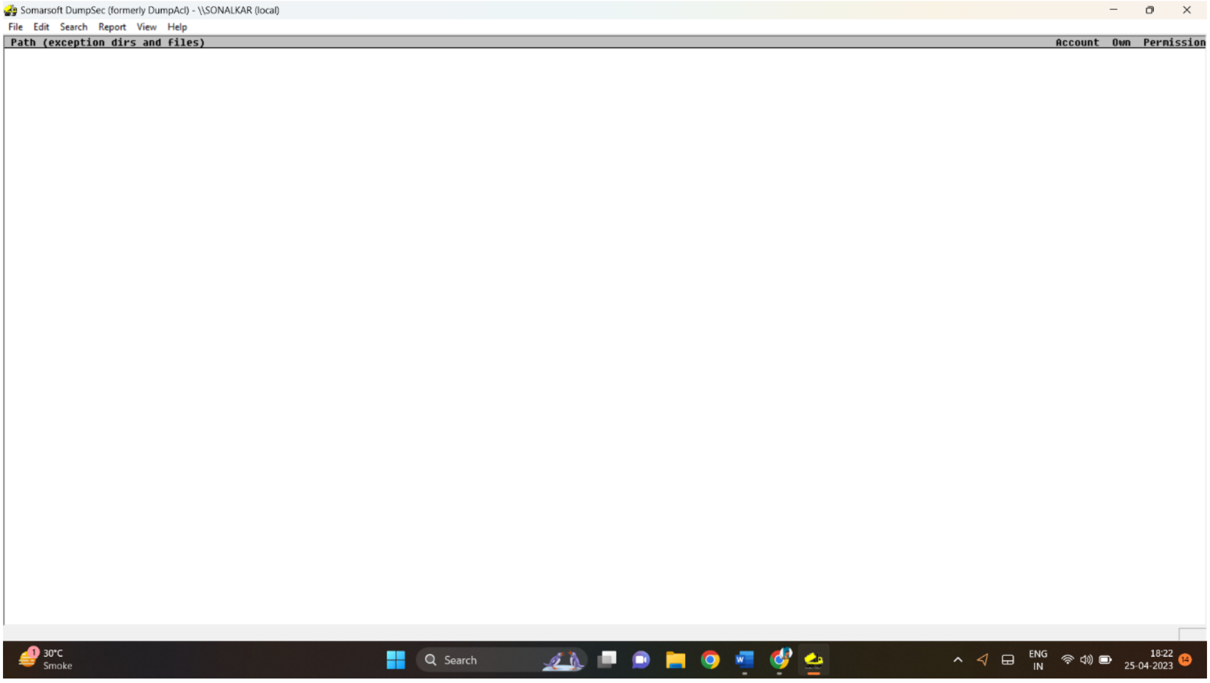
Dumpsec

DumpSec is a security auditing program for Microsoft Windows. It dumps the permissions and audit settings for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information.

Security experts use these kinds of resources to identify and fix security holes or weaknesses in systems. These tools assist those who work for legitimate businesses trying to build security into established IT systems, against the efforts of various hackers and black hat developers trying to exploit vulnerabilities in a system.

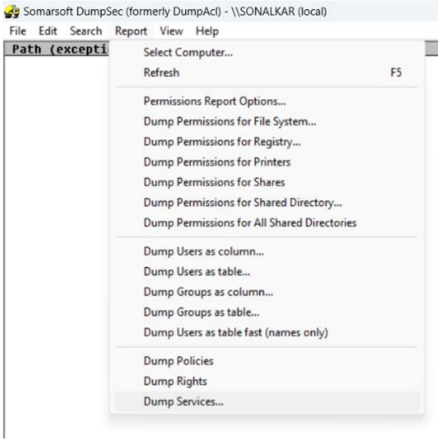
Home Page:

