Security Guard

by

Resource Development Associates

Installation instructions:

There are 3 components to Security Guard installation. First the Management Console must be installed on the host system. Usually this is the network server but this can be on the client system (see the section on Aliases for details). Then the Password Dialog must be installed. Usually this is on the network server in the same location as the management console but this can be on the client system (see the section on Aliases for details). The data must then be installed on the host system. Data cannot be installed on the client system because it must be shared among all the security system users.

Management Console:

The Management Console includes the files:
Aboutsg.fdl
Acceslvl.rdl
Pwordde.fdl
RDAtools.ldl
Sgmainmu.fdl
Undo.bmp

These files must be installed in the same directory. The file Aboutsg.fdl must also be copied to the windows directory (Windows, Winnt35, Winnt or Winnt40 - case is not important) of any machine from which you wish to run the management console.

The management console includes the Security Guard Main Menu, data entry form (Management Console screen) a report which allows you to produce access level reports on users, the RDAtools library which provides a dockable toolbar for the Management Console screen and a variety of other system functions and the Copyright (About) screen.

As a general rule, it is best to install the Management console to a server so that it can be run from a variety of workstations. Your license allows you to install it on multiple workstations, however, as long as they operate at one site (one LAN or WAN). You may also install a separate copy in your development environment however you must manage password and system synchronization between the development security database and the production security database manually under those circumstances as RDA could not plan for all contingencies in such a mixed environment.

Password Dialog:

The Password Dialog is the main component of Security Guard. This provides end users the ability to enter, and modify their passwords and submits the end user passwords to the Security

Guard system, selects the passwords for the systems and access levels the user has rights to and submits the real passwords to the Paradox session the user is running. The Password Dialog consists of 2 files:

pwdlgXXX.FDL
sgopnXXX.SDL

XXX is replaced by the Paradox version you are using such as 732, 516 or 10. Your Management Console comes with the Password dialog components which match the Management Console version you purchased. Other versions are available for a separate fee. All versions will work with the same Security database but will only function as a client with the Paradox version for which they were compiled.

The Password Dialog can be installed either in the same directory as the Management Console, which is the preferred method, or on the client machine. Installation on the client machine involves different Aliasing than if the Dialog is installed in the same directory as the Management Console.

The Password Dialog is called by the sgopnXXX.SDL. This script can be called from the launching icon command line or can be called by the opening form of your application. The first allows interactive use of Paradox while still allowing for system security. The second allows you to set your application to launch an opening screen and only call the Password Dialog prior to the user attempting to access data which would require password access. This allows wide flexibility for developers.

Security Data:

Security data should be installed in a separate directory on the host system but can be installed in the same directory as the management console if you wish. The latter is not recommended, however. Users must have at least change level access to the data directory as they are able to modify their passwords from the Password Dialog. The Security Data consists of the files:

Pwords.db
Pwords.px
Pwords.val
Rightslst.db
Rightslst.mb
Rightslst.px
Rightslst.val
Rights.db
Rights.px
Rights.val
Security.db
Security.px
Security.val
Security.xg0
Security.yg0

Direct access to the security data is available through the Management Console. The Password Dialog also accesses these files but only via a tcursor so the data is never available to end users. Staff granted access in the Management Console to the security data can only be granted Insert and Delete access. It is recommended that few staff be granted this access. Initially, one user exists in the database. The User name is Newuser and the password is Newuser (case is important for both). You are strongly encouraged to create a new account for the administrator and grant the administrator access to the Security Guard system and then delete this Newuser account as soon as you begin using the system. The uses of the various files are explained in the Management Console itself as well as in the Security Guard documentation file (Sgdoc.pdf).

Aliases:

Aliases must be created for Security Guard to function. These Aliases can have different paths for the Password Dialog if you wish. But normal path rules must be followed for accessing the data and the data must be controlled by the same .Net file for all users as with any shared Paradox data.

The Alias to the Management Console and the Password Dialog must be **:SecurityMain:**and the Alias to the Security Data must be **:SecurityData:**. If you wish to have the Password Dialog running from a different directory than the Management Console then the users accessing it from that other directory must also use a separate IDAPI.CFG file as an alias can not have 2 paths nor can an alias exist twice with different paths in the same CFG file.

Using Security Guard:

Once the files are installed in their directories and the Aliases are set up you can start Security Guard. The management console should be started from an Icon with a command line of:

```
"C:\Program Files\Borland\Paradox\PDXWIN32.EXE" sgmainmu.fdl -wc:\clientap\security
-pc:\temp\secupriv -oc:\progra~1\borland\common~1\bde\idapi.cfg -c -q
```

Where the paths to the -w, -p and -o switches are modified to the locations of the working directory for Security Guard (which does not have to be where you located the management console), the Security Guard private directory which you create and which, as with any Paradox application, must be separate from the private directories of your other Paradox applications, and the location of the IDAPI.CFG file which contains the appropriate aliases. You can, of course, use your default IDAPI.CFG and skip the -o switch as long as the aliases are properly established. You could, if you wanted, also create a script which sets the Aliases instead of them being permanent and then have the script call the sgmainmu.fdl. Once you launch the Management console you can begin setting up users, systems and security levels based on your needs.