Security Guard

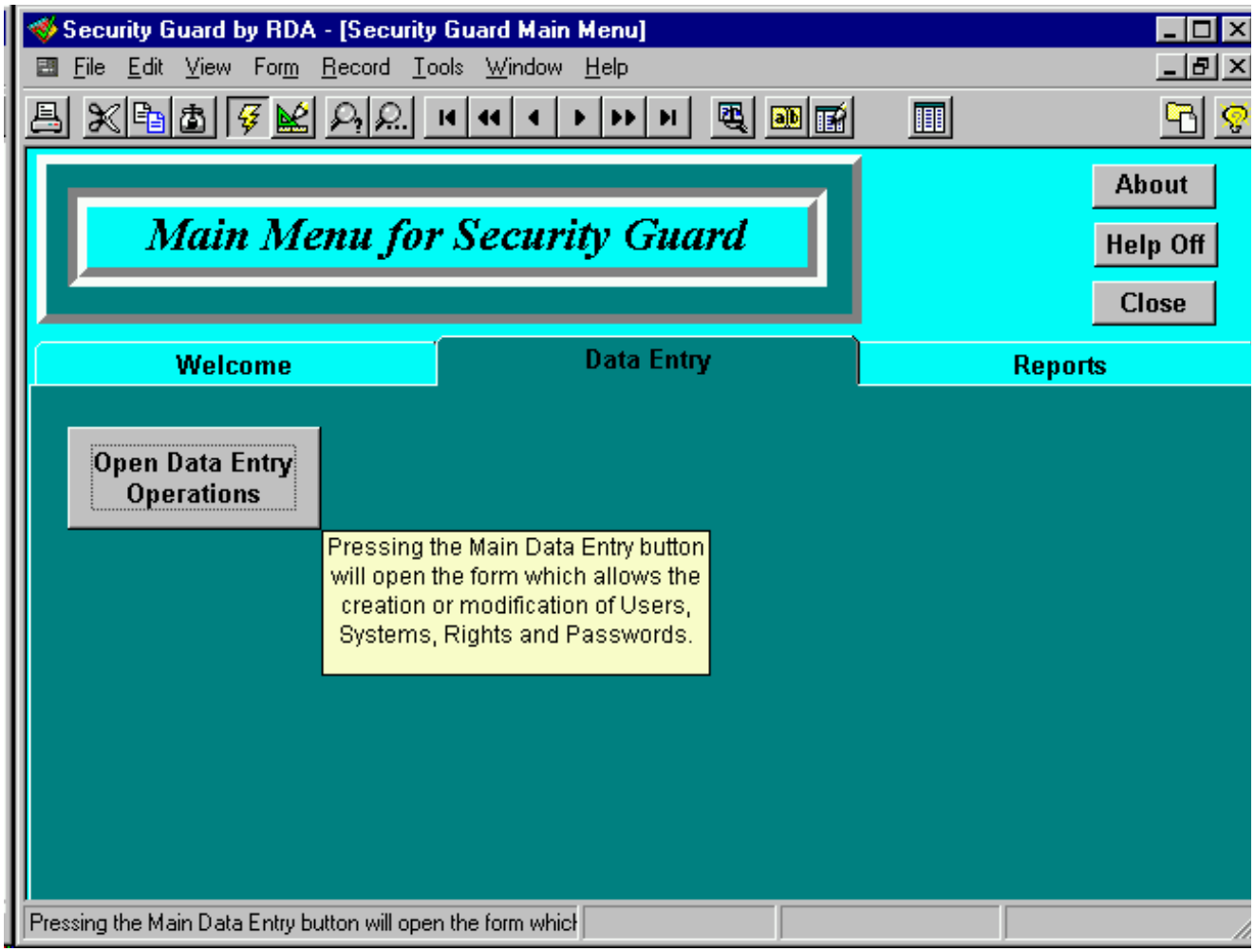
by

Resource Development Associates

Security Guard is a system for Paradox developers who wish to manage table and field level security without giving users actual table and field level passwords. Security Guard works on local tables, Local Area Networks (LANS) and the Internet. Both the desktop management console and the web browser based management console allows developers and administrators to create users and systems and have user passwords issue the actual table and field passwords. In this way no one except developers and administrators ever need the actual passwords. This improves security and eliminates the need to restructure tables to modify system security. This document covers the LAN based version of Security Guard. There is a separate document that covers the Internet based version. Both versions can be integrated to allow mixed LAN and Internet access to Paradox tables protected with passwords. The full Security Guard product comes with the LAN, Internet and Password Dialog components. Security Guard can also be purchased in an Internet only version for users who only or mostly plan to use their password

protected tables through the Paradox OCX based web server. The Internet version can also be mixed with the LAN based password dialogs to provide a mixed LAN and Internet solution with an Internet only Management Console for Security Guard. Details and pricing is available on our web site.

When the Security Guard system is opened on the desktop the main menu above is displayed. This menu includes the Welcome screen shown here. This contains contact information, a toggle button to turn the extended balloon help on or off (short balloon help is on by default as displayed above) an about and close buttons and notebook tabs for data entry and report functions.

