

## **Information about the Library Online Workaround 2/9/04**

### **Introduction**

Library Online provides a "workaround" to make the workstations usable when the server is unavailable. Here's how it theoretically works:

1. The patron attempts to log in. They receive a "Failed to connect to server" error message.
2. The patron repeats this process 3 times (Note: This does take some time in-between each attempt).
3. After the login attempts fail 3 times, the patron is given the option to have a 1 hour session. Library Online loads with whatever applications were available to the last patron. This session will not count against the person's daily time.

### **The problem**

This workaround relies on 2 local files: `disclaim.dat` (to display the Internet acceptable use policy) and `appnamepath.dat` (to display the applications).

In a perfect world, these two files would be written to the hard drive during each patron session. However, most libraries do not allow patrons to write to the hard drive, or, if they do, they use products like DriveShield to destroy any changes made to the hard drive when the machine is rebooted.

So, in order for this workaround to work, these 2 files must somehow be written to the hard drive and write-protected.

### **The problem on top of the problem**

This sounds simple enough, but there is an additional problem. In the version of Library Online we are currently using, the software looks for these 2 files in the default startup directory for **the user**. This varies from operating system to operating system and from environment to environment. I can't simply tell you to put these files in the `c:\telus` folder or some other folder. The correct folder for your environment needs to be determined before the files can be put in the correct place.

## **Recommended procedure**

If you can write to the hard drive as the default user:

1. Disable any security software that would prevent changes to the hard drive from being saved.
2. Log in as the default user.
3. Log in as you normally would.
4. End your session (or logout).
5. Search the hard drive for the files "appnamepath.dat" and "disclaim.dat". Hopefully, you will find only 1 set of these files, probably both in the same directory.
6. Make these files read-only.

If you cannot write to the hard drive as the default user:

1. Disable any security software that would prevent changes to the hard drive from being saved.
2. Log in as the administrator.
3. Log in as you normally would.
4. End your session (or logout).
5. Search the hard drive for the files "appnamepath.dat" and "disclaim.dat". Hopefully, you will find only 1 set of these files, probably both in the same directory.
6. If you locate the files in a directory which is not specific to the Administrative user (like c:\), leave the files where they are and make them read-only.

If you locate the files in a directory which is user-specific (like c:\documents and settings\administrator), move the files to the equivalent folder for the default user (like c:\documents and settings\defaultuser) and make them read-only.

## **To test your file placement:**

You can test this workaround by pulling the network cable from the computer and logging in. If you see the acceptable use policy and applications in the box, you're all set.

If you are using a domain name server, I would recommend that you do not pull the network cable from the computer itself, but instead cut off the Internet connection beyond the server. Because the default directory for the user may be on the server, the server needs to be part of the equation when testing the solution.

### **Additional information for Gates Machines:**

If the above procedure does not work for your Gates machines, here are some additional things to do:

1. Make sure Centurion Guard is unlocked.
2. Give full permissions to everybody for the c:\telus directory.
3. Give everybody write permissions to the "all" folder under policies.