Sage ACT! | White Paper

# Security Model

Sage ACT! maximizes flexibility and provides options for securing data

## Table of Contents

## Introduction

The Sage ACT! security model is designed to maximize flexibility and provide a variety of options for securing data. Managers and Administrators (in larger organizations the Administrator may work in the IT organization) can leverage Sage ACT! security features to limit access to the database, records within the database, and fields related to those records. The entire Sage ACT! product family uses the same Sage ACT! security model, ensuring consistent data protection without regard to the Sage ACT! application being used.

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

*The Sage ACT! security model supports both stand-alone and workgroup implementations.*

## Sage ACT! Security Overview

The Sage ACT! security model supports both stand-alone and workgroup implementations. Security in Sage ACT! can be scaled to suit your environment, whether you work alone, with a small team, or with a large workgroup[1]. 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 Sage ACT! are:

- **Administrator** – Administrator is the highest level role in Sage ACT!. Users with this role can access all features in Sage ACT!, and all records that have public or limited access. Only private data owned by other users is inaccessible to the administrator. (For more information about record access, see Lookup Contact by Access on page 19). The administrator is the only role allowed to *Manage Users, Delete database*, and set the *Password Policy*. Users who are responsible for maintaining the database and who need to access most features and data, should be administrators.

- **Manager** – Managers have access to all features except *Manage Users, Delete database*, and *Password Policy*. The manager role can be tailored for individual needs by granting or withholding four custom 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 tailored for individual needs by granting or withholding six custom 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 or edit groups or companies. Restricted users can run reports and write letters using existing templates, but they cannot modify letter or report templates. Restricted users can only

[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. Sage scalability recommendations are based on in-house performance testes using the recommended server system requirements found at: www.act.com/2011systreq to ensure your system meets these requirements. You must purchase one license of Sage ACT! per user.

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, hourly workers, or others requiring only limited access to features in Sage ACT!.

- **Browse** – The browse role gives users read-only access to information in the Sage ACT! database. Browse users can perform lookups, run reports, and print information, but cannot create or modify any data in the Sage ACT! database. Temporary employees and users who only need to reference information should be browse users.

**Make sure users can access all the records they need for reports that they are responsible for producing.**

User Tip

NOTE: The term “user” or “users” in this document refers to any Sage ACT! user regardless of role.

### Types of Security in Sage ACT!

- **Database Security** – Controls who can use a database. Individuals access a Sage ACT! database using a unique user name. The Sage ACT! database administrator also can implement a password policy to further restrict database access.

- **Feature Security** – Controls who can use specific features. Each Sage ACT! database user is assigned a role. Each role dictates which features (permissions) a user can access in the application. 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 in Sage ACT! has an owner known as a “record manager.” When a record is marked “*private*,” only the record manager can view it. Sage ACT! users can access all *public* data, their *private* data, and any *limited access* records they have specifically been granted access to. 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) in order to access any *extended data* (notes, history, activities, or secondary contacts) belonging to that parent record.

- **Field-Level Security** – Controls who can see and modify fields and what fields they can view and modify. Users who are assigned *administrator* or *manager* roles in ACT 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 Sage ACT! functionality.

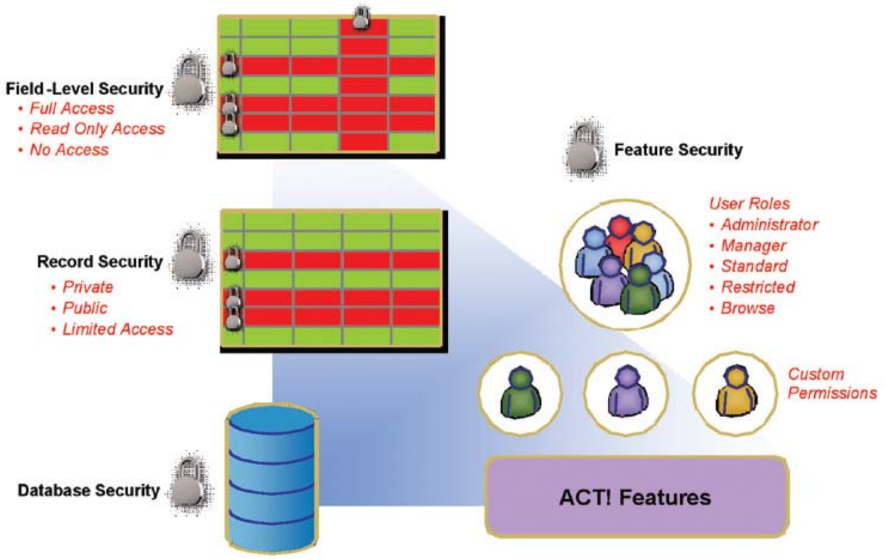


*Figure1 : This figure illustrates the types of security that make up the security model in Sage ACT!.*

## Database Security

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

***Access to a Sage 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 selects to open a Sage ACT! database, the Log On dialog box appears. The user must enter a valid user name to access the database. If the Sage ACT! database *administrator* has implemented a password policy, the user will also need to enter a valid password.

### Database Users

Each person who can access a Sage 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 Sage ACT! database can use that user name. Each user has a contact record (user record) which represents the user in the database. This user record is referred to as “My Record.”

Any user with permission to edit the contact can change the name on the contact 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 if a user is on vacation or medical leave.

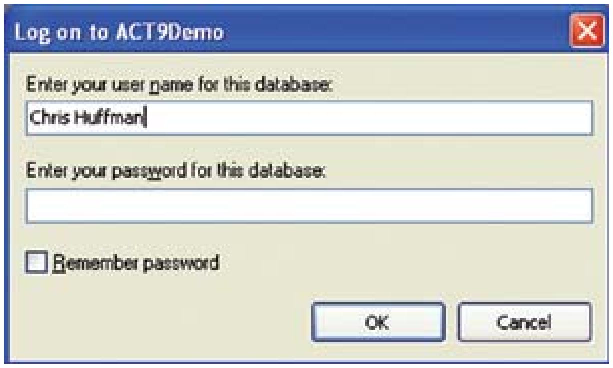
### Log-on Functionality

**General**

- Sage ACT! remembers the last user name used to open a Sage 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 Sage ACT! remembers both the user name and password, and populates both fields in the Log On dialog box when opening that database. Sage 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, Sage ACT! only remembers the last user name, as described in the first bullet above.