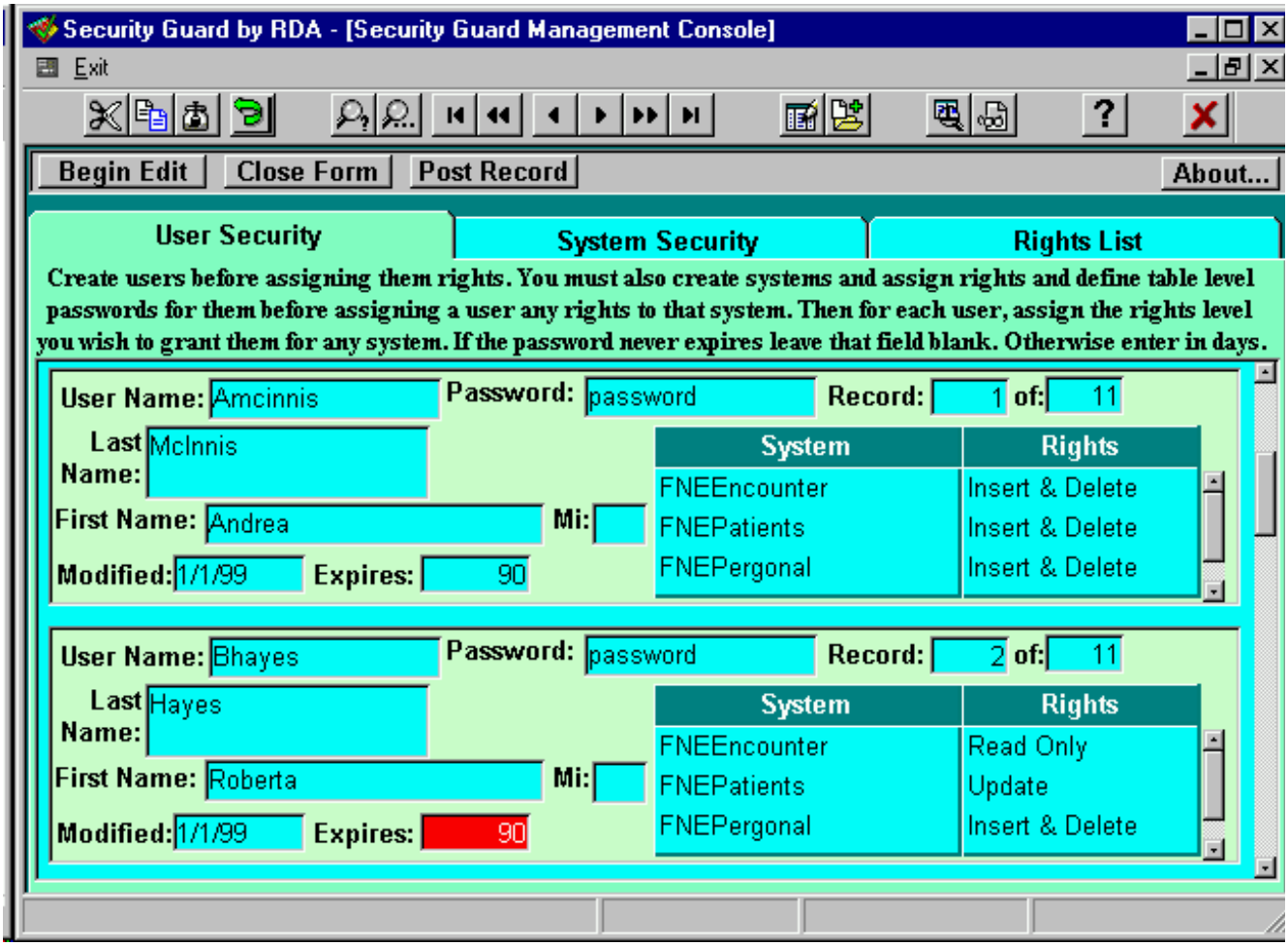


When the main menu is opened the Password Dialog is presented. Only users with sufficient access can go beyond this Main Menu screen. The Password Dialog is also used for protection and password submission to systems you develop and is described later in this document.

The data entry tab allows you to open the administration console if you have sufficient rights. Attempting to open the console without sufficient rights temporarily disables the system The data entry tab is displayed above with the extended balloon help on. (Note: the cursor must be on a button for the help balloon to display but cursors are not captured in the screen shots. Also this

balloon help technology is available for your applications in RDA's BubbleHelp which is also available from our online store.)

The Reports tab (not displayed) has a Print Reports and View Reports Tab each of which has a button for printing an Access Level by User report.

