Somarsoft DumpAcl V2.7.5 Help Contents

Send problem reports and comments to info@somarsoft.com.
For information about other Somarsoft products, visit http://www.somarsoft.com on the Internet.

Overview

Somarsoft DumpAcl is a program for Microsoft® Windows NT™ that will dump the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable listbox format, so that holes in system security are readily apparent. Somarsoft DumpAcl also dumps user, group and replication information. Somarsoft DumpAcl is a must-have product for Windows NT systems administrators and computer security auditors.

Windows NT contains the mechanisms for providing strong system security, using permissions to control access to files, registry keys, printers, shares and other securable items and auditing to log successful and failed access attempts. However, it can be very difficult to determine if permissions and audit settings have been set correctly, since there are so many files and registry keys on the typical system. The situation is analogous to having a building with unbreakable locks on each of 10,000 doors. The problem is not with the locks themselves, but rather with one person walking around on a regular basis and checking that none of the 10,000 doors is unlocked.

Somarsoft DumpAcl provides a solution to the problem of too many files and registry keys to check on a regular basis, by producing a concise and readable report of permissions and audit settings. By reviewing this report, you can determine if users have more access to the file system, registry or printers than you want to allow. You can then use file manager, registry editor or print manager to set permissions differently.

Somarsoft DumpAcl is simple enough that it can be used by end-users, after brief training by the network administrator. For example, the manager of the Sales department can be instructed to periodically run Somarsoft DumpAcl against a directory on a file server, containing sales spreadsheets and other files with confidential information, to ensure permissions on these files are set properly.

See Security notes for further general discussion of computer security.

Installation

1) Place `DUMPACL.EXE` and `DUMPACL.HLP` together in any directory.

2) The first time `DUMPACL.EXE` is run, it will create the following registry key:

```
HKEY_CURRENT_USER\SOFTWARE\Somarsoft\DumpAcl
```

3) Somarsoft DumpAcl makes no other changes to your system.

Uninstallation

1) Run `DUMPACL.EXE` with `/u` as a command line parameter. If successful, a message box will be displayed indicating that the `Somarsoft\DumpAcl` registry key has been deleted.

2) Delete `DUMPACL.EXE` and `DUMPACL.HLP` from your computer.

Command Line Options

The command line can contain one of the following:

1) The path of a previously saved report in Somarsoft DumpAcl native file format (*.DCL). The report in the specified file will be loaded and displayed. This type of command line allows opening a previously saved reports by double-clicking in file manager (assuming the DCL suffix has been associated with DUMPACL.EXE).

2) A series of batch command line parameters. Somarsoft DumpAcl can distinguish this type of command line from the preceding by the presence of at least one "/" on the command line. The parameters can be specified in any order.

Required parameters

/rpt=*report type* Type of report to produce:
dir=*drive:\path* Directory permissions report
registry=*hive* Registry permissios report (*hive* can be HKEY_LOCAL_MACHINE or HKEY_USERS)
share=*sharename* Specific shared directory permissions report
allsharedirs All non-special shared directories permissions report
printers Printers permissions report
shares Shares permissions report
users Users report (table format, all fields except groups, groupcomment and grouptype)
groups Groups report (table format, all fields)
policy Policy report
rights Rights report
services Services report

/outfile=*drive:\path* File in which to store report. This file will be replaced if it already exists.

Optional parameters for all reports

/computer=*computer* Computer for which to dump information. Ignored for directory reports (since computer is implied by computer associated with redirected drive). Default is to dump local information.

/saveas=*format* Fomat in which to store report:
native binary format, can be loaded back into Somarsoft DumpAcl
csv comma separated columns
tsv tab separated columns
fixed fixed width columns, padded with blanks
Default is to save as native format.

Optional parameters for permissions reports only

/noowner Do not dump owner. Default is to dump owner.
/noperms Do not dump permissions. Default is to dump permissions.
/showaudit Dump audit info. Default is not to dump audit info. Ignored if audit information cannot be displayed because the current user is not a member of the Administrators group.

(only one of the following options can be specified)
/showexceptions Show directories, registry keys and files whose permissions differ from those of the parent directory or registry key. **This is the default.**
/showalldirs Show all directories and registry keys. Show only those files whose permissions

differ from those of the parent directory.

/showdirsonly Show all directories and registry keys. Do not show any files.

/showall Show all directories, registry keys and files.

Optional parameters for users/groups reports only

/notruelastlogon Do not query all domain controllers for "true" last logon time. Instead use last logon time from specified computer. Default is to query all domain controllers, which can be time consuming.