Log on to ACT9Demo

Enter your user name for this database:
Chris Huffman

Enter your password for this database:

☐ Remember password

***Figure 2 :  This screen shot shows how users must log on to the ACT! database.***

**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 above.

**Multi-User Databases**

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

- The Log On dialog box always appears.
- *Remember password* functionality applies as described above.

**External Applications**

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

**Passwords**

The Sage ACT! Administrator can decide whether passwords are optional or mandatory for database users. Sage ACT! database *Password Policy* governs password use. The database administrator also can establish individual user settings. Sage ACT! encrypts all passwords.

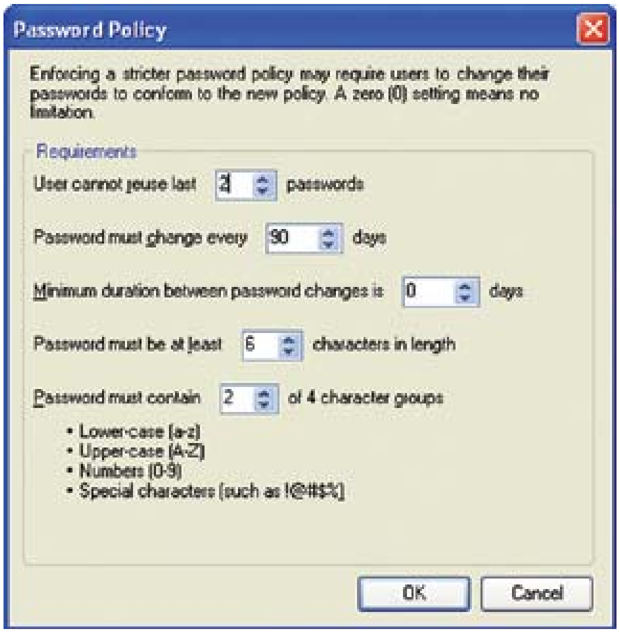
**Password Policy**

The Password Policy dictates the parameters of password use for all users of the database. The Sage ACT! administrator determines the Password Policy. This functionality provides an additional level of protection for the Sage ACT! database. By default, no password is required and no password parameters are defined. The Sage ACT! administrator can permit individuals to choose whether or not they use a password, or set any combination of the five optional password settings. The administrator sets password parameters by selecting *Password Policy* on the Tools menu. When a password policy has been defined, it applies to all users of the database.

***When a password policy has been defined, it applies to all users of the database.***

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 duration length of time a password can be used.
- **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 incorporate.
    - Lower-case (a-z)
    - Upper-case (A-Z)
    - Numeric (0-9)
    - Special Characters (printable Extended ASCII set)



Password Policy

Enforcing a stricter password policy may require users to change their passwords to conform to the new policy. A zero (0) setting means no limitation.

Requirements

User cannot reuse last 2 passwords

Password must change every 90 days

Minimum duration between password changes is 0 days

Password must be at least 6 characters in length

Password must contain 2 of 4 character groups

- Lower-case (a-z)
- Upper-case (A-Z)
- Numbers (0-9)
- Special characters (such as !@#$%)

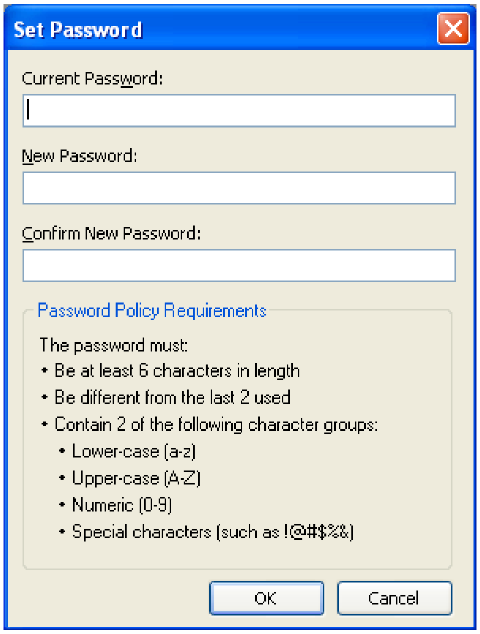
***Figure 3:  This screen shot shows how the ACT! administrator can* dictate the parameters of password use for all users of the database*.***

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 they log on to the database.

**User Tip**

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



Current Password:

New Password:

Confirm New Password:

Password Policy Requirements

The password must:

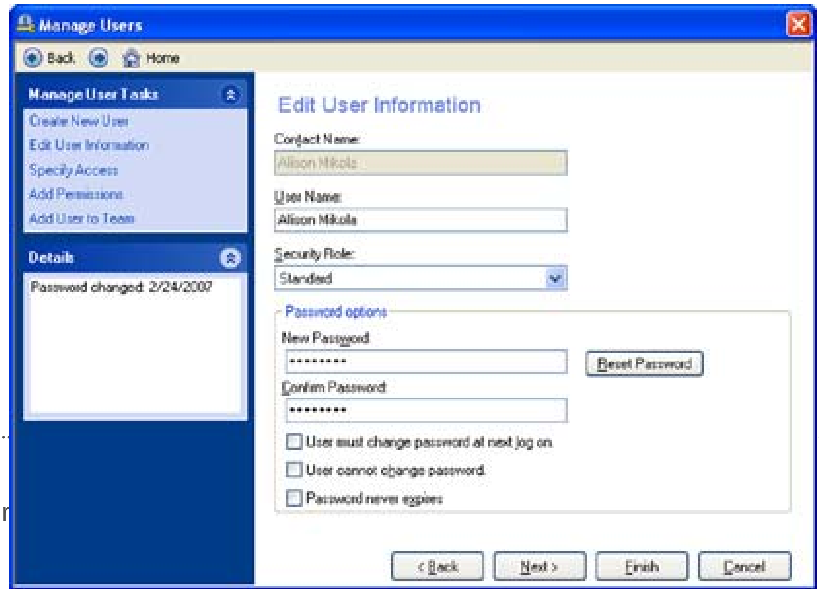
- Be at least 6 characters in length
- Be different from the last 2 used
- Contain 2 of the following character groups:
  - Lower-case (a-z)
  - Upper-case (A-Z)
  - Numeric (0-9)
  - Special characters (such as !@#$%&)

