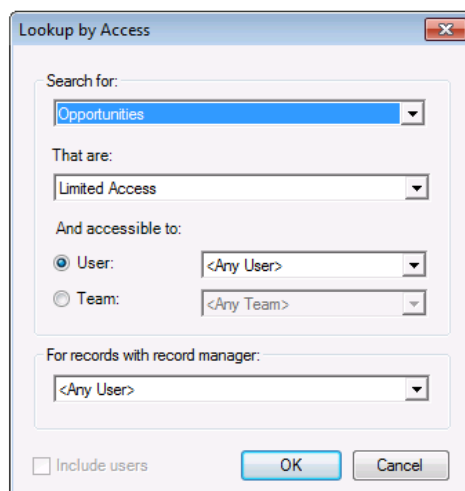


Figure 9: Lookup by access

Field-Level Security

Administrators and managers can secure fields using Define Fields functionality, allowing access to or denying access from specific users or teams of users. Users can be given full access, read only access, or no access¹⁵ to fields on a user-by-user basis. A field has a Default Permission that applies to all users until modified by the administrator. Field-Level Security (FLS) can be set on an inclusive (allow only these users to have full access) or exclusive basis (allow full access to everyone except these users). Users cannot limit access to some core fields or system fields because they are required for basic Act! functionality (see Appendix A).

Note:

Since all administrators and managers can define fields, security on fields is only a reminder to those types of users. For example, an administrator can give himself read-only access to a particular field to prevent himself from making any inadvertent changes to that field.

Field level security uses three levels of access:

- **Full Access** – User can view and modify data in the field.
- **Read Only Access** – User can view data in the field, but not modify it.
- **No Access** – User can neither view nor modify data in the field.

All users who can access a record can access read-only fields in that record in searches, reporting, mail merge, and views. Many system fields, such as Edit Date and Create Date, are permanently designated as read-only.

If a user has no access to a particular field, it's as if the field does not exist for that user. When that user accesses the database, the no-access field will not appear in any view, and the user cannot access the contents of a no access field in any way.

¹⁵ Only certain fields can be designated as read-only or no access.

Field access can be controlled using one or more types of permissions:

- **Default permission** – The base access level of a field which, in the absence of any team or user permissions, applies to all users of the database. The default permission applies to all users not affected by any team or user permissions.
- **Team permission** – Access granted to members of a specific team. Team permission takes precedence over the default permission.
- **User permission** – Explicit access granted to a specific user. User permission takes precedence over both team permission and the default permission.

Act! Interface

Team and User Permissions are available only in Act! Premium. Also, fields can be set to “no access” only in Act! Premium.

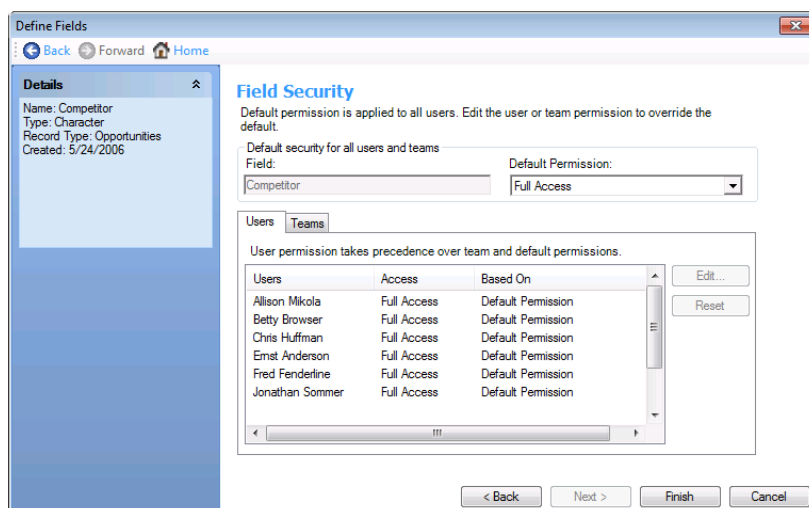


Figure 10: Field level security on the Competitor field

Features Affected by Act! Security

This section provides describes the effects of security on Act! features.

Differences Between Act! and Act! Premium

This document is based on functionality available in Act! Premium, which is targeted for individuals and smaller workgroups and has some differences in features related to security. The major differences between Act! and Act! Premium are described in this section.