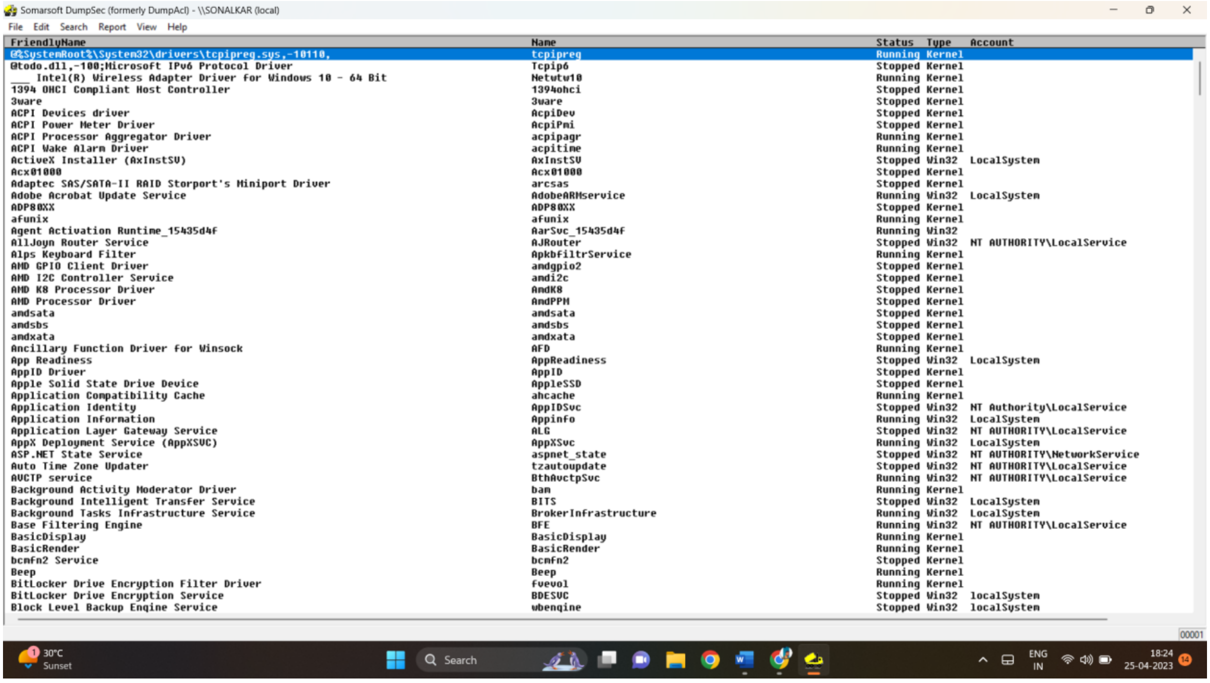

Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Path (exception dirs and files)
Account Own Permission
30°C
Smoke
Search
ENG
IN
18:22
25-04-2023

Go to reports and dump whatever you want

1. Dump Services:

We can see all the services in our computer and whether it is running or stopped. We can see the type also whether it is in kernel or windows. We can also see the account.

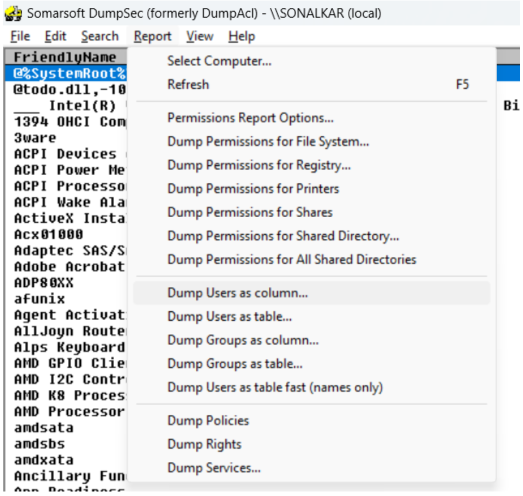

Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Path (excepti
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...


Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
00001
30°C
Sunset
Search
ENG
IN
18:24
25-04-2023

