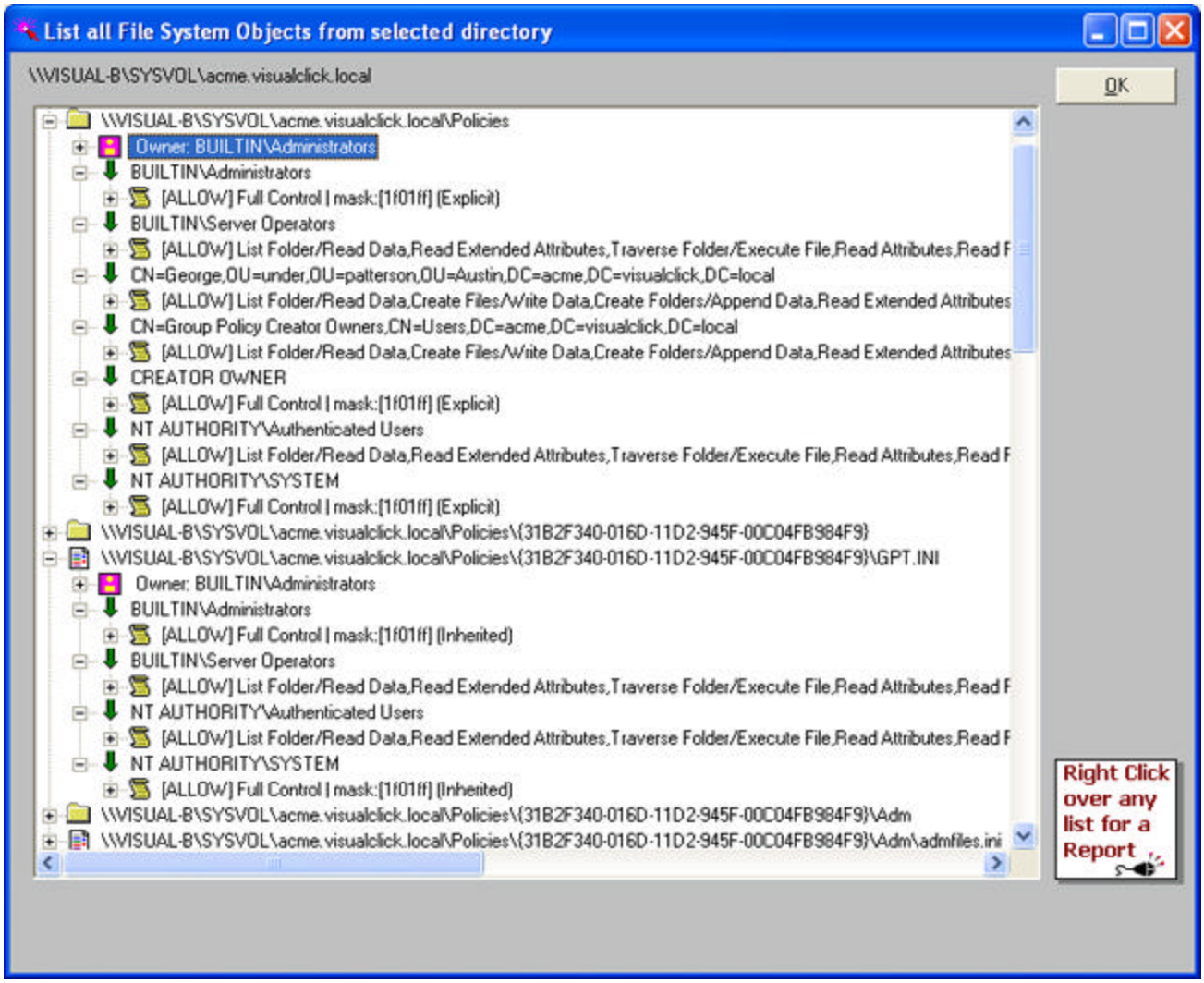
DSRAZOR Solution:
File System Security Reporter

Documenting file system security is a challenging task. The volume of data to be collected and the variety of ways to view it require an automated solution. With DSRAZOR for Windows you can collect and report file system security definitions interactively or via a batch process.