*Figure 4:  The Set Password dialog box appears when a user is required to change her password.*

**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; or
- Specify that a user's password never expires.



Password changed: 2/24/2007

Edit User Information

Contact Name: Allison Mikola

User Name: Allison Mikula

Security Role: Standard

Password options

New Password: ********

Confirm Password: ********

□ User must change password at next log on

□ User cannot change password

□ Password never expires

*Each Sage ACT! database user is assigned one of 5 roles in the database, and each role has different access to features within the application.*

***Figure 5:  The Manage Users screen defines password settings.***

User Tip

**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.**

An administrator can modify user settings by choosing *User Management* from the Tools menu and clicking *Edit User Information*.

**User Reset of Password**

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

- The database Password Policy has changed,
- An administrator has indicated that a user must change her password.
- A user's password has expired.
- Users will be required to change their passwords.

A user can, alternatively, 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 Sage ACT! database 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 the 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 permissions.

The table below lists the major permissions in Sage ACT! and which permission is assigned to each of the five roles. Default permissions are inherent to the role. Custom permissions also can be granted to Managers and Standard users. Please refer to Help for detailed descriptions of features in Sage ACT!.

| Permission | Administrator | Manager | Standard | Restricted | Browse |
|---|---|---|---|---|---|
| **All Records** | | | | | |

| Permission | Administrator | Manager | Standard | Restricted | Browse |
|---|---|---|---|---|---|
| **Manage Other User's 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 | Default Custom Permission | | |
| **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[3]. | 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**[4] – User can schedule activity series. | X | X | X | X | |

[2] In Sage ACT! Premium (access via web), administrative functions must be performed on the web server.

[3] In Sage ACT! Premium (access via web), administrative functions must be performed on the web server.

[4] In ACT Sage ACT! Premium (access via web), administrative functions must be performed on the web server.

| Permission | Administrator | Manager | Standard | Restricted | Browse |
|---|---|---|---|---|---|
| **Manage Activity Series** – User can create and edit activity series. | X | X | X | | |
| **Manage Other Users' Activity Series** – User can edit activity series that other users own. | X | X | | | |
| **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 Users' 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 Sage ACT! contacts in vCard format to non-Sage ACT! users. | X | X | | | |
| **Companies** | | | | | |
| **Manage Companies** - User can create and edit companies. | X | X | X | | |
| **Manage Other User's Companies** – User can change Record Manager and/or modify access to other users' Companies. | X | X | | | |
| **Delete Companies** – User can delete Companies which he owns. | X | X | Default Custom Permission | | |
| **Delete Other Users' Companies** – User can delete Companies owned by other users. | X | X | | | |
| **Communications** | | | | | |
| **Manage E-mail** - User can enable e-mail for use with Sage ACT! and can transfer/restore the e-mail 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 Sage 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 | |

| **Customization**[5] | | | | | |
|---|---|---|---|---|---|
| **Manage Layouts (Layout Editor)** – User can create and edit layout templates. | X | X | | | |
| **Customize Menus**[6]**/Toolbars** – User can modify menus and toolbars. NOTE: Menu/toolbar customizations apply only to the local copy of Sage ACT! The global toolbar cannot be customized at this time. The view is specific to a Sage ACT! view and can be customized. | 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 E-mail** – User can attach a contact, company, or group to an e-mail and can import such records received as an e-mail attachment. | X | X | X | | |
| **Export to Microsoft Excel®** – User can export data from designated list views to Excel. | X | X | Default Custom Permission | | |

[5] In Sage ACT! Premium (access via web), administrative functions must be performed on the Web server.

[6] This feature is not available when using web access.

| Database Management[7] | | | | | |
|---|---|---|---|---|---|
| **Back up Database** – User can back up the database (does not include backing up personal files). | X | X | | | |
| **Back up Attachments** – User can back up files attached to the database (does not include backing up personal files). | 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 database password policy. | X | | | | |
| **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 | Available Custom Permission | Available Custom Permission | | |

[7] In Sage ACT! Premium (access via web), administrative functions must be performed on the web server.

| | | | | | |
|---|---|---|---|---|---|
| **Restore Database** - User can restore a database back-up file. | X | | | | |
| **Scan for Duplicates** – User can scan the database for duplicate records. | X | X | X | X | X |
| **Share Database** – User can prepare 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 installation of Sage ACT!. | X | X | X | X | X |
| **Perform Lookups** - User can perform lookups and advanced queries on data in Sage ACT!. | X | X | X | X | X |
| **Printing** - User can print Sage ACT! address books, calendars, e-mail, envelopes, labels, lists, reports, and documents. | X | X | X | X | X |
| **Run Sage ACT! Update** - User can update the Sage ACT! application (does not include database upgrade). | Not governed by security or permissions | | | | |
| **Upgrade Database** - User can upgrade the database to work with a newer version of Sage ACT!. | X | X | Default Permission granted to “Lone Standard User” | | |
| **Groups** | | | | | |
| **Manage Groups** – User can create and edit groups | X | X | X | | |
| **Manage Other Users' Groups** – User can change 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 Users' Opportunities** – User can change 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 | | | |
| **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 | | |

| **Smart Tasks** | | | | | |
|---|---|---|---|---|---|
| **Smart Tasks** – User can schedule smart tasks. | X | X | X | X | |
| **Manage Smart Tasks** – User can create and edit smart tasks. | X | X | X | | |
| **Manage Other Users' Smart Tasks** – User can edit smart tasks that other users own. | X | X | | | |
| **Delete Smart Tasks** - User can delete smart tasks that he owns. | X | X | Default Custom Permission | | |
| **Delete Other Users' Smart Tasks** - User can delete smart tasks that other users own. | X | X | | | |
| **Synchronization, Database** [8] | | | | | |
| **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 database 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 | | |