/nosid Do not dump SID as part of users report. Default is to dump SID, which requires some additional and possible time-consuming processing.

Examples:

```
dumpacl.exe c:\temp\users.dcl
```

Start Somarsoft DumpAcl interactively, load and display a report that was previously saved in native format in `c:\temp\users.dcl`.

```
dumpacl.exe /rpt=dir=c:\users /showaudit /outfile=c:\temp\users.dcl
```

Run Somarsoft DumpAcl batch mode, produce a report of directory permissions for the `c:\users` directory showing owner, permissions and audit settings and store the report in native file format in `c:\temp\users.dcl`. The report will show only those directories and files whose permissions or audit settings differ from those of parent directory.

```
dumpacl.exe /computer=\\server1 /rpt=users /saveas=csv /outfile=c:\temp\users.txt
```

Run Somarsoft DumpAcl in batch mode, produce a report showing all user information in table format for users defined on `\\server1`, and store the report in comma separated columns format in `c:\temp\users.txt.`

```
dumpacl.exe /computer=\\server1 /rpt=share=sales /outfile=c:\temp\users.dcl /showalldirs
```

Run Somarsoft DumpAcl in batch mode, produce a report of permissions for the `\\server1\sales` shared directory, showing owner and permissions but not audit settings, and store the report in native file format in `c:\temp\users.dcl`. The report will show all directories under the `\\server1\sales` tree, and only those files whose permissions differ from those of the parent directory.

Known bugs, limitations and planned enhancements

1) Somarsoft DumpAcl does not indicate whether directory permissions are inheritable. File manager always makes directory permissions inheritable so this is not a severe limitation. That is, of the permissions in the list below, type (b) is always the same as (a), if you used File Manager to set file system permissions:

a) Permission applies to directory itself (Dir column of Somarsoft DumpAcl report)
b) Permission will be inherited by newly created subdirectories in directory (not shown by Somarsoft DumpAcl)
c) Permission will be inherited by newly created files in directory (File column of Somarsoft DumpAcl report)

2) The WIN32 SDK is not clear as to the interpretation of printer access masks and so there are likely bugs in the Somarsoft DumpAcl report for printers. This issue is being worked.

3) There are categories of securable items besides those currently dumped or mentioned above. Some of these categories may be added in the future. User suggestions are welcome.

4) The groups report may be enhanced to show the full user name. Several users have requested this enhancement. There are some issues with implementing this feature that are still under investigation. As a workaround, you can dump both users and groups in table format, export to a database, and join and produce a report in the database.

5) Unless you are a member of the administrators group, find and filter by account may not find all files or other items to which the account has the specified access.

For example, suppose write access is granted to group1 for file1. User1 belongs to group1, but DumpAcl cannot determine the the members of group1, because you do not have sufficient permission (not a member of the administrators or account operators group). Or suppose you cannot even examine the permissions for file 1 (not a member of the administrators or backup operators group). Either way, DumpAcl will not be able to determine that user1 has write access to file1.

If the account specified in the find or filter by account dialog is from a trusted domain, or any of the files or other items have permissions granted to a group from a trusted domain or to a local group which contains users or global groups from a trusted domain, then it is necessary to be administrator on both the local and the trusted domains in order for the find and filter by account to always find all files or other items for which the account has the specified access.

6) DumpAcl attempts to store all information in memory. If you have a large filesystem and specify that permissions are to be reported for all files, or permissions are not set in a consistent and orderly way, so that exception reporting is ineffective, then the amount of information to be stored may exceed available memory. The result will be an out-of-heap space error. You have 3 options at this point:

a) Enable reporting by exceptions at least for files, and possibly for directories as well. Do this using the permissions options dialog.
b) Reset permissions so they are consistent and grouping is therefore effective.
c) Perform multiple dumps, one for each subdirectory of the original directory tree root.

The long range solution is for DumpAcl to store data on disk.

7) When dumping a shared directory on a FAT or CDFS partition, permissions for the root may be different from what file manager shows. This is a fluke in NT.

8) Occasionally DumpAcl hangs due to operating system problems. In particular, there seems to be an intermittent bug in NT with insufficient RPC handles. If DumpAcl hangs and is not using any CPU time

(use performance monitor or pview or qslice from the NT resource kit to verify this) then it is hung inside the operating system, and the problem is probably with NT. If DumpAcl is closed and then restarted, the problem will often disappear.