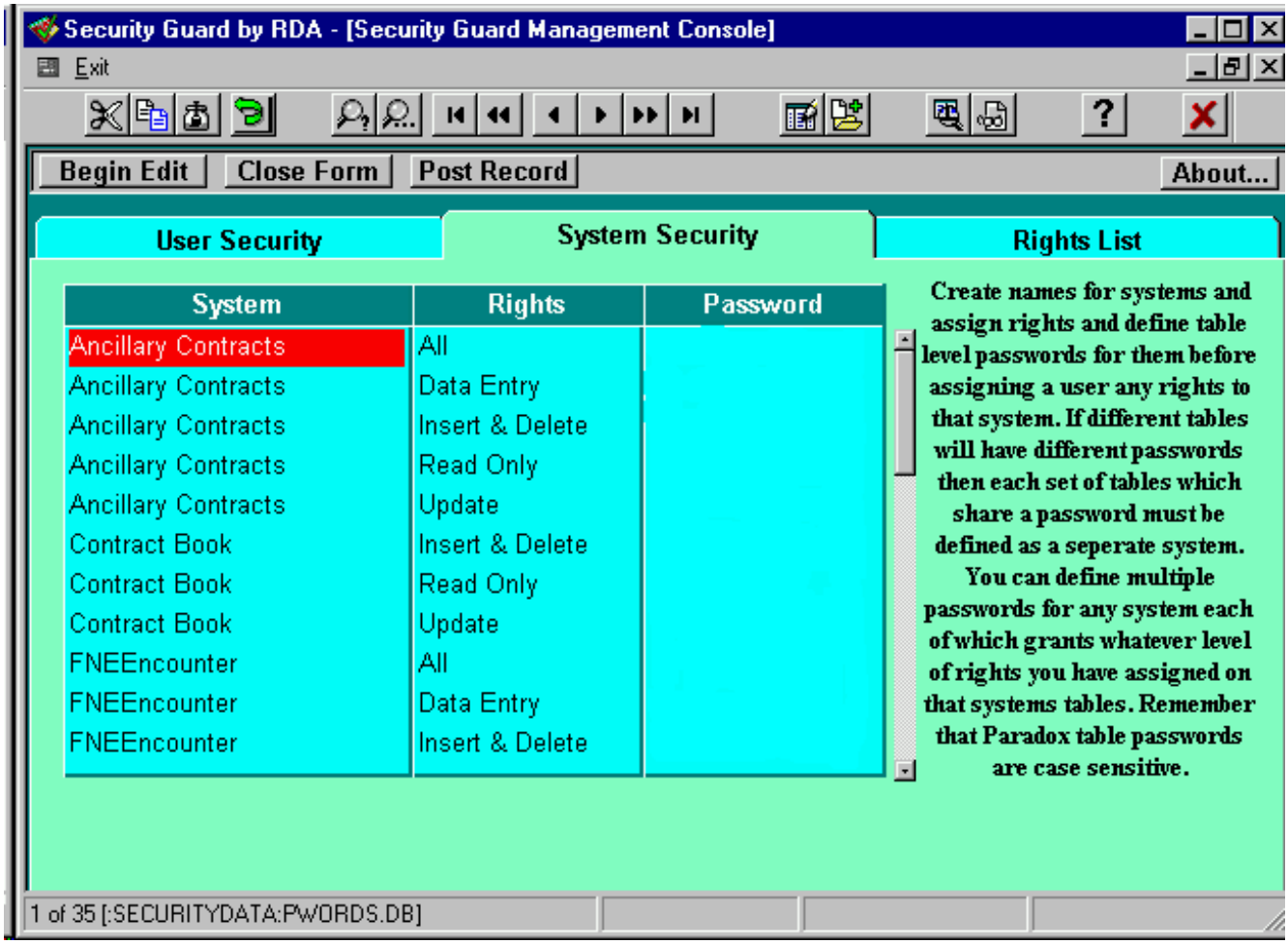


After opening the Management Console you can create and manage systems, system passwords, users, user passwords and user rights. When you first open the console you are presented with the User Security Tab as displayed below. This is where Users are created and granted system access rights. Users may be granted any level of rights to any system managed by Security Guard. There are no effective limits on how many systems or rights levels can be managed. Users passwords can also be managed here. Users must have their initial password set when the user is created. After that the user can update or change their password from the Password Dialog or the administrator can do so from the console.

The management console also has a custom tool bar and a button bar which provide editing and