[8] In Sage ACT! Premium (access via web), administrative functions must be performed on the Web server.

| **Synchronization, Other** | | | | | |
|---|---|---|---|---|---|
| **Accounting Link Tasks** - User can set up and perform accounting link synchronization. | X | Default Custom Permission | Available Custom Permission | | |
| **Handheld Device Sync**[9] - User can set up and perform handheld device synchronization. | X | Default Custom Permission | Available Custom Permission | | |
| **Outlook Activity Sync**[10] - User can update the Sage ACT! calendar with activities from Microsoft Outlook. | X | X | X | X | |
| **Outlook Contact Sync** - User can set up and perform contact synchronization with 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 Sage ACT! Premium are:

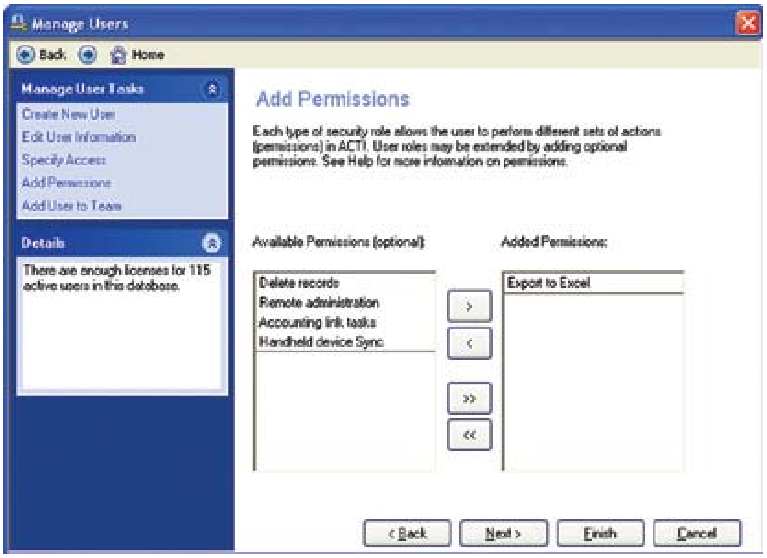
- **Accounting link tasks** - Ability to perform Accounting Link tasks.
- **Delete records** – A user's ability to delete Contacts, Companies, Groups, Opportunities, Notes, and Histories which he owns (is the record manager for).
- **Export to Excel** - Ability to export list view data to Microsoft Excel.
- **Handheld device sync**[11] – Ability to set up and perform handheld device synchronization.
- **Remote administration** – Ability of a non-administrator in a remote database to perform database maintenance, back up a database, and restore a database back-up 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.

***A custom permission is an optional permission which can be granted to, or restricted from, an individual who has a manager of standard role.***

[9] This feature is not available when using web access.

[10] This feature is not available when using web access.

[11] This feature is not available when using web access.



Add Permissions

Each type of security role allows the users to perform different sets of actions (permissions) in ACT!. User roles may be extended by adding optional permissions. See Help for more information on permissions.

There are enough licenses for 115 active users in this database.

Available Permissions (optional):

- Delete records
- Remote administration
- Accounting link tasks
- Handheld device Sync

Added Permissions:

- Export to Excel

*Figure 6: Custom permissions are assigned by selecting Manage Users from the Tools menu, and chossing to Edit User Information for a selected user. Onlyadministrators can Manage Users.*

**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*[12] (granted by default, but can be removed)
  - *Manage Subscription List* (granted by default to managers of a synchronizing database, but can be removed)
  - *Remote Administration* (available to mangers 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*[13] (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[14] | 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.

***Record security in Sage ACT! is determined by ownership, by role, and by the Access Control List (ACL).***

[12] This feature is not available when using web access.

[13] This feature is not available when using web access.

[14] This feature is not available when using web access.

**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[15] | 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 Sage ACT! is determined by ownership, by role, and by the *Access Control List* (ACL). The ACL lists users and/or teams who can access a record. A team is a collection of users; administrators can assign user access to individual contacts, companies, groups, or opportunities using the ACL.

Each record in Sage ACT! has an owner known as a “Record Manager.” A Record Manager can change the ownership and modify the ACL 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 ACL of any records they can access. Standard and Restricted users can modify the ownership and ACL of only those records they own. The Record Manager (owner) is always included in the ACL 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 find it using lookups, include it in reports, print its information, or include it in mail merges. Inaccessible records do not appear in any views or lists.

The three access types in Sage ACT! 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 below in the “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 record[16] by designated users and/or teams. Record managers can always access contacts they own. All users with administrator roles also can access all limited access records by default.

[15] This feature is not available when using web access.

[16] Only certain fields can be designated as read-only or no access. Limited access is only available to Sage ACT! Premium users only.

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.

**User Tip**

**Users can modify Record Creation Preferences to set the default ACL 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) Parent and extended data records are explained in the following sections.

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 Sage ACT! and can own extended data. “Extended data” refers to record types which cannot exist independently, such as Notes, Histories, Activities, and Secondary Contacts. Extended data always belongs to one or more parent records (Contacts, Companies, Groups, or Opportunities).

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 ACL 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.

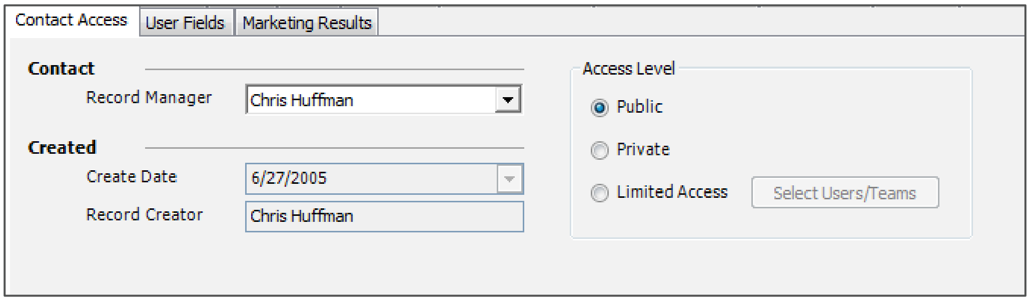
> **Example:** User A has access to a contact, Joe Smith, but cannot access a private note owned by User B (record manager) for Joe Smith.