Custom Permissions

While there are six custom permissions in Act! Premium, only four custom permissions are available in Act! Pro. In Act! Pro, "Delete records" and "Export to Excel" are granted by default and cannot be removed.

Default permissions for roles are identical in Act! Pro and Act! Premium. The Accounting link tasks, "Handheld device sync," "Remote administration," and "Manage Subscription List" custom permissions are available to standard role users in Act! Pro. "Delete records" and "Export to Excel" appear in the interface only for Act! Premium.

Record Security

Teams and limited access list features are available only in Act! Premium.

Field-Level Security

Only the Default Permission setting for field level security is available in Act! Pro. In addition, fields cannot be set to no access in Act! Pro. User and team permissions are available only in Act! Premium.

Calendars

While users cannot open activities they don't have access to, the existence of those activities does impact Act! calendar views and the Availability tab of the Schedule dialog box. Other users in a workgroup can determine "free-busy" information. Users without access can only determine the owner, date, and time of the activity.

Activities displayed in the calendar without details are either private and owned by another user (scheduled for), or they are public but belong to an inaccessible contact record. Other users, without access, cannot view the details of such activities. The activities themselves are not included in activity lists, reports, or lookups for those users.

Data Exchange

Data import and export adheres to all four types of security (database, feature, record, and field level). Only administrators and managers can import or export Act! data. Standard users can export lists to Microsoft Excel and can import Act! contact records received via email (see [Permissions](#)).

During import/export, log-on credentials determine the data that can be extracted from the source database and inserted into the target database. The user performing the import/export must have the appropriate permissions in both databases.

Further, the user performing the import or export can only bring in and/or update data which that user can access. Inaccessible data is not available in the source database, and inaccessible records in the target database will not be updated with any new data.

The same concepts apply to field-level security. Any read-only field is available as a source of data during the data exchange process, but cannot be used as destination for incoming data. No access fields cannot be used as sources of data.

Note:

To avoid issues with field level security, the user performing the import or export should have access to all fields which are intended to be involved in the data exchange process.

Duplicate Checking

The primary Duplicate Checking function occurs when records are created. If duplicate checking is enabled, a user creating a contact, company, or group receives an alert if the record she is attempting to create is a duplicate of an

accessible record of similar type. If the user creating the duplicate cannot access the existing record, she will not receive the alert message.

Example 1: Duplicate checking is enabled. Chris Huffman tries to create a group called “Prospects.” The duplicate matching criteria identifies an existing public group. Chris will be notified that there is already a “Prospects” group in the database.

Example 2: Duplicate checking is enabled. Chris Huffman attempts to create a group called “Friends.” The duplicate matching criteria identifies an existing group. However, Chris cannot access the matching group. In this case, Chris will not be notified that a “Friends” group already exists in the database.

File Security

Act! leverages Windows file security to manage access to non-database items stored in the file system. These items include:

- Attachments to contacts, groups, companies, activities, histories, opportunities or notes
- Document tab items
- Layout templates
- Saved queries
- Report templates
- Word processor templates
- Dashboards

To use features related to these items, users must have Windows access to the related folders. When a database is shared, this access is handled by Act!.

If access to these folders or individual files is modified through the operating system, some features cannot work properly. Along with the functionality related to the previous items, affected features can also include opening the database and performing synchronization tasks.

Companies and Groups

Tree Views

Companies and groups can be organized hierarchically to mirror organizational structures or simply for convenience. This organization appears in a tree view in the main company and group views, as well as in company/group selection dialog boxes.

Both companies and groups can be assigned any of the three available record access levels —public, private, or limited access¹⁶. This flexibility presents challenges in the hierarchy display.

To accommodate the need to organize the hierarchy and the need for the database to contain companies/groups of varying access levels, the existence of limited access companies and groups is revealed in tree views. However, only the names of companies/groups can be seen by all users in views. The user can view, search, or obtain reports on other data, details, memberships, or other information related to the company or group only if the user can access the company or group in question. Inaccessible private companies and groups do not appear in tree views.

Sub-Groups and Company Divisions

While public and limited access companies and groups can exist anywhere in the organizational hierarchy, there are limitations related to private companies and groups. A private company or group cannot have sub-groups or divisions with public or limited access.