9) DumpAcl hangs for a minute or so when attempting to resolve permissions involving accounts from trusted domains, if those trusted domains are not currently accessible. This is normal and part of the NT design.

10) The policies report does not show the setting of the "user must logon to change password" policy. Microsoft has not documented how to obtain the setting of this value. As soon as they do, DumpAcl will be enhanced to show it.

Permissions and Audit Settings for File System Entries

The permissions options dialog allows specifying reporting by exception. This is preferred since it greatly reduces the size of the report. (Reporting by exception was called "grouping" in previous versions of DumpAcl). When reporting by exception is specified for both files and directories, only files and directories whose ownership, permissions and/or audit settings differ from those of the parent directory are displayed. When reporting by exception is specified for files only, all directories are displayed and only those files whose owner, permissions and/or audit settings differ from those of the parent directory are displayed.

If not all of owner, permissions and audit settings are selected for display (using the Permissions Options dialog), then only those settings which are displayed are taken into consideration in determining whether a directory or file is exceptional. That is, if only permissions are displayed, and exception reporting is specified for files, then a file is displayed only if its permissions are different from those of the parent directory, regardless of whether the files owner or audit settings are different from those of the parent directory.

Note that ownership implies full control. In order to know who has rights to access a files, it is necessary to know both the owner of the file and the permissions on the file. Thus, it is normally inadvisable to show permissions but not owner. If you are tempted to do this because it makes the report shorter, then you probably have a very misleading organization of permissions. You should investigate why the owners of files are not also given full control over those files by explicit permissions.

The CREATOR OWNER account is ignored in comparisons of permissions, since this pseudo-account is converted to the account of the user who creates a file in a directory.

Dir column (used for directories only)

R	Account can list the contents of the directory.
W	Account can add new files and subdirectories to the directory.
X	Account can traverse the directory as part of a path.
D	Account can delete the entire directory.
P	Account can change permissions for the directory and all files and subdirectories.
O	Account can change ownership of the directory.
All	Same as RWXDPO.
No access	Account is denied all access to directory.

File column (used for directories and files)

For files, this column lists the permissions that apply to the file. For directories, this column lists permissions that will be inherited by files created in the directory, unless the creator of the file explicitly specifies other permissions.

R	Account can read the file.
W	Account can write to the file.
X	Account can execute the file.
D	Account can delete the file.
P	Account can change permissions for the file.
O	Account can change ownership of the file.
All	Same as RWXDPO.
No access	Account is denied all access to file.

Audit settings

R	Audit attempts to read file or list directory contents.

W	Audit attempts to write to file or add files/subdirectories to directory.
X	Audit attempts to execute file or traverse directory as part of a path.
D	Audit attempts to delete file or directory.
P	Audit attempts to change change permissions for the file or directory.
O	Audit attempts to change ownership of the file or directory.
All	Same as RWXDPO audit settings.

See also Special Permissions and Audit Settings.

Example and interpretation:

```
Path (dir and file exceptions)  Account        Own Dir   File  Success Failure

c:\DIR1\                        Administrators  o  all   all
c:\DIR1\                        Everyone           R X   R X
c:\DIR1\                        CREATOR OWNER            all
c:\DIR1\                        SYSTEM             all   all

c:\DIR1\DIR2\File1.txt          Administrators  o        all
c:\DIR1\DIR2\File1.txt          Everyone                 RWXD          all
c:\DIR1\DIR2\File1.txt          SYSTEM                   all
```

All directories and files under `C:\DIR1\` have the same permissions as listed for `C:\DIR1\`, except for file `C:\DIR1\DIR2\MyFile1.txt`. Administrators is owner of these directories and files. Also, failed attempts by anyone to access (read, write, delete, execute, change permissions or take ownership) the `C:\DIR1\DIR2\MyFile1.txt` file are audited.

Permissions and Audit Settings for Registry Keys

Only the HKEY_LOCAL_MACHINE and HKEY_USERS hives can be dumped if a remote computer is specified.

The Key column shows the permissions for the key itself. The Inheritable column shows the permissions that will be inherited by new subkeys created under the key, unless the creator of the subkey explictly specifies other permissions.

The permissions options dialog allows specifying reporting by exception. This is preferred since it greatly reduces the size of the report. (Reporting by exception was called "grouping" in previous versions of DumpAcl). When reporting by exception is specified, only registry keys whose ownership, permissions and/or audit settings differ from those of the parent key are displayed.