### Tools for Managing Record Security

A variety of tools are available for managing record security.

#### Access Controls

The *Access Control* appears on default layouts for Contacts, Companies, Groups, and Opportunities. This control is found on the Contact Info, Company Info, Group Info, Opportunity Info tabs, and lets the user change access to the current record.



**Contact**

Record Manager: Chris Huffman

**Created**

Create Date: 6/27/2005

Record Creator: Chris Huffman

Access Level

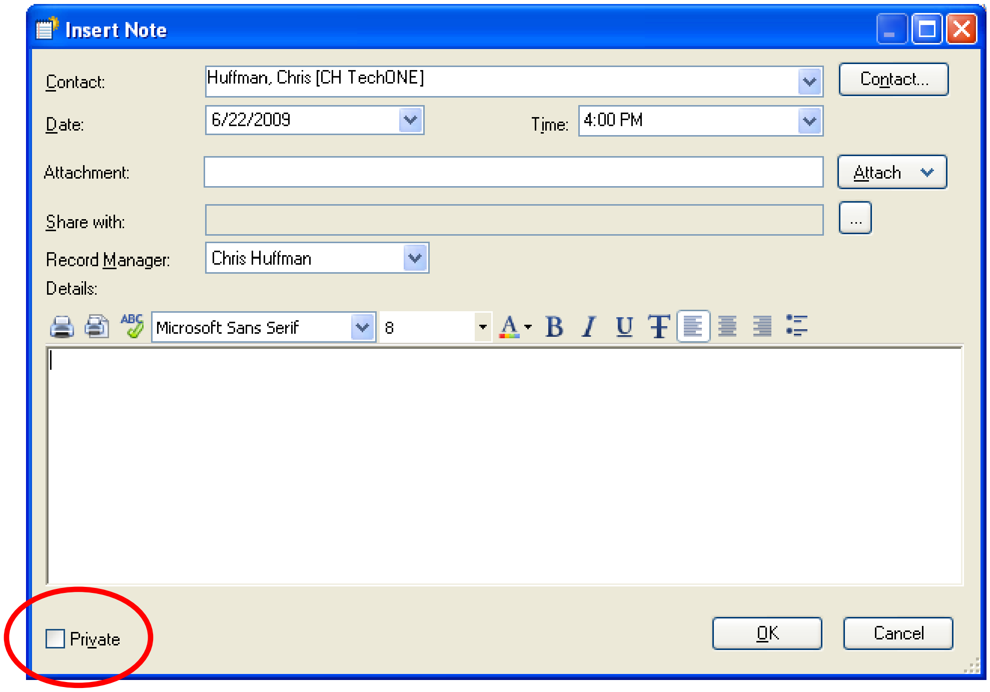
● Public

○ Private

○ Limited Access

*Figure 7: The access control lets users change access to the current record.*

Users set access to extended data by selecting or clearing the private checkbox found in the lower left corner of the create/edit dialog boxes for each extended data type (Activities, Notes, History, and Secondary Contacts).



Contact: Huffman, Chris [CH TechONE]

Date: 6/22/2009

Time: 4:00 PM

Attachment:

Share with:

Record Manager: Chris Huffman

Details:

Microsoft Sans Serif 8

□ Private

*Figure 8: Users can select or clear the private checkbox to set access to extended data.*

#### Edit Contact or Opportunity Access

Users with the proper access role can change the access of contacts or opportunities en masse, by selecting one of five bulk update functions from the *Contacts> Edit Contact Access* menu when the

***All users can access all user records in a database. Extended data on user records can be secured.***

*All users can access all user records in a database. Extended data on user records*

Contact List is displayed, or from the *Opportunities> Edit Opportunity Access* menu when the Opportunities List is displayed. The commands operate on the selected contacts or opportunities in the list.

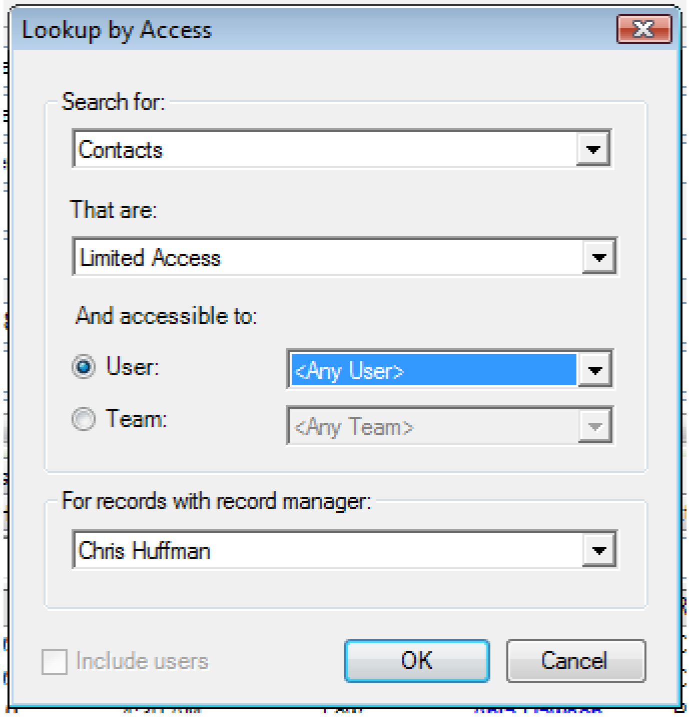
The available functions include:

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

To change contact (or opportunity) access, the user must be an administrator, manager, or the record manager of the selected Contact (or Opportunity).