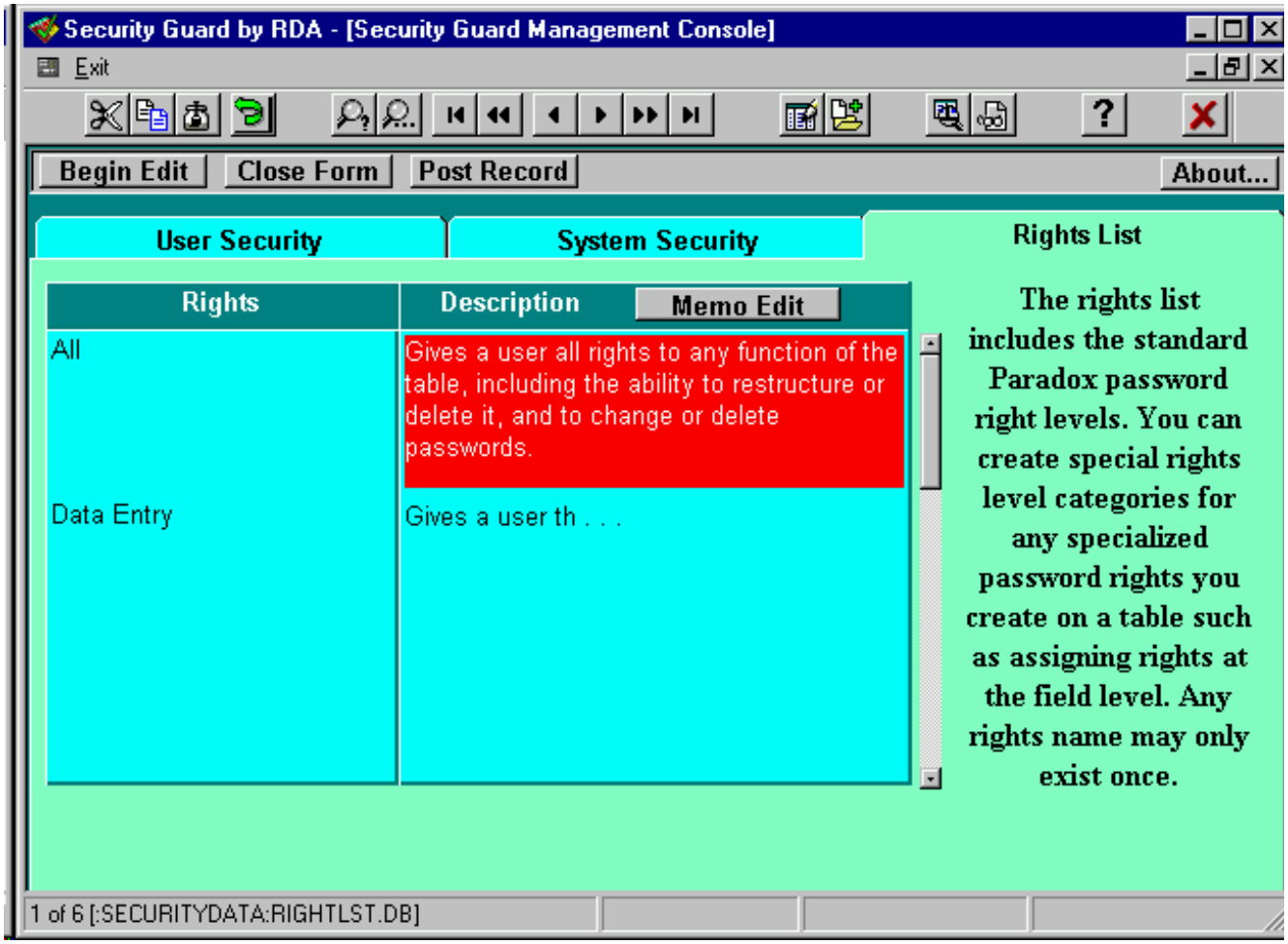
posting functions, cut, copy and paste functions, undo functions etc. Keyboard shortcuts are also displayed in the balloon help for the toolbar.

Systems must be created and given passwords on the Systems Security tab prior to being able to grant a user rights to the system. The System Security tab allows you to assign various system names rights levels and the Paradox password that confers that level of rights. These are the passwords that are actually issued to a Paradox session when the User submits their password. All tables which share the same passwords for the same rights level make up a single named system. The system security tab is displayed below (passwords have been blocked out here but display in the actual system).



Security Guard comes with an administrator account built in and the Insert and Delete password for the system already assigned to that account. Administrators should modify the administrator account and assign the Security Guard system to any administrator accounts on initial installation of the system.

The final tab in the console is the rights list. This is the lookup table for the System Security rights and comes with the standard Paradox table right types already built in. Administrators can modify



this rights list to add custom rights. This tab is displayed below.