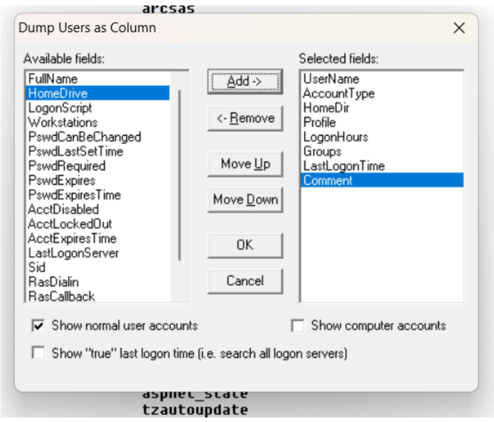
```
FriendlyName                                                  Name                    Status  Type   Account
@%SystemRoot%\System32\drivers\tcpipreg.sys,-10110,           tcpipreg                Running Kernel
@todo.dll,-100;Microsoft IPv6 Protocol Driver                 Tcpip6                  Stopped Kernel
___ Intel(R) Wireless Adapter Driver for Windows 10 - 64 Bit  Netwtw10                Running Kernel
1394 OHCI Compliant Host Controller                           1394ohci                Stopped Kernel
3ware                                                         3ware                   Stopped Kernel
ACPI Devices driver                                           AcpiDev                 Stopped Kernel
ACPI Power Meter Driver                                       AcpiPmi                 Stopped Kernel
ACPI Processor Aggregator Driver                              acpipagr                Running Kernel
ACPI Wake Alarm Driver                                        acpitime                Running Kernel
ActiveX Installer (AxInstSV)                                  AxInstSV                Stopped Win32  LocalSystem
Acx01000                                                      Acx01000                Stopped Kernel
Adaptec SAS/SATA-II RAID Storport's Miniport Driver           arcsas                  Stopped Kernel
Adobe Acrobat Update Service                                  AdobeARMservice         Running Win32  LocalSystem
ADP80XX                                                       ADP80XX                 Stopped Kernel
afunix                                                        afunix                  Running Kernel
Agent Activation Runtime_15435d4f                             AarSvc_15435d4f         Running Win32
AllJoyn Router Service                                        AJRouter                Stopped Win32  NT AUTHORITY\LocalService
Alps Keyboard Filter                                          ApkbfiltrService        Running Kernel
AMD GPIO Client Driver                                        amdgpio2                Stopped Kernel
AMD I2C Controller Service                                    amdi2c                  Stopped Kernel
AMD K8 Processor Driver                                       AmdK8                   Stopped Kernel
AMD Processor Driver                                          AmdPPM                  Stopped Kernel
amdsata                                                       amdsata                 Stopped Kernel
amdsbs                                                        amdsbs                  Stopped Kernel
amdxata                                                       amdxata                 Stopped Kernel
Ancillary Function Driver for Winsock                         AFD                     Running Kernel
App Readiness                                                 AppReadiness            Stopped Win32  LocalSystem
AppID Driver                                                  AppID                   Stopped Kernel
Apple Solid State Drive Device                                AppleSSD                Stopped Kernel
Application Compatibility Cache                               ahcache                 Running Kernel
Application Identity                                          AppIDSvc                Stopped Win32  NT Authority\LocalService
Application Information                                       Appinfo                 Running Win32  LocalSystem
Application Layer Gateway Service                             ALG                     Stopped Win32  NT AUTHORITY\LocalService
AppX Deployment Service (AppXSVC)                             AppXSvc                 Running Win32  LocalSystem
ASP.NET State Service                                         aspnet_state            Stopped Win32  NT AUTHORITY\NetworkService
Auto Time Zone Updater                                        tzautoupdate            Stopped Win32  NT AUTHORITY\LocalService
AVCTP service                                                 BthAvctpSvc             Running Win32  NT AUTHORITY\LocalService
Background Activity Moderator Driver                          bam                     Running Kernel
Background Intelligent Transfer Service                       BITS                    Stopped Win32  LocalSystem
Background Tasks Infrastructure Service                       BrokerInfrastructure    Running Win32  LocalSystem
Base Filtering Engine                                         BFE                     Running Win32  NT AUTHORITY\LocalService
BasicDisplay                                                  BasicDisplay            Running Kernel
BasicRender                                                   BasicRender             Running Kernel
bcmfn2 Service                                                bcmfn2                  Stopped Kernel
Beep                                                          Beep                    Running Kernel
BitLocker Drive Encryption Filter Driver                      fvevol                  Running Kernel
BitLocker Drive Encryption Service                            BDESVC                  Stopped Win32  localSystem
Block Level Backup Engine Service                             wbengine                Stopped Win32  localSystem
```

2. Dump Users:

It will return Username, Account Type, Profile, Groups, etc. We can arrange in columns as well as Tables.



