PROFESSIONAL COMPUTER MANAGEMENT INC.

April 2009 • Volume 6 • Issue 2

info

NEWSLETTER for ACT! by Sage

Securing Your Customer Information

Information about your customers is one of your business's biggest assets—securing that information is one of the highest priorities of successful companies. You have worked too hard to build your customer base to risk losing it to your competition or perhaps to a disgruntled employee. ACT! by Sage provides a powerful multifaceted security model that can be scaled to suit your business environment. In this article, we will discuss the various security options available within ACT! by Sage and how you can use them to tailor your security setup to meet the needs of your company. Note: functionality may vary among the ACT! by Sage product family, in this article we will discuss the features of ACT! by Sage Premium 2009.

User Roles And Permissions

There are five user roles within ACT! that you can use to control broad functionality. Each ACT! database user is assigned one of five roles in the database. Briefly here is what each role allows the user to do:

- Administrator: Allows access to all available functionality.
- Manager: Allows access to all features except Manage Users, Delete Database, and Password Policy.
- Standard: Users with this role can access most areas of the application, create and 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. Users who perform a variety of tasks, including creating and modifying word-processing and report templates, but who do not need to modify or maintain the database, should be assigned the Standard user role.
- Restricted: Allows access to only basic functionality. A Restricted user can create and edit records, but cannot delete or modify records or templates.
- Browse: Allows read-only access to specific parts of the database.

You can tailor the permissions for the Manager and Standard user roles using user-based Custom Permissions.

Consider using the Custom Permissions to judiciously revoke the ability to *Delete*

Securing Your Customer Information

(continued from cover)

Records or *Export to Excel* to preserve the integrity of your database and to prevent a disgruntled employee from walking off with your customer information.

Passwords

Passwords form the basis of any security system and a well-structured password policy is essential. Here are the password policy parameters within ACT! by Sage:

- **Re-use**: Restricts the use of the last x-number of recently used passwords.
- **Change Interval**: Sets the maximum length of time in days that a password can be used.
- **Minimum Duration Between Changes**: Sets the minimum duration length of time a password can be used. Setting the password minimum age parameter to two days, for example, prevents a user from repeatedly changing a password during a single session in order to cycle through the password history to reuse an old password.
- **Length**: Sets the minimum number of characters a password must contain. A good length for passwords is eight characters. This is long enough to be difficult to crack, but short enough that users can remember the password without writing it down.
- **Required Number of Character Groups**: Specifies the number of character types the password must incorporate. Available types are: Lower-case (a-z), Upper-case (A-Z), Numeric (0-9), and Special Characters (printable Extended ASCII set).

You can define overriding password settings by user. For example, if the password policy dictates a password change every 90 days, but a user's settings indicate that the user cannot change a password, the user's setting applies. Other user-specific password settings include the requirement for the user to change their password upon next login, and to indicate that a user's password never expires.

Database Security

You can maintain multiple ACT! by Sage databases and vary the security setup within each database according to your business needs. Access to a database is protected through the use of unique user names that grant users the right to open a database after logging on. The user must enter a valid user name and a password to access the database.

Feature Security

Feature Security controls who can use specific features. Each ACT! by Sage database user is assigned a role. Each role dictates which features a user can access in the application.

Record Security

Record Security in ACT! by Sage is determined by ownership, by role, and by the Access Control List (ACL). The ACL records the users and teams who can access a record. Administrators can assign user or team access to individual contacts, companies, or groups using the ACL.

Each record in the database has an owner called a record manager. A record manager can change the ownership and modify the ACL of records that he or she owns. The exception to this policy is for Browse role users—they are not allowed to modify the database in any way.

Record Security could be used, for example, to allow your sales representatives access to only their customers and prospects.

Field-Level Security

Field-Level Security represents the most precise level of control. Administrators and managers can secure individual fields, allowing or denying access to specific users or teams of users. Users can be given **Full Access**, **Read-only Access**, or **No Access** to fields on a user-by-user basis. Field-Level Security 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). Each field has a Default Permission that applies to all users until modified by the administrator.

Use this level of security to protect sensitive data that you either do not want certain users to see, or to ensure that certain users cannot deliberately or inadvertently change the data.

The Role Of Windows Security

ACT! by Sage uses Microsoft Windows file security to manage access to non-database items stored in the file system. These items include: attachments, document tab items, layout templates, saved queries, report templates, and word processor templates. In order for a user to use features related to these items, they must have Windows access to the related folders.

Call us for more information about ACT! by Sage or to help you establish a security structure that works for your organization.

((Tips & Tricks))

Password Protection Tips

» Avoid dictionary words in any language when creating a password.

» Avoid using significant dates or your children's or pet's names in a password.

» Never use the option to save or remember a password to your computer.

» An idea for a strong password is to base it on a song title or other phrase. For example, the phrase might be: "This may be one way to remember" and the password could be: Tmb1w2r.

» Enable password protected screen savers that kick in after five minutes of inactivity.