If not all of owner, permissions and audit settings are selected for display (using the Permissions Options dialog), then only those settings which are displayed are taken into consideration in determining whether a key has different settings from those of its parent.

Note that ownership implies full control. In order to know who has rights to access a key, it is necessary to know both the owner of the key and the permissions on the key. Thus, it is normally inadvisable to show permissions but not owner. If you are tempted to do this because it makes the report shorter, then you probably have a very misleading organization of permissions. You should investigate why the owners of key are not also given full control over those key by explicit permissions.

The CREATOR OWNER account is ignored in comparisons of permissions, since this pseudo-account is converted to the account of the user who creates a key.

Permissions

Q	Account can query values for the key.
S	Account can create or set values for the key.
C	Account can create sub keys under the key.
E	Account can enumerate sub keys under the key.
N	Account can request notification whenever the key changes.
L	Account can create a registry link.
D	Account can delete the key.
P	Account can change permissions for the key.
O	Account can change the key owner.
R	Account can read the permissions for the key.
Read	Same as QENR permissions.
All	Same as QSCENLDPOR permissions.
No access	Account is denied all access to key.

Audit Settings

Q	Audit attempts to query values for the key.
S	Audit attempts to create or set values for the key.
C	Audit attempts to create sub keys under the key.
E	Audit attempts to enumerate sub keys under the key.
N	Audit attempts to request notification whenever the key changes.
L	Audit attempts to create a registry link.
D	Audit attempts to delete the key.
P	Audit attempts to change permissions for the key.
O	Audit attempts to change the key owner.
R	Audit attempts to read the permissions for the key.

Read	Same as QENR audit settings.
All	Same as QSCENLDPOR audit settings.

See also Special Permissions and Audit Settings.

Example and interpretation:

```
Path                       Account         Own Key        Inheritable

HKEY_CURRENT_USER          SYSTEM              all        all
HKEY_CURRENT_USER          Administrators   o  all        all
HKEY_CURRENT_USER          Frank               all        all

HKEY_CURRENT_USER\Private  Administrators   o  all        all
HKEY_CURRENT_USER\Private  SYSTEM              all        all
```

All keys under HKEY_CURRENT_USER have the same permissions as listed for HKEY_CURRENT_USER except for the HKEY_CURRENT_USER\Private key and its subkeys. The administrators group is owner of all of the keys.

Permissions and Audit Settings for Printers

Permissions

printonly — Account can print to the printer.

managedocs — Account can delete or pause documents for the printer. If this permission is granted to the CREATOR OWNER pseudo-account, then users have permission to manage their own print documents. Users can manage the documents of other users only if they are members of a group other than CREATOR OWNER which has the ManageDocs permission for the printer.

all — Account can print to the printer, manage documents, delete the printer, change permissions for the printer, and change ownership of the printer.

no access — Account is denied all access to printer.

Audit Settings

U — Audit attempt to use printer.

A — Audit attempt to administer printer.

D — Audit attempt to delete printer.

P — Audit attempt to change permissions.

O — Audit attempt to change ownership.

All — Same as UADPO audit settings.

See also Special Permissions and Audit Settings.

Example and interpretation:

```
Printer         Account         Own Permission  Success   Failure

Laser           CREATOR OWNER       managedocs
Laser           Administrators   o  all
Laser           Everyone            print                 all
Laser           Power Users         managedocs
```

All users can print to the printer named Laser, and can manage the documents they print. Power Users can print and manage the documents of other users. Administrators can perform all printer functions, including deleting the printer and changing permissions and ownership. Administrators is owner of the printer. Failed attempts by any user to access the printer (print, manage documents, delete, change permissions or take ownership) are audited.

Permissions for Shares

Shares do not have an owner or audit settings. Some shares do not have DACL

Permissions for file shares

read — Account can read the shared directory and it subdirectories and files.

change — Account can read and write the shared directory and it subdirectories and files, including adding and deleting subdirectories and files.

all — Account can read, write, change permissions on and change ownership of the shared directory and it subdirectories and files.

no access — Account is denied all access to shared directory and its subdiretories and files

See also Special Permissions and Audit Settings.

Example:

```
Path                               Account           Permission

C$=C:\ (special admin share)                         admin-only (null dacl)

C_DRIVE=C:\ (disktree)             Administrators    all

temp=C:\temp (disktree)            Group1            no access
temp=C:\temp                       Group2            change
temp=C:\temp                       Everyone          read
```

Special Permissions and Audit Settings

axhhhhhhh — Non-standard allow permissions or audit settings, see WIN32 SDK documentation.

dxhhhhhhh — Non-standard deny permissions, see WIN32 SDK documentation.