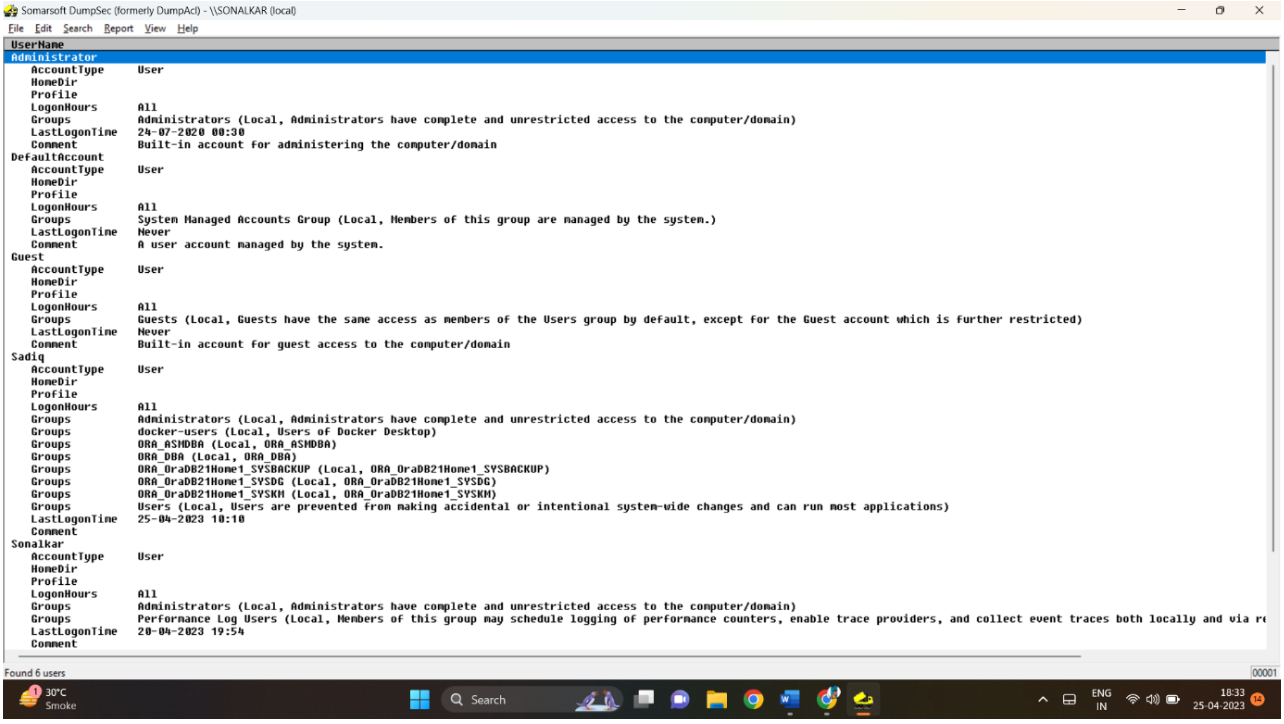
We can select want we want to see



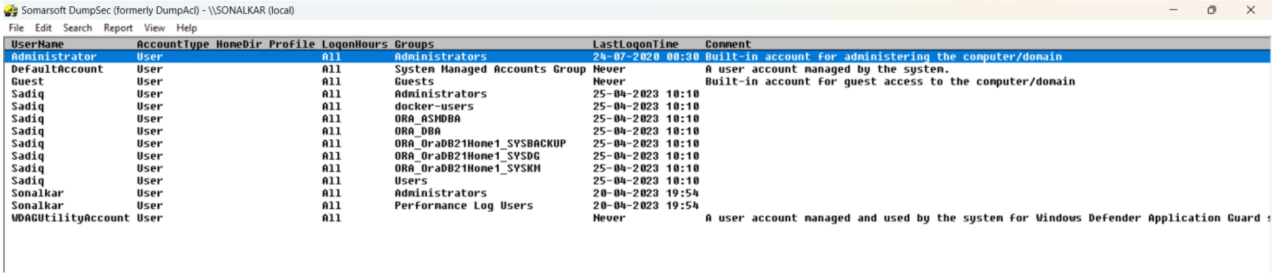
Available fields:
FullName
HomeDrive
LogonScript
Workstations
PswdCanBeChanged
PswdLastSetTime
PswdRequired
PswdExpires
PswdExpiresTime
AcctDisabled
AcctLockedOut
AcctExpiresTime
LastLogonServer
Sid
RasDialin
RasCallback

Selected fields:
UserName
AccountType
HomeDir
Profile
LogonHours
Groups
LastLogonTime
Comment

