

## **Implementing Permissions Effectively with Netware**

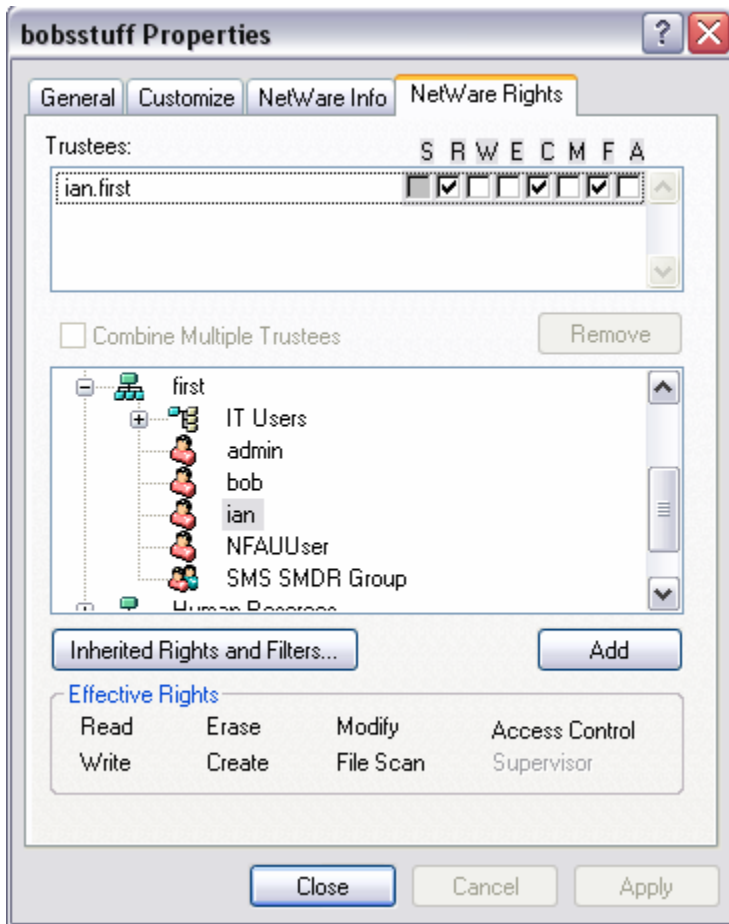
One of the major advantages of Novell NetWare is the permissions structure when a administrator effectively designs the NetWare edirectory, Novell has the unique ability to assign any permission scope to any object in the edirectory unlike Microsoft Windows that can only assign permissions to files and directory's, this major advantage is critical to the success of NetWare in educational environments with complex permissions for every user. Additionally NetWare allows individual users more control of who can access there folders.

This document will focus on the three ways of implementing permissions

- Users Assigning permissions to groups
- Controlling Access to contexts and OU's
- User Access rights – Admin Group's (Netware variant)