==>access denied — User who is executing Somarsoft DumpAcl cannot read the permissions or audit settings.

unprotected (no dacl)
unprotected (null dacl) — No DACL was present or DACL was Null, both of which situations are equivalent to "all" permission for Everyone. It is normal for shares to be initially created with a null DACL. Also, directories and files on the volumes formatted with the FAT filesystem have no DACLs. Directories and files created on the volumes formatted with the NTFS filesystem normally have a DACL; however, it is possible for an ACL editing program to remove this DACL.

admin-only (no dacl) — This permission only applies to administrator shares (ADMIN$, C$, D$, E$, etc). These shares are automatically created by the operating system. These shares were originally required for compatibility with Lan Manager. The operating system only allows administrator to use these shares. This restriction to administrators is not performed by DACLs, but is internal to the operating system.

Ownership

The owner of a securable item is indicated by an "o" in the Own column when the Show Owner option is selected. Shares do not have an owner.

When Reporting by exceptions is specified, Somarsoft DumpAcl takes ownership into consideration in attemping to group items. Two items with the same permissions but different owners are considered to have equivalent settings provided the owners have explicit permission to change permissions or take ownership of their respectively owned item (i.e. other than as a consequence of being the owner).

Example and interpretation:

(reporting by exception disabled, or enabled and John and Mary NOT both members of Managers group):

```
Path                             Account         Own Dir        File

c:\Dir\                          John             o
c:\Dir\                          Managers            all        all

c:\Dir\File                      Mary             o
c:\Dir\File                      Managers            all        all
```

(reporting by exception and John and Mary both members of Managers group):

```
Path                             Account         Own Dir        File

c:\Dir\                          John             o
c:\Dir\                          Managers            all        all
```

(i.e. `c:\Dir\File` not shown because it was "grouped" with its parent directory).

In this example, permissions are the same for the file and directory, but ownership differs. If John and Mary are members of the Managers group, then John can take ownership and change permissions on the `c:\Dir\` directory and Mary can take ownership and change permissions on the `c:\Dir\File` file (because All permission allows taking ownership). Therefore, Somarsoft DumpAcl considers the file to have equivalent effective permissions as the parent directory, and so it is not displayed.

Ownership is important because the owner of an item can always set permissions for that item. If Mary were not a member of the Manager group, she could still change permissions on the `c:\Dir\File` file at any time, and thereby obtain access to information that someone thought was only available to Managers. Likewise, if John were not a member of the Manager group, he could still change permissions on the `c:\Dir\` directory at any time to give himself full control (via inheritance) of newly created files in this directory, that one might think (if looking only at the permissions on the directory) would only be available to Managers.

Miscellaneous Notes

1) Computer accounts shown in the users reports are those with UserName ending in "$". A computer account is needed for a workstation to join a domain. There is a password associated with computer accounts. This password is automatically changed and kept in sync between the domain controller and the workstation. If the passwords get out of sync, users at the workstation won't be able to log onto the domain. Fix this problem by removing the workstation from the domain and then adding it back.

2) The account shown on the Services report is the account under which the service runs. It is usually a good idea to run as many Win32 services as possible under ordinary user accounts, instead of LocalSystem. Many Unix breakins have occurred due to bugs in daemons (equivalent to Windows NT services) running under the root account (equivalent to LocalSystem).

3) Information about users authorized to access the server using RAS can be obtained using the RASUSERS.EXE utility in the NT3.5 resource kit.

4) Windows NT only stored the last logon time on the authenticating logon server. So, if there are two or more domain controllers (primary plus one or more backups), it is necessary to access all controllers and use the latest of the last logon times reported. The Dump Users reports have an option to enable or disable this scanning. The scanning is normally enabled, but you might disable it if you want to compare the last logon times among the different controllers, for some reason.

Permissions reporting for enterprises

Somarsoft DumpAcl can be used interactively to perform security auditing of a single computer. For larger enterprise type networks, the following techniques might be useful.