☑ Show normal user accounts
□ Show computer accounts
□ Show "true" last logon time (i.e. search all logon servers)


Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Found 6 users
00001
30°C
Smoke
Search
ENG
IN
18:33
25-04-2023

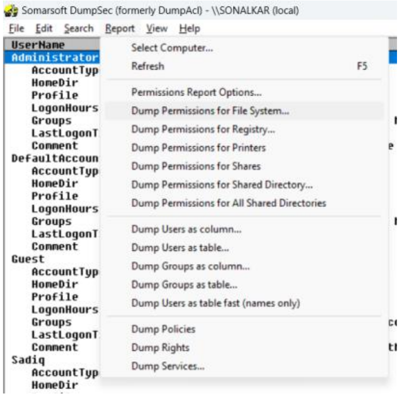
```
UserName
Administrator
   AccountType     User
   HomeDir
   Profile
   LogonHours      All
   Groups          Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)
   LastLogonTime   24-07-2020 00:30
   Comment         Built-in account for administering the computer/domain
DefaultAccount
   AccountType     User
   HomeDir
   Profile
   LogonHours      All
   Groups          System Managed Accounts Group (Local, Members of this group are managed by the system.)
   LastLogonTime   Never
   Comment         A user account managed by the system.
Guest
   AccountType     User
   HomeDir
   Profile
   LogonHours      All
   Groups          Guests (Local, Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted)
   LastLogonTime   Never
   Comment         Built-in account for guest access to the computer/domain
Sadiq
   AccountType     User
   HomeDir
   Profile
   LogonHours      All
   Groups          Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)
   Groups          docker-users (Local, Users of Docker Desktop)
   Groups          ORA_ASMDBA (Local, ORA_ASMDBA)
   Groups          ORA_DBA (Local, ORA_DBA)
   Groups          ORA_OraDB21Home1_SYSBACKUP (Local, ORA_OraDB21Home1_SYSBACKUP)
   Groups          ORA_OraDB21Home1_SYSDG (Local, ORA_OraDB21Home1_SYSDG)
   Groups          ORA_OraDB21Home1_SYSKM (Local, ORA_OraDB21Home1_SYSKM)
   Groups          Users (Local, Users are prevented from making accidental or intentional system-wide changes and can run most applications)
   LastLogonTime   25-04-2023 10:10
   Comment
Sonalkar
   AccountType     User
   HomeDir
   Profile
   LogonHours      All
   Groups          Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)
   Groups          Performance Log Users (Local, Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via re
   LastLogonTime   20-04-2023 19:54
   Comment
```


Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help

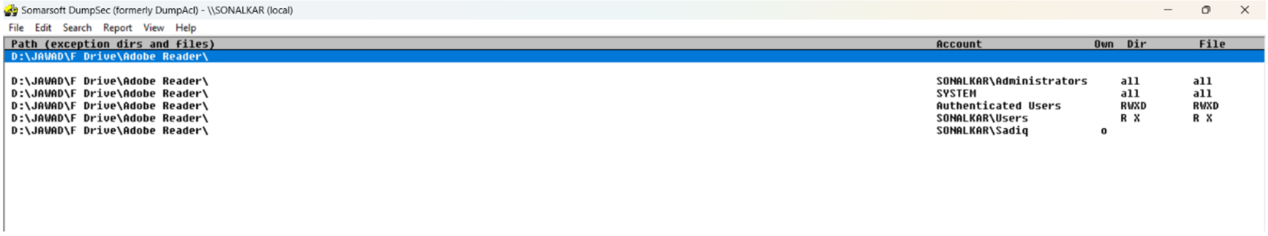
```
UserName          AccountType HomeDir Profile LogonHours Groups                        LastLogonTime    Comment
Administrator     User                        All        Administrators                24-07-2020 00:30 Built-in account for administering the computer/domain
DefaultAccount    User                        All        System Managed Accounts Group Never            A user account managed by the system.
Guest             User                        All        Guests                        Never            Built-in account for guest access to the computer/domain
Sadiq             User                        All        Administrators                25-04-2023 10:10
Sadiq             User                        All        docker-users                  25-04-2023 10:10
Sadiq             User                        All        ORA_ASMDBA                    25-04-2023 10:10
Sadiq             User                        All        ORA_DBA                       25-04-2023 10:10
Sadiq             User                        All        ORA_OraDB21Home1_SYSBACKUP    25-04-2023 10:10
Sadiq             User                        All        ORA_OraDB21Home1_SYSDG        25-04-2023 10:10
Sadiq             User                        All        ORA_OraDB21Home1_SYSKM        25-04-2023 10:10
Sadiq             User                        All        Users                         25-04-2023 10:10
Sonalkar          User                        All        Administrators                20-04-2023 19:54
Sonalkar          User                        All        Performance Log Users         20-04-2023 19:54
WDAGUtilityAccount User                       All                                      Never            A user account managed and used by the system for Windows Defender Application Guard s
```