### 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> Advanced> Contact by Access (or Opportunity by Access).



Lookup by Access

Search for: Contacts

That are: Limited Access

And accessible to:

● User: <Any User>

○ Team: <Any Team>

For records with record manager: Chris Huffman

□ Include users

*Figure 9: This screenshot shows how users can find contact or opportunity records using criteria related to access.*

The following examples* are different types of lookups relating to record access:

- Look up limited access Contacts, owned by Chris Huffman (record manager), which are accessible to Allison Mikola.

- Lookup all of my private Contacts.
- Lookup public Contacts owned by Allison Mikola (record manager).
- Lookup all Contacts owned by Allison Mikola.

**All lookups are limited to those contacts that can be accessed by the user performing the lookup.*

## Field-Level Security

Administrators and managers can secure fields through the 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 access[17]” 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 Sage ACT! functionality (see Appendix A).

***Administrators and managers can secure fields through the Define Fields functionality. Users can be given “full access,” “read only access,” or “no access” on a user-by-user basis.***

**User Tip**

**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[17] to a particular field to prevent himself from making any inadvertent changes to that field.**

FLS uses three levels of access:

- **Full Access** – User can view and modify data in the field.
- **Read Only Access**[18] – User can view data in the field, but not modify it.
- **No Access**[19] – 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 in Sage ACT!, such as Edit Date and Create Date, are permanently designated as read-only.

If a user has “no access” to a particular field, it is 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.

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

- **Default permission** – The base access level to 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 user 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.

Team and User Permissions are available only in Sage ACT! Premium. Also, fields can be set to “no access” only in Sage ACT! Premium[20].

[17] Only certain fields can be designated as read-only or no access.

[18] Only certain fields can be designated as read-only or no access.

[19] Only certain fields can be designated as read-only or no access.

[20] Only certain fields can be designated as read-only or no access.

# Features Affected by Sage ACT! Security

This section provides insight on the effects of security on features in Sage ACT!.

## Differences Between Sage ACT! Pro and Sage ACT! Premium

This document is based on functionality available in Sage ACT! Premium, which is targeted for individuals[21] and smaller workgroups and has some differences in features related to security. The major differences between Sage ACT! Pro and Sage ACT! Premium are listed below.

### Custom Permissions

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

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

### Record Security

The "Teams" and "limited access" ACL features are available only in Sage ACT! Premium.

### Field-Level Security

Only the Default Permission setting for FLS[22] is available in Sage ACT! Pro In addition, fields cannot be set to "no access" in Sage ACT! Pro User and Team permissions are available only in Sage ACT! Premium (see above).

## Attachments

By default, users are allowed to attach files and e-mail messages to the Sage ACT! database. Administrators can choose to limit this ability through the use of the Attachments settings in the Preferences, Admin tab.

Only Administrators can include attachments when backing up the database.

## Calendars

While users cannot open activities they do not  have access to, the existence of those activities does impact Sage 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 and the date and time of the activity.

[21] You must purchase one license of Sage ACT! per user.

[22] Only certain fields can be designated as read-only or no access

.

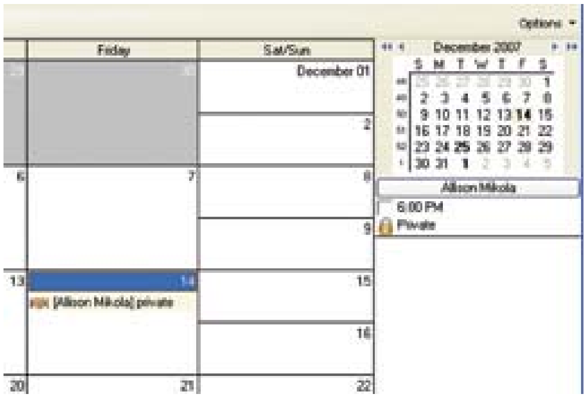


*Figure 10: Users can view the existence of activities but may not be able to access detailed information.*

Activities displayed in this fashion 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 FLS). Only administrators and managers can import or export Sage ACT! data. Standard users can export lists to Microsoft Excel and can import Sage ACT! contact records received via e-mail (see Permissions).

***Data import and export adheres to all four types of security.***

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.

**User Tip**

**Administrators have the greatest access to all records. Only private records owned by other users (and related extended data) are not accessible during the import/export process.**

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[23].

**User Tip**

**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.**

[23] Only certain fields can be designated as read-only or no access.

## 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 in the ACT2010Demo database. 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 in the ACT10Demo database. 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

Sage 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 by an administrator *(Tools> Database Maintenance> Share Database)*, this access is handled by Sage 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 above 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 record access levels available in Sage ACT!—public, private, or limited access[24]. 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

***Both Companies and Groups can be assigned any of the three record access levels – public, private or limited access.***

information related to the Company or Group only if the user performing 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 the 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.

### 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[25] 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 via Tools>Preferences>Startup tab>Company Preferences. This preference applies to associated activities and opportunities for linked records.

24 Only certain fields can be designated as read-only or no access. Limited access is only available to Sage ACT! Premium users only.

.

**User Tip**

**If the parent records (Contacts, Companies, Groups, or Opportunities) have different ACLs, 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 Sage ACT! security model applies to and affects external applications which access the Sage ACT! database and data within it. Security for Sage ACT! data is enforced for these applications just as it is in Sage ACT!. This includes Sage ACT! Network Sync Service, Sage ACT! Internet Sync Service, Sage ACT! Scheduler, Sage ACT! SDK (Software Developer's Kit), Sage ACT! Premium, Sage ACT! Link for Palm OS, and Sage ACT! Link for PocketPC.

### Synchronization

Sage ACT! database 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 set up of synchronization.

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.

### Handheld Devices

Synchronization to handheld devices using ACT! Mobile Live transfers only data that the user can access. Security is enforced during synchronization.

## Conclusion

The Sage ACT! security model supports both stand-alone and workgroup implementations. Security in Sage ACT! can be scaled to suit your environment, whether you work alone, with a small team, or with a large workgroup. Security can be enforced at the database level, the feature level, the record level, and the field level. Administrators have the greatest access to all records and can set parameters and permission levels for users. These layers of security affect a number of features in Sage ACT! by allowing only users with the right permissions to view information in the database.