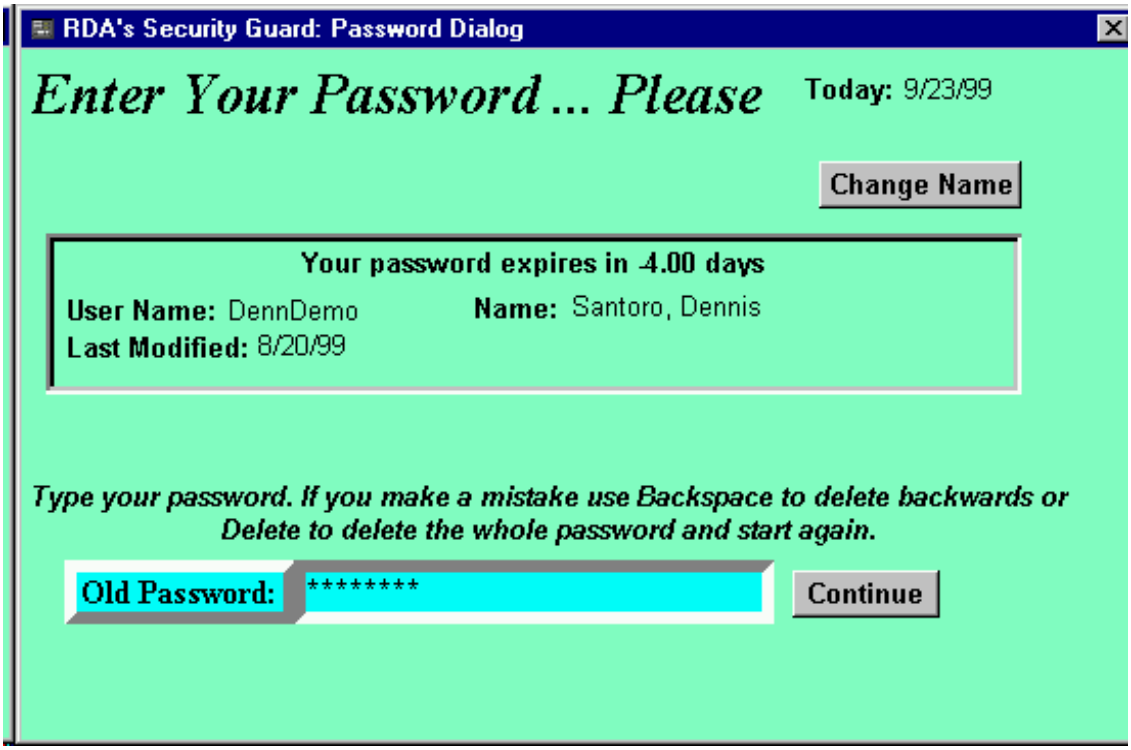
The Administration Console is currently available for Paradox 7 (32 bit only) and Paradox 8, 9 &10. The Password Dialog box is available for Paradox 5, 7 (16 and 32 bit), 8, 9 and 10.

The Security Guard Password Dialog box is run by a script which launches the dialog box. The script can be run from the startup screen of your application or directly from the command line of an icon which launches Paradox for interactive sessions. This allows developers and administrators to build security into custom applications or interactive Paradox use. When the Dialog is launched it accesses the user name from the network and compares it to the list of user names in the system. If the user is in the system the dialog box displays the user's current system status and requests a password as shown below. This includes a display of the user name currently accessing the system, days left to expiration of the password, when the password was last modified and the user name. The user can use the change button to change to a user name with different credentials if they wish. This allows administrators to provide varying levels of rights to users for use under different circumstances as well as allowing one user to log on from a station currently logged into the network by a different user.

If the current network credentials do not match an existing user in the Security Guard database the user is informed of this and given an opportunity to change to a different user name before the Password Dialog displays. The user must present both valid Security Guard credentials and password to be granted access to any systems protected by Security Guard. If the user's password is near expiration or has expired the user will be given the opportunity to change or update the password. Passwords can not be changed or updated without issuing the proper current or expired password. Expired passwords will allow the user to change or update their password but will not allow access to any system protected by Security Guard. Passwords on the Password Dialog are always displayed as asterixes. The password expired warning and password change process are displayed below.

After entering a password, pressing enter or the OK button submit the users credentials from the Security Guard database to the Paradox session granting the user rights in the session to all systems to which the user has been previously granted rights by the administrator. And since the passwords are placed in memory only they are not written to disk and therefore not exposed.

The Password Expired Warning



Step 1 for changing passwords.

Step 2 for changing passwords.