3. Dump Permissions for file system:

This only scans the folder it won’t scan for text file or etc. We can see the account, owner, directory and the file. R- Read, W- Write, X- Execute, D- Delete.

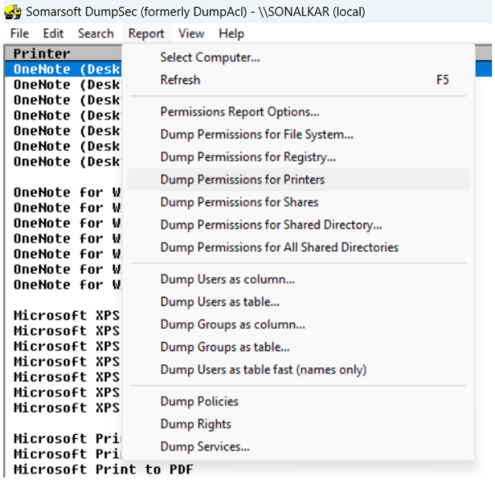

Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...

```
UserName
Administrator
   AccountTyp
   HomeDir
   Profile
   LogonHours
   Groups
   LastLogonT
   Comment
DefaultAccoun
   AccountTyp
   HomeDir
   Profile
   LogonHours
   Groups
   LastLogonT
   Comment
Guest
   AccountTyp
   HomeDir
   Profile
   LogonHours
   Groups
   LastLogonT
   Comment
Sadiq
   AccountTyp
   HomeDir
```


Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help

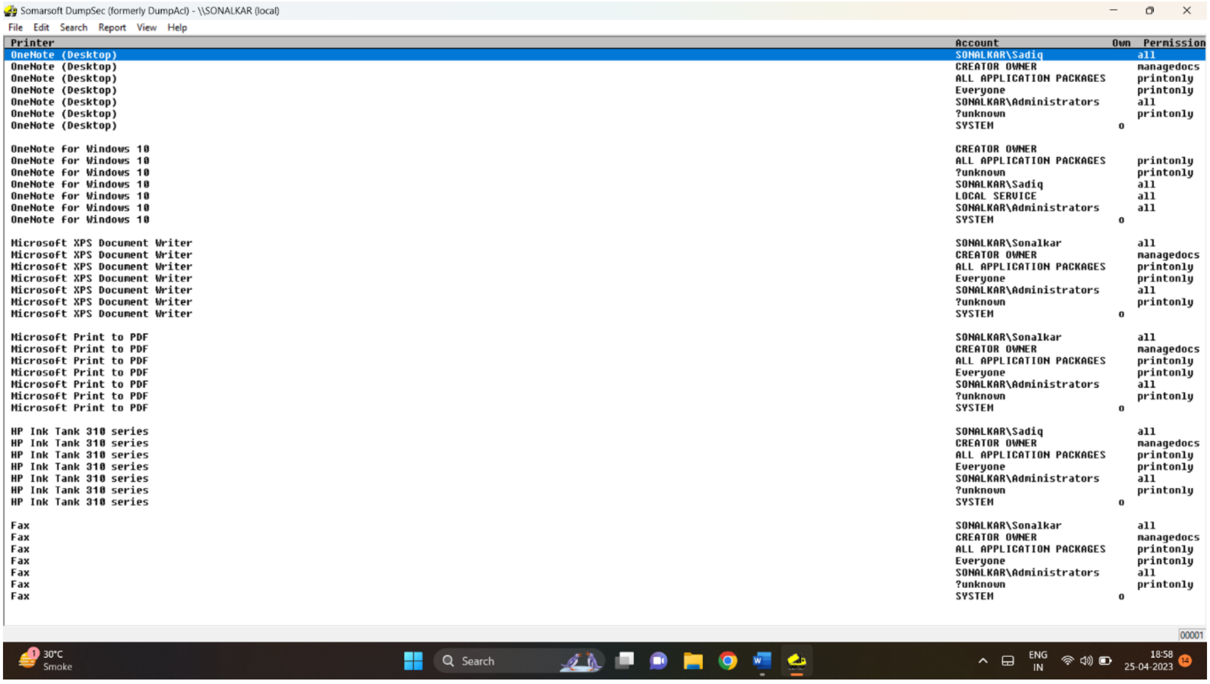
```
Path (exception dirs and files)                                                      Account                   Own  Dir     File
D:\JAWAD\F Drive\Adobe Reader\

D:\JAWAD\F Drive\Adobe Reader\                                                       SONALKAR\Administrators        all     all
D:\JAWAD\F Drive\Adobe Reader\                                                       SYSTEM                         all     all
D:\JAWAD\F Drive\Adobe Reader\                                                       Authenticated Users            RWXD    RWXD
D:\JAWAD\F Drive\Adobe Reader\                                                       SONALKAR\Users                 R X     R X
D:\JAWAD\F Drive\Adobe Reader\                                                       SONALKAR\Sadiq            o
```