### **User Assigned Access Rights**

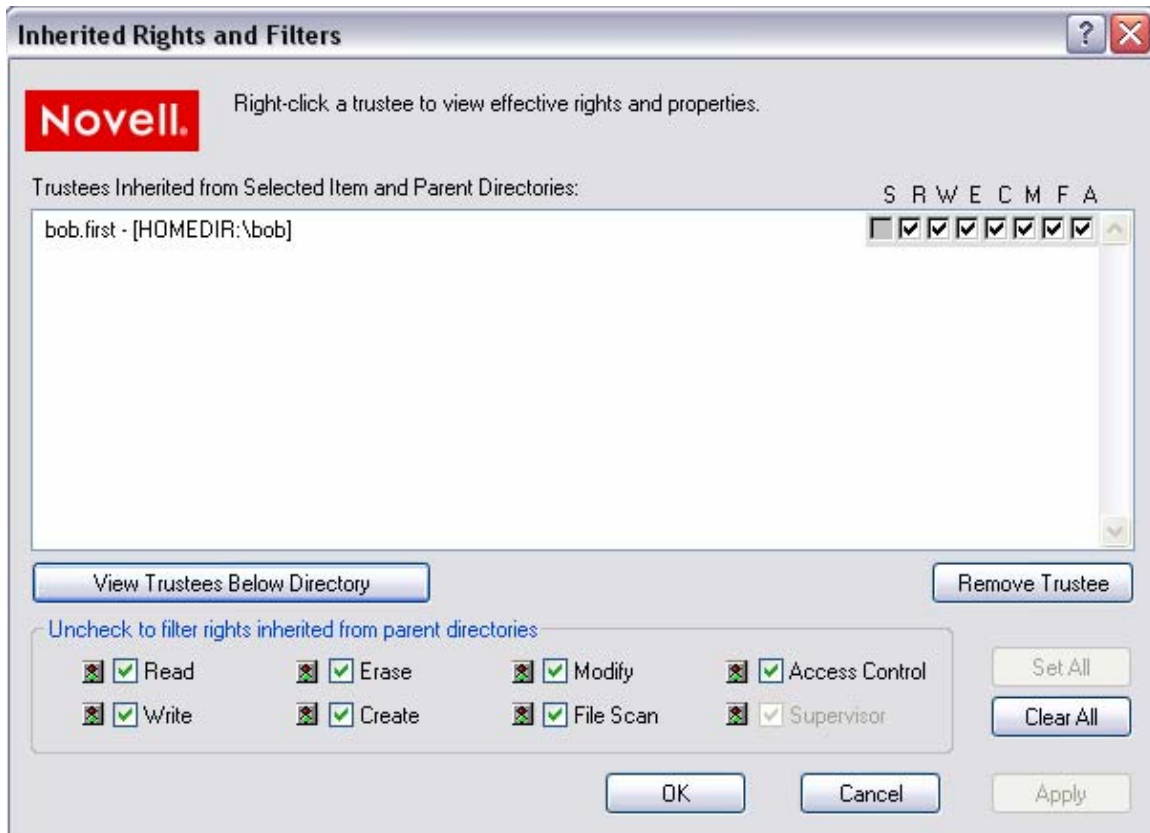
This critical feature in Novell Netware is the ability for users to control permissions to there files, like in UNIX the parameters for file control are the same, read write file scan supervisor and so on. By clicking on a network file that the user has supervisor rights to the user can control who has access to the files. And the system is built on the principle that everyone who is not on the approved list does not have access to the file, the exception being admin and security equal to admin who have root access to everything



In the instance above the owner creator of the file bobsstuff has given the user ian read create and file scan rights to the folder bobsstuff

If the user ian were given access control rights to the file ian could then deny the creator owner bob from accessing the folder. This is a critical problem for users that leave there workstations unattended in public places.