Set up a batch job to run Somarsoft DumpAcl at night to dump information for computers on the network. Domain User/Group info need only be dumped once (from a primary or backup domain controller). A typical batch job might look like:

```
dumpacl /rpt=users /computer=server1 /outfile=c:\dumpacl\users.dcl
dumpacl /rpt=groups /computer=server1 /outfile=c:\dumpacl\groups.dcl
dumpacl /rpt=allsharedirs /computer=server1 /outfile=c:\dumpacl\server1.dcl
dumpacl /rpt=allsharedirs /computer=server2 /outfile=c:\dumpacl\server2.dcl
dumpacl /rpt=allsharedirs /computer=server3 /outfile=c:\dumpacl\server3.dcl
```

A security auditor can later use the File'Load Native File and File'Load Multiple Native Files options to load the output files into DumpAcl for review. The Load Multiple Native Files option, combined with the Find/Filter by Account option is particularly useful for answering questions like "*show me all the files to which user xxx has write permission, and do this for all servers on the network*".

The batch job can be run under an administrator account. The output files can later be loaded into DumpAcl by a security auditor who does not have administrator privileges. However, the Find/Filter by account options may not work correctly if DumpAcl is being run under an account that is not an administrator. This is because administrator privilege is needed to find the groups to which the specified account belongs. If the Find/Filter is for the Everyone group, then this is not an issue, since no user to group mapping is required in this case.

Copyright/License/Warranty Disclaimer

Send problem reports and other comments to info@somarsoft.com.

You should carefully read the following terms and conditions before using this software. Use of this software indicates your acceptance of these terms and conditions. If you do not agree with them, do not use the software.

License Agreement

This is not free software. You are hereby licensed to: use the Shareware Version of the software for a 30 day evaluation period; make as many copies of the Shareware version of this software and documentation as you wish; give exact copies of the original Shareware version to anyone; and distribute the Shareware version of the software and documentation in its unmodified form via electronic means. There is no charge for any of the above.

You are specifically prohibited from charging, or requesting donations, for any such copies, however made; and from distributing the software and/or documentation with other products (commercial or otherwise) without prior written permission, with one exception: Disk Vendors approved by the Association of Shareware Professionals are permitted to redistribute Somarsoft DumpAcl, subject to the conditions in this license, without specific written permission.

You are specifically prohibited from copying or redistributing the keyfile (`DUMPACL.KEY`) that will be sent to you upon receipt of your registration payment.

Unregistered use of Somarsoft DumpAcl after the 30-day evaluation period is in violation of United States and International copyright laws.

A single registered copy of Somarsoft DumpReg can only be installed/executed on a single computer by a single-user. If you install Somarsoft DumpReg on a workstation and that workstation is used by multiple users, then you must have a license for each of those users. If you install Somarsoft DumpReg on a file server and execute it over the network from remote workstations, then you must have a license for the greater of the number of remote workstations or number of users who use these remote workstations.

There is no license required for dumping the registry for remote computers, using the Select Computer capability. Thus, if you have 3 administrators who will be running the program, and these administrators share 2 administrator workstations, and there are 100 user workstations and 5 servers and you run Somarsoft DumpReg at the administrator workstations and remotely dump the servers and user workstations, then you need 3 licenses (because there are 3 users). If you run Somarsoft DumpReg locally at all workstations and servers, then you would need 107 licenses.

Site/organization licenses are available. A site/organization license license gives you the right to use the software on a unlimited number of computers belonging to a single organization (corporation, government agency, etc). Visit http://www.somarsoft.com/ordering.htm for pricing.

Upon receipt of your registration payment, you will be sent a key file (`DUMPACL.KEY`), which is to be placed in the same directory as `DUMPACL.EXE`. This key file will be your proof of registration. The presence of this key file will enable certain functions of Somarsoft DumpAcl which are disabled in the unregistered version. These functions involve the ability to produce hardcopy printouts of the Somarsoft DumpAcl report.

For how to register and pay for Somarsoft DumpAcl, see Order form.

Note that Somarsoft reserves the right to increase the registration fee at any time without notice. If the fee has been increased, and your payment is received after such increase, then Somarsoft has the right to require additional payment before accepting your registration and sending you a key file. Once you have paid the then current registration fee, and Somarsoft has accepted your fee and sent you a key file, you have the right to use the version of Somarsoft DumpAcl that you paid for, for as long as you want, without additional payment. Future versions of Somarsoft DumpAcl may require a different key file. You may be required to pay an additional fee to upgrade to such future versions.

Governing Law

This agreement shall be governed by the laws of the state of California.