[25] Only certain fields can be designated as read-only or no access.

.

## Glossary of Terms

**Access** – The ability to view a record. Users who can access a particular record can view it. Accessible records can be searched, reported upon, and appear in related views and lists. A user must have access to a record to modify it in any way, however, the ability to modify or delete the record is conveyed in separate permissions.

Contacts, Companies, Groups, and Opportunities can be private, public, or limited access. Extended data can only be private or public access. A user must have access to the parent (Contact, Company, Group, or Opportunity) record in order to access an extended data record belonging to that parent record (see Cascading Access).

**ACL** – Access Control List. The list of users and/or teams who can access a contact. The record manager (owner) of a contact is always on the ACL. ACLs are used to control who has access to particular records. Record managers, managers, and administrators can modify contact ACLs.
The ACL of a *public* contact is "all users," and the ACL of a *private* contact is limited to the record manager (owner) of the contact. A contact with *limited* access can be accessed by the record manager of the contact, users with the administrator role in the database, and any other users or teams listed in the ACL.

**Calendar delegate** – A user granted the ability to schedule activities for another user. Any administrator, manager, standard, or restricted user can grant delegate authority to another user. Browse users cannot be a calendar delegate for another user. Administrators and managers always have the ability to schedule activities for other users.

**Cascading access** – Accessibility to extended data records (Notes, Histories, Activities, and Secondary Contacts) is limited to users with access to the parent record.

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

Cascading access does not grant a user more access to an extended data record than the user has for the extended data record.

> **Example:** A user who can access a contact cannot access a private note for that contact, if the note is owned by a different user (record manager).

**Core Field** – A field required by Sage ACT!. Users cannot delete core fields, and some core fields cannot be secured because they are integral to basic Sage ACT! functionality. Contact name field is an example of a core field.

**Credentials** – The user name and password combination required for a user to log on to a Sage ACT! database.

**Custom permission** – An optional permission which can be granted to, or restricted from, an individual user. Administrators irrevocably have all permissions in the database. Administrators can give custom permissions to users with manager and standard roles. Restricted and browse users cannot be granted any custom permissions.

Available custom permissions:

- **Accounting link tasks** - Ability to perform Accounting Link tasks.
- **Delete records** – Ability to delete records the user is the record manager of.
- **Export to Excel** - Ability to export list view data to Microsoft Excel.
- **Handheld device sync**[27] – Ability to set up (externally) and perform handheld device sync.
- **Remote administration** – Ability to back up, restore, and perform database maintenance of a remote database in a synchronizing environment.
- **Manage subscription list** – Ability to modify the database synchronization subscription list.

**Database Logon Credentials** – The combination of user name and password required to gain access to a Sage ACT! database.

**Extended data** – Record types which cannot exist independently. Such records include Notes, Histories, Activities, and Secondary Contacts. Extended data belongs to one or more parent records (Contact, Company, Group or Opportunity).

Notes and Histories can belong to Contacts, Companies, Groups, Opportunities and/or any combination of those records. Activities, and Secondary Contacts can belong to one or more contacts.

**Field-level security (FLS)** – The ability to control access to data by the user (and/or by team) on a field-by-field basis. Access to field data can be set by user or team.

FLS has three levels of access:

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

Field access can be controlled through the use of one or more types of permissions:

- *Default permission* – The base access level to 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, who can also have team or user permissions.
- *Team permission* – Access granted to user 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*.

The *No Access* level of field security is only available in Sage ACT! Premium.

**Limited access** – A security level which allows access to a Contact, Company, Group, or Opportunity record by designated users and/or teams. Record managers always have access to Contacts which they own. All users having administrator roles also have access to all limited access Contacts by default. The limited access security level is available only in Sage ACT! Premium.

**Lone Standard User** – A user who is assigned the standard role in a remote database, where no

[27] This feature is not available when using web access.

administrators are present in the “who list” of users. The “who list” defines the users who are the intended users of a remote database. Users must be on the “who list” to log on to the remote database. In this scenario, the “lone standard user” can upgrade the database, a permission not normally granted to standard users.

**Parent record** – A Contact, Company, Group, or Opportunity record. These top-level record types can exist independently of any other record type in Sage ACT! and can own extended data (Notes, Histories, etc).

**Password** – A password is a string of characters used to give a user access to a Sage ACT! database. When a user has an established password, he must provide both his user name and password each time he opens or accesses a Sage ACT! database. Password requirements in a Sage ACT! database are configurable by administrators through use of the database Password Policy.

**Password Policy** – The Password Policy of a database defines password requirements for the Sage ACT! database. By modifying the Password Policy, an administrator can control password re-use, force users to change their password after a certain number of days, set a minimum duration between password changes, and/or define password parameters such as length and types of characters that must be included in a valid password. The Password Policy function is available on the Tools menu.

Administrators can also require a user to change their password on next log-on, specify that a user cannot change her password, or specify that a particular user’s password never expire. These additional functions are available by selecting *Manage Users* in the Tools menu.

**Permission** – The ability of a user or role to perform a specific action. Most actions and functions in Sage ACT! have permissions associated with them. The ability to perform these functions is managed by granting or limiting permissions through role assignment and through the use of custom permissions.

> **Example:** A user can have access to a contact (can view it), but not be able to modify the contact.

**Private access** – A security level which restricts access to a record to the record manager of that Contact. Contacts, Companies, Groups, Opportunities, and all extended data record types can be marked as private.

**Public access** – A security level which allows access to a record by all users in the database. Contacts, Companies, Groups, Opportunities, and all extended data record types can be public access. All user records (Contacts) are public.

**Record creator** – The user who created the record. All record types have a record creator. The record creator is the record manager by default.

**Record manager** – The user of the database who “owns” and controls the record. All top-level entities (Contacts, Companies, Groups, and Opportunities) and extended data records have record managers. The record manager can manage access to records they own and always has access to those records. By default, the record manager is the record creator. When a record is marked *private*, only the record manager can view it.
Record managers have greater permissions to act upon their own records.