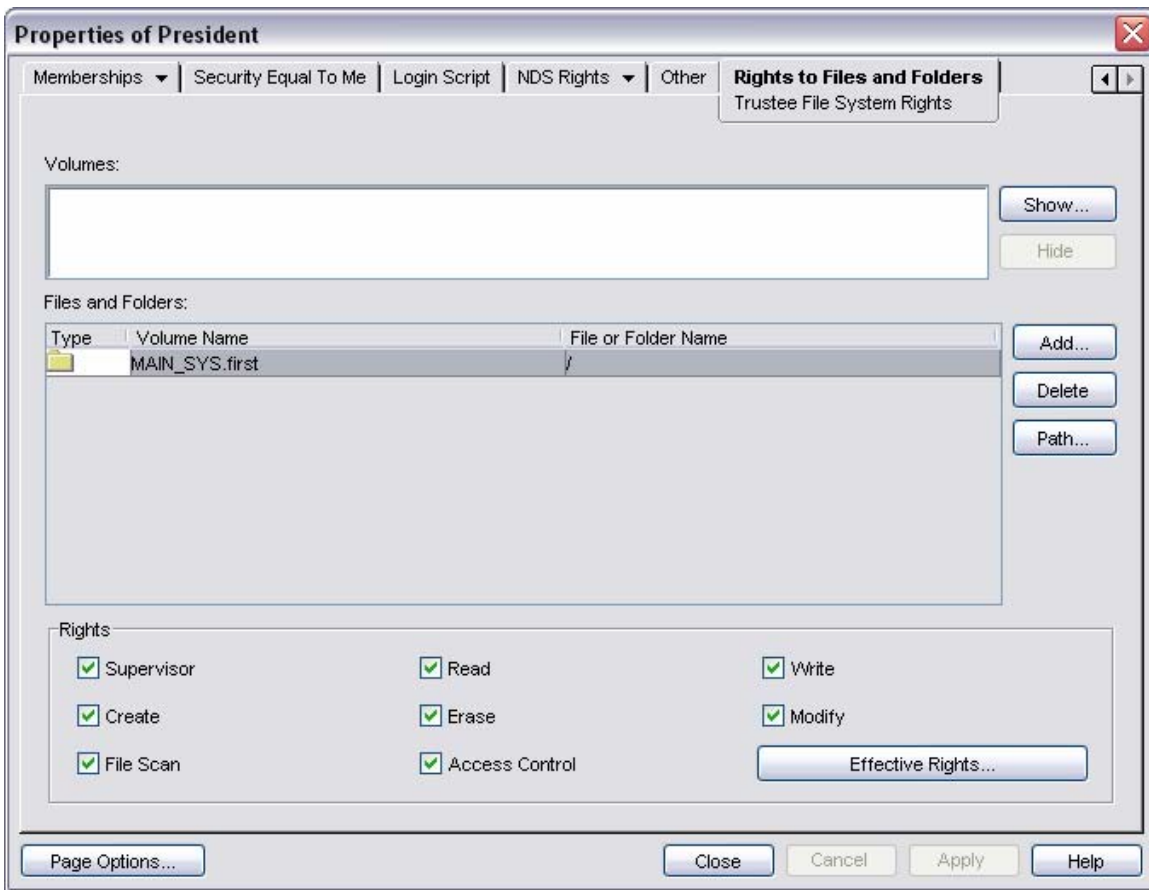
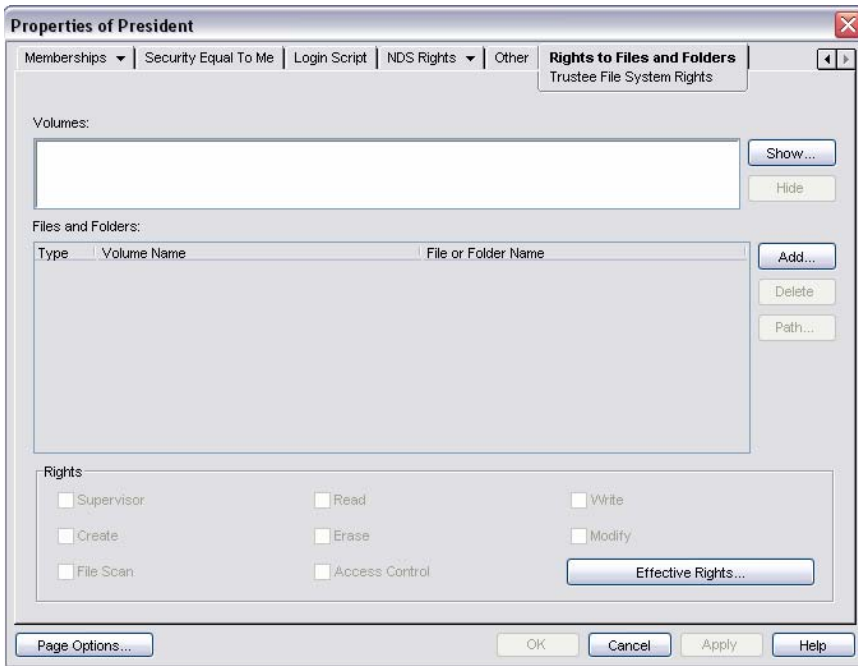
The screenshot bellow illustrates the inherited rights of the creator owner bob. A dialog that can be accessed and modified by anyone with the A (or access control) flag assigned.