Disclaimer of Warranty

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OF MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the varying hardware/software environments in which Somarsoft DumpAcl may be used, THERE IS NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

Good data processing procedure dictates that any program be thoroughly tested with non-critical data before relying on it. The user must assume the entire risk of using hte program. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

Order Form - Somarsoft DumpAcl V2.7.5

Current Somarsoft voice/fax numbers, hardcopy mail address and up-to-date ordering instructions including current prices are available at http://www.somarsoft.com/ordering.htm or via email from info@somarsoft.com. This information is not included here because it may change from year to year.

You can register and pay for Somarsoft DumpAcl by 4 methods:

VISA/Mastercard/AMEX credit card. Send this form via hardcopy mail or fax, or send information via email (you must accept risks of eavesdropping on email), or place order by voice phone. The credit card company will handle currency conversions, for customers outside the US.

Check in US dollars drawn on a US bank, payable to Somarsoft. Send with this form via hardcopy mail.

International money order in US dollars, payable to Somarsoft. Send with this form via hardcopy mail. International money orders are available at the Post Office, banks, etc.

CompuServe registration service (GO SWREG, specify ID 2723). Charge will appear on your CompuServe monthly statement. Key file will be sent via email only.

When your registration payment is received, you will be sent a key file (DUMPACL.KEY) via email (SMTP MIME or CompuServe attachment). This key file will be your proof of license and will contain your registration name (see below) in encrypted format. When a valid key file is properly installed, the registration name will will appear in the Help'About dialog box and all functions of Somarsoft DumpAcl will be enabled. Optionally, you can also have a 3.5" diskette shipped via hardcopy airmail, containing the keyfile and most recent version of the software.

____ single-user licenses = ______

organization license of type __________________________ = ______

Current California sales tax (8.5%) = ______
(not applicable if key file sent via email only or
if shipping address not in California, USA)
Airmail shipping and handling = ______
(not applicable if key file sent via email only)

Pay by: Check Visa Mastercard AMEX Total = ______

Credit card #: ___________________________________ Exp date: ______

Card owner signature: ____

Registration name: ____
(name that will appear in the key file, normally a company name)

Email address: ____

Voice: __________________________ Fax: ____________________________

Shipping address (include country if outside USA):

____

____

____

Security notes

What is security?

A secure system is one that is protected against various natural disasters and human attacks. Security with respect to a computer system is very similar to security with respect to a bank vault. A computer system or bank vault containing valuables (data in the case of a computer system, secret documents or jewels in the case of bank vault) is secure if:

1) No one can look at, modify or remove any of the valuables for which they do not have the proper authority. In the computer context, this requires:

> Permissions are set properly.
> Computer is physically secured, possibly inside a locked room.
> Data is encrypted if computer cannot be physically secured (e.g. portable PC).
> Backup tapes are physically secured in a safe, or else encrypted.
> Viruses and trojan horses do not get introduced into the system.

2) No person or natural disaster such as a fire can easily destroy the valuables. In the computer context, this requires:

> Permissions are set properly.
> Backups are performed regularly.
> Copies of backup tapes are stored offsite.
> Viruses and trojan horses do not get introduced into the system.

3) No one can easily disrupt authorized access to the valuables (denial of service). In the computer context, this requires:

> Permissions are set properly.
> Viruses and trojan horses do not get introduced into the system.

An example of disrupting authorized use of a computer system is a virus that modifies and thereby corrupts the registry so a database program will not run. The database itself maybe intact (because it was protected by permissions), but the data cannot be accessed until the registry is repaired, which may require reinstalling the database program. This temporary disruption can be as costly as actual loss of data for many mission critical computer systems.

Note the importance of *permissions* and *viruses/trojan horses*, which are implicated in all types of security risks. Permissions are the primary protection against malicious users and viruses and trojan horses which run under user accounts. There is no way to protect against viruses and trojan horses which run under administrator or system accounts. So it is very important to avoid running untrusted programs when logged on as an administrator, or to allow untrusted program to be run as services under a system or administrator account.

What should a well-organized set of permissions look like?

A well-organized set of permissions will produce a short Somarsoft DumpAcl report. In general, the shorter the report produced by Somarsoft DumpAcl, the easier to understand, and so the more confident the systems administrator will be that permissions have been set properly.

Issue of registry key permissions

Use Somarsoft DumpAcl to produce a report of the HKEY_LOCAL_MACHINE registry hive. Note that Everyone has write and delete access to many keys. So any user who can access the registry locally or remotely can make changes that might disrupt system operations.

