

## **ArrayTrack™ Security Levels- Detailed Information**

External ArrayTrack™ users have two basic security options.

Unprompted local version:

This is the simplest option. For trusted users on trusted networks only. Security is applied by the ArrayTrack™ application itself based on the OS-reported user id. The main weakness in this approach is that all users have access to the shared Oracle login information, which is stored on each user's hard drive. Initially each user must configure this connection information the first time the application is run, or else the ArrayTrack/preferences file containing this connection information must be distributed into each user's home directory. Since each user has access to the shared database login information, a malicious user could bypass the application-level security by using other software to connect to the database, or more simply by creating alternate OS-level user id's on their client machine and then using these to connect as other users. Also, further security cannot be applied at the database level because all users login directly to the database schema and thus cannot be differentiated at the database level.

Prompted login version:

This version is more secure than the unprompted version, and can be made very secure with the help of an active database administrator. At the minimum level of security for this version, a database administrator would simply create a database user identifier (schema) for each application user, using scripts provided with the ArrayTrack™ distribution. Running this way is already more secure than the unprompted version, since no sensitive login information is stored on anyone's hard drive, and each user only knows the login to their own private schema for accessing ArrayTrack™ tables. This means that the database administrator may apply further restrictions and auditing of individual users at the database level. Such restrictions (though not present by default) would prevent users from being able to access restricted information by using another program to access the database. Also, there is no reliance on the OS-reported user id - the user must type in a user name (this first time) and password (each time) to run the application. Although the database user/role creation scripts that ship with ArrayTrack™ have no database-level restrictions (so security is applied only by the ArrayTrack™ application itself by default), a more restricted security system would be easy for a knowledgeable database administrator to implement at the database level.