

## 6.0 Network Security



During installation, you must have full access to both the local hard drive and the network server. All users should have full network permissions for the `DIWE5NET` folder and the folders it contains.

After the program is installed, though, it is possible to protect certain folders by assigning different levels of network permissions to different groups of DIWE users. Restricting access is not a function of DIWE but of the network operating system. This section explains how to restrict access to Windows 2000 Server; the same process works for other networks, although the terminology may be different.

### 6.1 Assigning DIWE5 Permissions

After DIWE has been installed, all users can be restricted to reading and executing files in the `DIWE5` folder. The only exception is when you must modify the `winDIWE.ini` file while troubleshooting or configuring your installation.

### 6.2 Assigning DIWE5NET Permissions

DIWE has three levels of users: Student, Instructor, and Administrator. To provide the highest level of security, you need three corresponding user groups, created through Windows 2000 Server. Each user must log in to Windows and be identified as a member of one of those three groups to use the program. Note, however, that there is no actual connection between DIWE users and Windows network users. A person could log in to Windows using a student ID and then log in to DIWE as The Administrator. When that person tries to perform administrative tasks, such as creating new classes, error messages appear if access to the `DIWE5NET` folder has been restricted.

To assign these network permissions, first set the `DIWE5NET` folder so it does not inherit permissions from its parent folder; then do the same for the `Defaults` folder and the `PM` folder. All other folders should be allowed to inherit permissions. Once the inheritance rules have been set, assign the permissions as shown in the following table.

Folder	Administrator Permissions	Instructor Permissions	Student Permissions
DIWE5NET	Full (Modify, ReadExec, List, Read, Write)	List, Read	List, Read
Bitmaps	List, Read	List, Read	List, Read
Classes	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)
Defaults	ReadExec, List, Read	None	None
Invent	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)	List, Read
PM	ReadExec, List, Read	ReadExec, List, Read	None
Records	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)
Respond	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)	List, Read
Users	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)	Full (Modify, ReadExec, List, Read, Write)

Abbreviations: ReadExec = Read and Execute    List = List Folder Contents

Be sure to test DIWE after changing network permissions. Networks are complex, and the specifications above may not work for all sites. If some part of the program fails, give users additional network permissions to the corresponding folder.

### 6.3 Further Restrictions for Invent and Respond

The Invent and Respond folders in the DIWE5NET folder on the file server contain Invent prompt files (\*.inv) and Respond prompt files (\*.rev). Some are standard with DIWE, and others are created by the instructors. In addition to making the Invent and Respond folders read-only for students, you may want to mark the standard prompt files as read-only to prevent instructors from accidentally overwriting an original prompt series file.

## 6.4 Additional Security Measures

Even after you apply the more restrictive network permissions specified above, it is still possible for users to damage the DIWE installation by deleting or modifying files, whether accidentally or maliciously. Several additional measures can be taken to improve security.

- Make frequent backups.

All files in all folders within the DIWE5NET folder should be backed up regularly—on a daily basis if possible—so that no more than one day's work is lost in case of a computer malfunction or accidental erasure.

- Make sure that the full access permissions to DIWE5NET are not applied to other folders on the network server, unless that's what you want.

- Hide the DIWE5NET folder.

Hiding a folder does not provide true security; however, hiding the folder makes it less likely that users will change files accidentally. Use My Computer or Windows Explorers to open the Properties of the DIWE5NET folder and mark it as hidden. Be aware, however, that hiding the folder may confuse instructors, who may have legitimate reasons for accessing the folder.