Consider the following scenario. A student in an undergraduate university computer lab logs on using another student's account (they found the other students password written in the front cover of that students notebook) and makes various changes to the registry of workstations and servers in the lab so that these computers no longer function properly, but the malfunction is so intermittent and obscure that only an expert systems administrator would be able to trace the problem to the registry. Since the damage was done using another user's account, there would be no way to identify the true perpetrator. The only way to correct the damage will be to reinstall NT, but then the perpetrator will just come back and break the system again. Undergraduate students are notorious for finding such mischief a great source of amusement, and having plenty of time on their hands to engage in it.

It is possible to disable remote connection to the registry by removing the read access for Everyone to the root key of HKEY_LOCAL_MACHINE. Do NOT propagate the resulting permissions to subkeys. This may or may not cause problems with services running on the local machine. It is easy to reverse this change, however, if you experience problems. The long-term solution is for there to be an explicit way to disable remote connections to the registry. And the default for a newly installed NT server should be for remote connections to be disabled (just as the Guest account is disabled by default). Since ordinary users cannot normally logon to an NT server locally, the registry is protected by disabling remote connections.

More info about security

Visit the Somarsoft Web site at http://www.somarsoft.com for a further discussion of computer security issues.

A useful security technique

Suppose you want users to be able to access a file through a program, but not directly (i.e. not by using file manager, file open dialog or the command line). For example, suppose you are writing a Visual Basic program that will run on client machines and update an Access or similar shared file database on a file server. You must give all users who will run the program write access to the database file, but you do not want the users to modify the database other than using the Visual Basic program. To do this set up directories and permissions as follows:

`\HIDE1\`	(no access permission for everyone)
`\HIDE1\DBXXX.MDB`	(read/write permission for everyone)

Users cannot even list the files in the `HIDE1` directory, and so will be unable to access the `DBXXX.MDB` file using file manager or the file open dialog box. They also won't be able to easily determine the name of this file (it should have an obscure name) and so won't be able to copy or delete it using the command prompt. Programs executed by users can access the `DBXXX.MDB` file, provided these programs specify the full file path during the open.

The feature of NT which makes this technique possible is called the Bypass Traverse Checking user right. You can disable this feature using User Manager. Bypass Traverse Checking causes NT to behave differently from Unix. In Unix (and NT when Bypass Traverse Checking is disabled), a program must have list permission for all directories in the path, as well as the appropriate permission on the file being opened.

This technique is vulnerable to users who know how to program in any language, including Basic. For better but also more complex security, use a client server design, where the client executed by the user communicates via RPC or other methods with a service running under a privileged account. Files can then be protected using normal permissions.

Internet Security

While this topic is not strictly related Somarsoft DumpAcl, it is a topic of great current interest and not completely addressed in the Microsoft documentation.

If a Windows machine is directly connected to the Internet, and is running TCP/IP, then remote users can establish SMB network connections to that machine, provided they know or can guess the password of an account. (Note: SMB network connection are used for Windows file/print sharing. SMB networking is not discussed in the standard Unix oriented Internet security literature). If the guest account is enabled, then no password is required for the remote user to logon. Such a remote user can then modify files on shared directories, print to shared printers, manipulate the registry, and access any of the myriad of poorly documented Windows functions which are RPC enabled. Such a remote user could cause great havoc, in other words.

One solution to this problem is to disable the guest account on all machines accessible from the Internet, and then establish strong passwords on remaining accounts. Also, policies could be set to disable these accounts after a limited number of failed logins, to avoid the possibility of a remote user running an automated program to attempt to logon. NT does not allow limiting failed login for the Administrator account (to avoid denial of service attacks) and so this account could be renamed, which would require the remote user to guess both the name and password instead of password alone.

A more secure solution is to disable SMB networking over the Internet altogether. One way to accomplish this is by blocking TCP/IP and UDB ports 137 to 139 on the router to the Internet. Another way is to disabling the binding between the SMB services (NetBios, Server and Workstation in NT) TCP/IP transport on the interface which is connected to the Internet (Network card or RAS connection). These bindings can be disabling using Control Panel in NT.

The secure way to connect a small NT network to the internet is as follows:

Internet	<->	Router with:	<->	NT gateway machine with:	<->	Internal network
		SMB filtering - TCP/IP and UDB ports 137 - 139 (prevents attacks against gateway machine from Internet)		IP routing disabled (prevents direct Internet access to internal network).		NT, Windows 95 and other machines, running TCP/IP.
				Application level proxy firewall (allows safe access to Internet from internal network).		
				Properly configured Web, Mail, DNS and other servers to which both internal and external Internet users should have access.		