Users can also assign permissions to group's contexts or ou's however this practice should be discouraged by administrators due to the fact that everything and everyone in the context or ou can access the file. Context permissions and OU permissions should only be assigned by a admin

### Controlling access to contexts

To assign permissions to a specific volume to all the users in a specific context the rights to system files and folders in console1 is used. This will allow everyone in the context to access a volume. This is usefull when creating common shares of files that everyone in a department can access. However this control supersedes any user installed permission in the mannor prescribed in the previous section



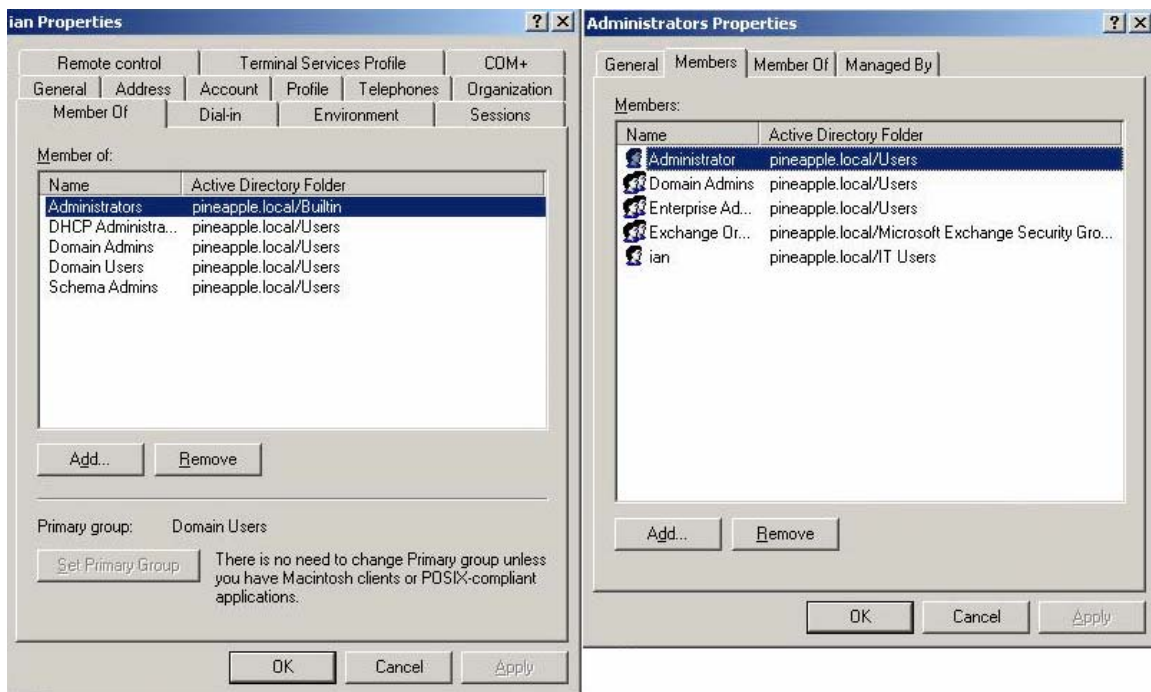
In the above two figures the first shows how the users of the president's OU have only default access, the second illustrating how the users have been granted supervisor and Access control rights to the sys context

## User assigned group access – administrators

With the Microsoft windows platform if an administrator wishes to assign a user admin rights to the network they must simply add them to the administrators workgroup. However that is not true for the Novell platform. Users must be given “security equal to me” access by the administrator, and then in turn have rights to give it to someone else, this can be a administrative issue and further stresses the need to control access to NWADMIN and console1 to prevent abuse of this problem.

For instance if one user was granted supervisor rights to a entire context, and used ConsoleOne to give another user “security equal to me” rights to that context then the second user could assign those permissions to 10 more users without the administrator ever being aware of it

The bellow screenshots illustrate how a windows user can be assigned permissions and how an administrator can view the contents of an administrators group in server 2003



The next screenshot illustrates the admin giving security equal to me to the user ian and ian giving security equal to me access to bob