**Example:** By default, a standard user can delete records he is the record manage of, but cannot delete records belonging to other users.

**Remote database** – A “subscribing” database in a synchronization scenario. A remote database can synchronize only with its main (publisher) database. A main database can synchronize with many remote databases, but a remote database has only one main database “parent.”

**Role** – A role is made up of one or more permissions. Every user in Sage ACT! is assigned one of the five available pre-defined roles. Within each role, an administrator can grant or remove custom permissions on a user-by-user basis.

- **Administrator** – the highest level role in Sage ACT!. The administrator can perform any function in the application. Administrators can access all records except private records belonging to other users.
- **Manager** – the second highest level role in Sage ACT!. Managers can perform most functions in the application, but not certain high-level database functions such as Manage Users, Delete Database, and Password Policy. Managers can access all records except private records belonging to other users.
- **Standard** – the average role in Sage ACT!. Standard users can perform most day-to-day functions in the application, but not high-level database functions. Standard users can only modify access of those records they are the record manager (owner) of.
- **Restricted** – the second lowest level role in Sage ACT!. A restricted user can perform many common functions in the application, but cannot delete records, create/edit report and letter templates, or perform database synchronization.
- **Browse** – the lowest level role in Sage ACT!. Browse users can view records, perform lookups, reports, and perform other tasks that do not involve modification of the database.

**System Field** – A field required by Sage ACT! which cannot be directly modified or deleted by a user. Users cannot modify security on these. These fields typically have “read-only” access since they are integral to basic Sage ACT! functionality. Edit Date is an example of a system field.

**Team** – A Team is a collection of users. Teams can be used to assign user access to individual contact records through use of the *Access Control List*, and can also be used to assign access to fields through *field-level security*. Teams cannot access private records, and Teams cannot own records.

**Users** – Users can log on to a Sage ACT! database. Each user has a user name which allows access to the database. Only active users of a database can log on.

**User name** – User name is a unique identifier associated with a user having access to a Sage ACT! database. Only one user can have a particular user name. Any user who has permission to edit the record can change the name on the contact record, but only an administrator can change the name of the user associated with that record.

**User records** – A user record is a contact record associated with a particular user name. All users of the database have their own user record (My Record), and all user records in a database are accessible to all other users.

## Appendix A – Default Fields in Sage ACT!

The following table lists all the default fields in a new Sage ACT! database. The table also shows which FLS access level can be assigned to each field. Some core fields and system fields cannot be secured because they are integral to basic Sage 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 |
| 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 |

| Field Name | Type | May be Deleted? | Full Access | Read Only | No Access |
|---|---|---|---|---|---|
| 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 |
| 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 |

| Field Name | Type | May be Deleted? | Full Access | Read Only | No Access |
|---|---|---|---|---|---|
| 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 |
| 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 |

| Field Name | Type | May be Deleted? | Full Access | Read Only | No Access |
|---|---|---|---|---|---|
| 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 |

### ASIA

210 Middle Road
#06-04
IOI Plaza
Singapore 188994
+65 6336 6118
www.sageasiapac.com

### AUSTRALIA / NEW ZEALAND

Level 6, 67 Albert Street
Chatswood, NSW 2067
Australia
+61 2 9921 6500
www.sagebusiness.com.au
www.sagebusiness.co.nz

### BELGIUM / LUXEMBOURG

Rue Natalis 2
4020 Liège
Belgium
+32 4 343 77 46
www.sage.be

### CHINA

Suite 2605,
Liu Lin Tower No. 1
Huaihai Zhong Road
Shanghai 200021
People's Republic of China
+ 86 21 63850097
www.sagesoft.cn

### FRANCE

Ciel – Service Commercial ACT!
35, rue de la Gare
75917 Paris cedex 19
France
+33 1 55 26 34 77
www.MonAct.fr

### GERMANY

Emil-von-Behring Str. 8-14
60439 Frankfurt am Main
Germany
+49 69 50007 6260
www.sage.de

### INDIA

100, Second Floor
Okhla Industrial Estate Phase-III
New Delhi 110020
India
+91 11 4071 2488
www.sagesoftware.co.in

### IRELAND

3096 Lake Park Drive
Citywest Business Park
Dublin 24
Ireland
+353 (0) 1 642 0800
www.sage.ie

### MIDDLE EAST

Office No. 315, Building 12
P O Box 500198
Dubai Internet City
Dubai
United Arab Emirates
+971 (4) 3900180
www.me.sage.com

### POLAND

Sage sp. z o.o.
Ul. Berna 89
01-233 Warszawa
Poland
+48224555600
www.actsage.pl

### SOUTH AFRICA

Softline Technology Park
102 Western Services Road
Gallo Manor Ext 6
Johannesburg, 2191
South Africa
+2711 304 3000
www.pastel.co.za

### SPAIN

Labastida, 10-12
28034 Madrid
España
+34 91 334 92 92
www.sagecrm.es

### SWITZERLAND

Sage Schweiz AG
D4 Platz 10
6039 Root Langenbold
Switzerland
+41 58 944 19 19
www.sageschweiz.ch

### UNITED KINGDOM

North Park
Newcastle Upon Tyne
NE13 9AA
0800 44 77 77
www.sage.co.uk/act

### UNITED STATES

8800 North Gainey Center Drive
Suite 200
Scottsdale, Arizona 85258
1 866 903 0006
www.act.com

**About Sage ACT!**
Sage ACT! makes it easy for you to have meaningful conversations with customers by giving you an organized view of the people you do business with. Like the millions of small businesses and sales teams who use Sage ACT!, you'll always be prepared with recent emails, meeting notes, task reminders, and social media profiles, because all of these details live in one place.

**Important Note:** Review Sage ACT! system requirements at www.act.com/2011systreq. You must purchase one license of Sage ACT! per user. Scalability varies based on hardware, size, and usage of your database. **Compatibility:** Visit www.actsolutions.com or contact your add-on product provider to help determine compatibility.

**Sage**
8800 N. Gainey Center Dr., Suite 200
Scottsdale, AZ 85258
www.act.com | 866-903-0006

Sage ACT!