Jan 11, 2012

Informix Database Permissions Setup

The Fitrix Informix databases can be secured to allow access to tables for read permissions only. This is useful when you have configured ODBC connections for external applications, and you want to ensure these applications cannot corrupt tables.

This example assumes you want to limit access for a Linux user 'john', so that when he is connected to the Informix database, he can only read data.

NOTE: If you are restricting access due to a previously configured ODBC connection, the ODBC configuration included a 'User Name' and 'Password' which would be used to connect to the database. You would be applying the following instructions to this user. Therefore, it is good practice to create a Linux user name and password that would be used only for connecting to the database, and would not be used as a typical Linux login to run the Fitrix applications.

Step-By-Step

1. Verify that you have not granted special database permissions to 'public' (such as DBA, resource, or connect). If so you should revoke these permissions for 'public' (NOTE: you may need to revoke multiple times, once for each of DBA, resource, and connect). If you are unsure, you can:
   a. Execute the 'dbschema' command, directing the output to a file.
   b. View the output file. Any special permissions will be listed in the first few lines of the file.
2. Verify that you have not granted special database permissions to 'john' (such as DBA, resource, or connect). If so you should revoke these permissions for 'john' (NOTE: you may need to revoke multiple times, once for each of DBA, resource, and connect). If you are unsure, you can:
   a. Execute the 'dbschema' command, directing the output to a file.
   b. View the output file. Any special permissions will be listed in the first few lines of the file.
3. Grant 'connect' permissions to 'john' to the database
4. Grant 'select' permissions on each table for 'john', for each table you want to allow john to read.
   a. NOTE: if you do not grant select permission for specific tables, then user 'john' will not be able to read those tables, either.

Special Considerations

5. If you have previously granted special permissions to 'public', when you execute step 1 above, you will potentially be revoking access rights for ALL users, not just the user 'john'. If so, you must grant these special permissions to the specific users accessing the database, after completing steps 1-4.