
Chapter 12

Sharing Databases on a Network

With Standard & Poor's Research Insight, you can share databases that you create on a network just as you can share subscription databases. User-defined databases can also be accessed by multiple users simultaneously and new information is available to all network users as it is being written to speed the flow of customized financial and market information through your organization.

This chapter covers

- simultaneous access
- changing concepts in a network environment
- write-to privileges and passwords
- recommendations

Simultaneous Access

Research Insight provides simultaneous access to user-defined databases, allowing information to be shared by several people at the same time. Generally, you can continue to read a database while someone else is writing changes to that database.

Although simultaneous access is possible, you should try to avoid writing to databases that are in use. If user A is running a report or screening the database for a specific data item, and user B is changing values for the same data item, user A may see all, some or none of the changes. It's all a matter of timing.

We recommend that changes be made to shared, user-defined databases during off hours, or that users be informed to detach from a database temporarily so that changes can be written to it. Taking this approach ensures that everyone has access to the same data.

Note: Although information can be accessed as it is written, it will not be visible in the **Look Up** list. The **Look Up** list has to be closed and re-opened after the addition of information for the information to be visible.

Changing Concepts in a Network Environment

Research Insight allows you to change or delete any re-defined COMPUSTAT concept. However, before you edit a concept that is shared in a network environment, consider how the write-to database impacts the change.

If you want to change a concept definition and make the change available to everyone on the network, the write-to database must be a shared network database. (Generally, this database is named CS5NET.)

Alternately, if you want to change a concept for your personal use while leaving the network definition unchanged for everyone else, the write-to database must be your own private database (generally named CS5USER), and you must rename the concept and save it with the new name. If you do not rename the concept, Research Insight removes the old definition from the network dictionary because there cannot be two definitions for the same concept. The definitions collide. Unfortunately, once Research Insight resolves this collision, the other network users are left without a concept because they cannot access your private database where the concept is now stored.

It is always good practice to rename any concept that you change and save the concept with the new name. That way, the original COMPUSTAT concept and its definition is always available for future use.

Refer to Chapter 10 - Managing Your Databases for a complete explanation of the write-to database.

Write-to Privileges and Passwords

Research Insight has a password feature that allows you to limit access to the Database Group dialog box (shown on the next page). Without the password, a user cannot change the write-to database or the database configuration of any group. The password feature can be used by individuals to protect their own databases, and it can be used by network administrators to limit write-to privileges to one or two users.

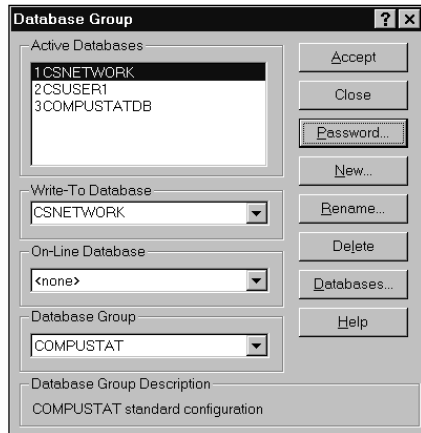
To use the password to limit access to network databases, the network administrator needs to enter the password on each workstation site. Keep in mind that passwords are not fail-safe, and they are not meant to replace a sound network management policy.

Note: Regardless of password protection, it is possible for individual users on a network to delete, rename or move information contained in network databases with the Collision Detection feature of Research Insight. Users should be advised against doing so. Instead, to reconcile collisions, users should be advised to make the necessary changes to their own databases.

Adding a Password

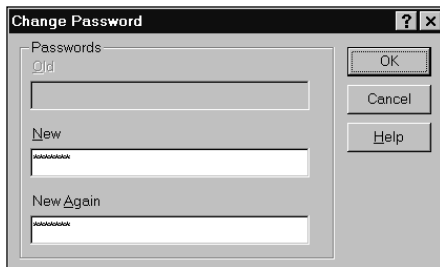
Begin from the Research Insight desktop:

1. From the **Databases** menu, select **Database Group** to display the Database Group dialog box.



2. Click the **Password** button.

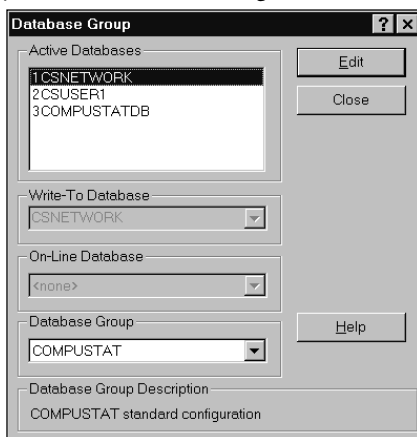
The Change Password dialog box appears.



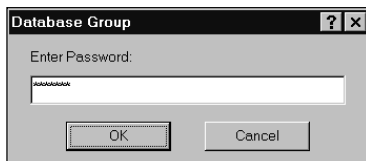
3. Enter a password in the **New** field. (Note: passwords are case-sensitive.)
4. Repeat the password in the **New Again** field.
5. Click **OK**.

The Database Group dialog box appears again.

After you close the Database Group dialog box and return to it at any point in the future, you will see the following:



Any time you click **Edit** in this dialog box, Research Insight first asks you for a password before allowing you to proceed, as shown below.



Without the password, users cannot change the write-to database or proceed to the Databases dialog box.

Changing a Password

Begin from the Database Group dialog box:

1. Click **Edit**.
Enter your old password in the **Enter Password** field and click **OK**.
The Database Group dialog box appears.
2. Click the **Password** button.
The Change Password dialog box appears.
3. Enter your old password in the **Old** field.
4. Enter your new password in the **New** field.
5. Reenter your new password in the **New Again** field.
6. Click **OK**.
Your password has been changed.

Deleting a Password

Begin from the Databases Group dialog box:

1. Click **Edit**.
Enter your old password in the **Enter Password** field and click **OK**.
The Database Group dialog box appears.
2. Click on the **Password** button again.
The Change Password dialog box appears.
3. Enter your old password in the **Old** field.
4. Click **OK**.
Your password has been deleted.

Recommendations

As is the case with all networked systems, Network Management must establish clear policies and inform all users of those policies. On that note, we make the following recommendations for managing shared, user-defined databases on a network:

- Only one or two people should write to or make any changes to shared, network databases.
- Make large scale changes to databases during off hours, or inform users to temporarily detach from a database so that changes can be written to it.
- Store definitions and their associated data values in the same database. (This minimizes the chance for orphan data.)
- Attach no more than eight databases to a group.
- Inform users to make changes to their databases to resolve collisions with network databases.

- Create as few databases as possible. (Research Insight has pre-defined, user databases for network users. The databases are named CS5NET for the COMPUSTAT (North America) database and GV5NET for COMPUSTAT (Global)
- Backup your user databases on a regular basis.
- Backup concepts for users and networks.

These recommendations allow you to enjoy all of the benefits of sharing user-defined, Research Insight databases, while minimizing the potential for problems common to network systems.