Company Linking

A contact linked to a company can be updated based on changes made to the linked company record. This linking functionality occurs only if the user initiating the update can access both the linked contact and company records. Additionally, the user initiating the update must have at least read only access to the linked fields on the company record and full access to the linked fields on the contact record.

¹⁶ Only certain fields can be designated as read-only or no access. Limited access is only available to Act! Premium and Act! Premium (access via web) users.

Record Access Limitations

For company linking updates to occur, the user performing the update must have access to both the company and the linked contact. If a contact is inaccessible:

- Company link updates will not occur.
- A contact and company link cannot be established.

If a company is inaccessible:

- Company link updates will not occur.
- A contact and company link cannot be established.
- The linked contact displays the company name, even if the company is inaccessible. However, the user cannot access the linked company record.
- An administrator, manager, or the record manager of a contact can unlink the contact from a linked company even though the company record is inaccessible.

Field-Level Security Limitations

For company linking updates to occur, the user performing the update must have at least read-only access to linked company fields and full access to linked contact fields. If the user does not have access to linked fields, those fields cannot be updated using the company linking feature. However, all accessible fields will be updated.

Shared Notes and Histories

Notes and histories can be shared (co-owned) by multiple parent records. When shared notes or histories are created, users who can access any parent contact, company, group, or opportunity record can also access the shared notes/histories.

This sharing occurs by default between a contact and a company when the two are linked. All notes and histories created on a linked contact are shared with the company to which it is linked. This functionality can be disabled by changing company preferences. This preference applies to associated activities and opportunities for linked records.

Note:

If the parent records (contacts, companies, groups, or opportunities) have different access levels, data that might be thought to be secured based on cascading access will be seen by users having access to any of the parent records.

Supporting Applications

The Act! security model applies to and affects external applications which access the Act! database and data within it. Security for Act! data is enforced for these applications just as it is in Act!. This includes Act! Network Sync Service, Act! Internet Sync Service, Act! Scheduler, Act! SDK (Software Developer's Kit), and Act! Premium (access via web).

Synchronization

Act! synchronization is a database-to-database process. Security is enforced, not in the synchronization process itself, but instead in security for the database, features, records, and fields. During synchronization, data is transferred and updated without regard to access by the user who set up synchronization, or by the user who initiated synchronization. For example, an administrator with little or no access to a certain set of data can designate that data to be synchronized to a particular remote database through use of the sync set definition.

Security ultimately controls what data a user can see and what functions the user can perform. The data that is transferred between databases is defined during synchronization setup. While synchronization can be used to filter data sent to the remote (subscriber) database, the data accessible to the user of that remote database is always a subset of the data the user would see if she were to log onto the main (publisher) database.

Appendix A – Default Fields in Act!

The following table lists all the default fields in a new Act! database. The table also shows which field level security access level can be assigned to each field. Some

core fields and system fields cannot be secured because they are integral to basic Act! functionality.

Field Name	Type	May be deleted?	Full Access	Read Only	No Access
Contacts					
Address1	contact	no	x	x	x
Address2	contact	no	x	x	x
Address3	contact	no	x	x	x
Alternate Extension	contact	no	x	x	x
Alternate Phone	contact	no	x	x	x
Birth Date	contact	x	x	x	x
City	contact	no	x	x	no
Company	contact	no	x	x	no
Contact	contact	no	x	x	no
Country	contact	no	x	x	x
Department	contact	no	x	x	x
E-mail	contact	no	x	x	no
Extension	contact	no	x	x	x
Fax Extension	contact	no	x	x	x
Fax Phone	contact	no	x	x	x
Home Address1	contact	no	x	x	x
Home Address2	contact	no	x	x	x
Home Address3	contact	no	x	x	x
Home City	contact	no	x	x	x
Home Country	contact	no	x	x	x
Home Extension	contact	no	x	x	x
Home Phone	contact	no	x	x	x
Home State	contact	no	x	x	x
Home ZIP Code	contact	no	x	x	x
Home	contact	no	x	x	x
ID/Status	contact	no	x	x	no
Last Results	contact	no	x	x	x
Messenger ID	contact	no	x	x	x
Mobile Extension	contact	no	x	x	x