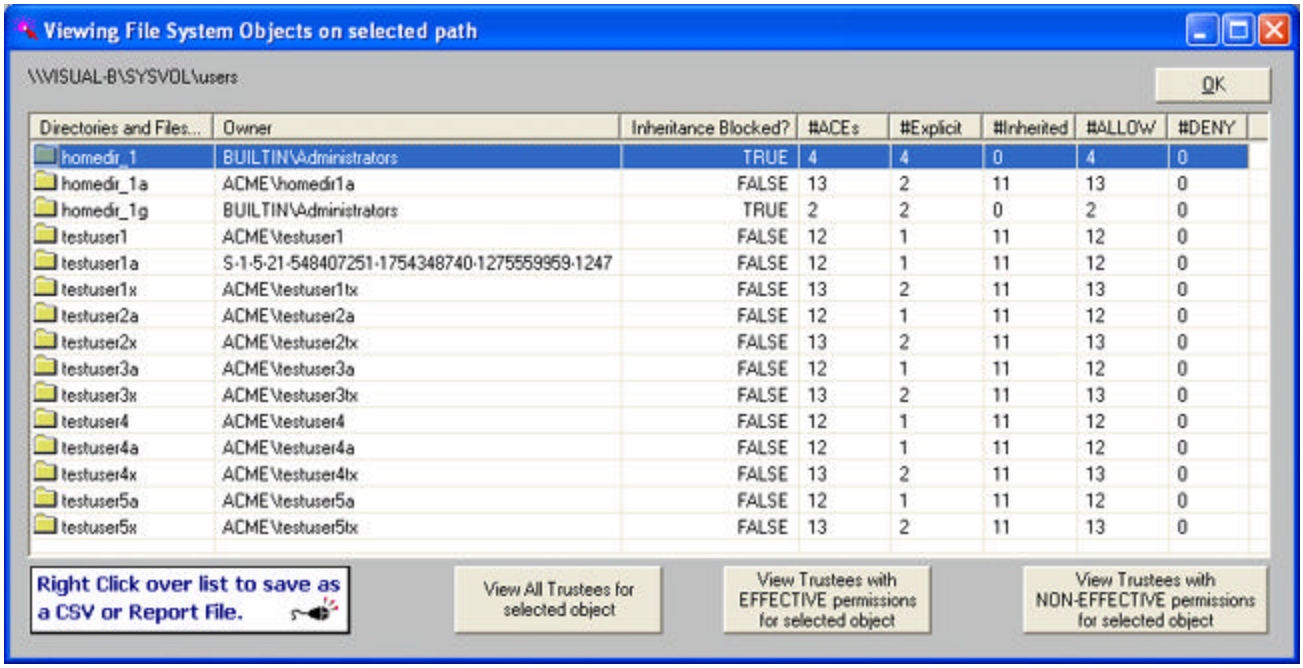
The following sample screen image is from DSRAZOR's ready-to-run applets (`WalkFSACLowner.dsr`). This image shows file system objects (folders and files) including two entries we have expanded to reveal the file system object's owner and trustees (explicit and inherited).



The preceding image is a detailed view of owners and trustees of every file system object.

The following image reveals a summary view of file system folders. The columns indicate if *permission inheritance is blocked*, the number of ACEs, number of ACEs explicitly assigned, number of ACEs inherited, number of ACEs that allow permission and the number that deny permission.

Worldwide: (512) 330 0542 | UK: 0800 814 1318
Email: sales@visualclick.com



The buttons across the bottom open new windows that show the selected level of detail.

Effective permissions are those permissions that apply directly to the file system object listed.

Non-effective permissions are those permissions that do not apply to the listed file system object (for instance, permissions that apply to a “folder only” do not apply to files).

About *Permission Inheritance Blocked*

Both effective and non-effective permissions can be inherited *down* the file system. Inherited permissions are inherited all the way down the file system unless blocked. If blocked, no permissions set ‘above’ the selected folder are inherited or passed on to sub-folders. Files can also be set to block permission inheritance. In the image above you will notice two entries include an inheritance block, further, notice that neither of these entries have any inherited permissions.

When permission inheritance is blocked, only those accounts with explicitly defined permissions will be able to access the blocked folder or file.

If you have any folders and/or files with permission inheritance blocked you may have a problem backing up these objects. Most backup applications logon with a pre-selected account. If this logon account does not have explicit permission assigned to file system objects where permission inheritance is blocked then the backup will not be able to backup these objects.

Note that some backup applications use a kernel-level driver at the server; this type of backup application can backup everything as the kernel-level driver has full access to the file system and cannot be blocked by security permissions.

The screen images shown here are simple examples, DSRAZOR can be customized to provide the documentation you require whether your environment has one million files or hundreds of billions of files.

Solve your file system security documentation requirements *today* with DSRAZOR for Windows!

Worldwide: (512) 330 0542 | UK: 0800 814 1318
Email: sales@visualclick.com