Field Name	Type	May be deleted?	Full Access	Read Only	No Access
Mobile Phone	contact	no	x	x	x
Pager Extension	contact	no	x	x	x
Pager Phone	contact	no	x	x	x
Personal E-mail	contact	no	x	x	x
Phone	contact	no	x	x	no
Referred By	contact	no	x	x	x
Salutation	contact	no	x	x	no
Spouse	contact	x	x	x	x
State	contact	no	x	x	no
Title	contact	no	x	x	x
User 1	contact	x	x	x	x
User 2	contact	x	x	x	x
User 3	contact	x	x	x	x
User 4	contact	x	x	x	x
User 5	contact	x	x	x	x
User 6	contact	x	x	x	x
User 7	contact	x	x	x	x
User 8	contact	x	x	x	x
User 9	contact	x	x	x	x
User 10	contact	x	x	x	x
Web Site	contact	no	x	x	x
ZIP Code	contact	no	x	x	no
Companies					
Address1	companies	no	x	x	x
Address2	companies	no	x	x	x
Address3	companies	no	x	x	x
Billing Address 1	companies	no	x	x	x
Billing Address 2	companies	no	x	x	x
Billing Address 3	companies	no	x	x	x
Billing City	companies	no	x	x	x
Billing Country	companies	no	x	x	x
Billing State	companies	no	x	x	x
Billing ZIP Code	companies	no	x	x	x

Field Name	Type	May be deleted?	Full Access	Read Only	No Access
City	companies	no	x	x	no
Company	companies	no	x	no	no
Company Description	companies	no	x	x	x
Country	companies	no	x	x	x
Division	companies	x	x	x	x
Extension	companies	no	x	x	x
Fax Extension	companies	no	x	x	x
Fax Phone	companies	no	x	x	x
ID/Status	companies	no	x	x	no
Industry	companies	no	x	x	x
Number of Employees	companies	x	x	x	x
Phone	companies	no	x	x	no
Referred By	companies	no	x	x	x
Region	companies	x	x	x	x
Revenue	companies	x	x	x	x
Shipping Address1	companies	no	x	x	x
Shipping Address2	companies	no	x	x	x
Shipping Address3	companies	no	x	x	x
Shipping City	companies	no	x	x	x
Shipping Country	companies	no	x	x	x
Shipping State	companies	no	x	x	x
Shipping ZIP Code	companies	no	x	x	x
SIC Code	companies	x	x	x	x
State	companies	no	x	x	no
Territory	companies	x	x	x	x
Ticker Symbol	companies	x	x	x	x
Toll-Free Extension	companies	no	x	x	x
Toll-Free Phone	companies	no	x	x	x
Web Site	companies	no	x	x	x
ZIP Code	companies	no	x	x	no
Groups					
Address1	groups	no	x	x	x
Address2	groups	no	x	x	x

Field Name	Type	May be deleted?	Full Access	Read Only	No Access
Address3	groups	no	x	x	x
City	groups	no	x	x	x
Country	groups	no	x	x	x
Group Description	groups	no	x	x	x
Group Name	groups	no	x	no	no
State	groups	no	x	x	x
ZIP Code	groups	no	x	x	x
Opportunities					
Competitor	opportunities	no	x	x	no
Gross Margin	opportunities	no	no	x	no
Opportunity Field 1	opportunities	no	x	x	no
Opportunity Field 2	opportunities	no	x	x	no
Opportunity Field 3	opportunities	no	x	x	no
Opportunity Field 4	opportunities	no	x	x	no
Opportunity Field 5	opportunities	no	x	x	no
Opportunity Field 6	opportunities	no	x	x	no
Opportunity Field 7	opportunities	no	x	x	no
Opportunity Field 8	opportunities	no	x	x	no
Opportunity Name	opportunities	no	x	x	no
Reason	opportunities	yes	x	x	x
Referred By	opportunities	no	x	x	no
Total	opportunities	no	no	x	no
Weighted Total	opportunities	no	no	x	no



About Swiftpage

Swiftpage is committed to empowering individuals, small business and mobile sales teams to better manage their business interactions, more intelligently engage their customers, and convert more interactions into transactions. The company's growing network of partners, customers, end-users and employees collectively represent the Swiftpage Nation, united across the globe as one team, on one journey. Learn more at www.swiftpage.com and join the conversation at social.swiftpage.com.

© 2013 Swiftpage ACT! LLC. All Rights Reserved. Swiftpage, Act!, Saleslogix, and the Swiftpage product and service names mentioned herein are registered trademarks or trademarks of Swiftpage ACT! LLC, or its affiliated entities. All other trademarks are property of their respective owners.