4. Dump Permission for Printer:



Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...

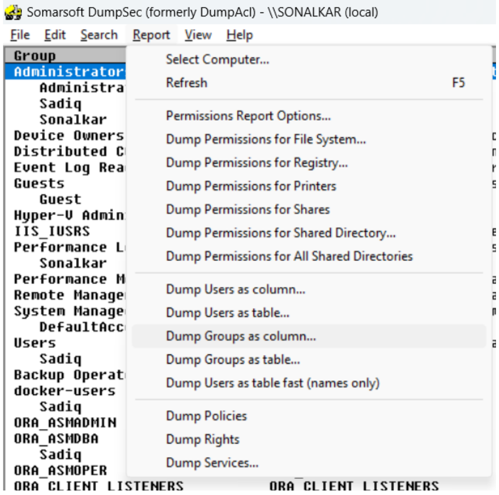
```
Printer
OneNote (Desk
OneNote (Desk
OneNote (Desk
OneNote (Desk
OneNote (Desk
OneNote (Desk
OneNote (Desk

OneNote for W
OneNote for W
OneNote for W
OneNote for W
OneNote for W
OneNote for W
OneNote for W

Microsoft XPS
Microsoft XPS
Microsoft XPS
Microsoft XPS
Microsoft XPS
Microsoft XPS
Microsoft XPS

Microsoft Pri
Microsoft Pri
Microsoft Print to PDF
```



Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
00001
30°C
Smoke
Search
ENG
IN
18:58
25-04-2023
14

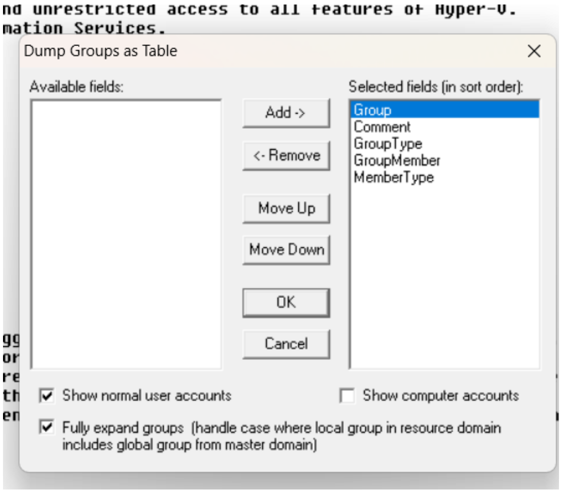
```
Printer                          Account                      Own  Permission
OneNote (Desktop)                SONALKAR\Sadiq                    all
OneNote (Desktop)                CREATOR OWNER                     managedocs
OneNote (Desktop)                ALL APPLICATION PACKAGES          printonly
OneNote (Desktop)                Everyone                          printonly
OneNote (Desktop)                SONALKAR\Administrators           all
OneNote (Desktop)                ?unknown                          printonly
OneNote (Desktop)                SYSTEM                        o

OneNote for Windows 10           CREATOR OWNER
OneNote for Windows 10           ALL APPLICATION PACKAGES          printonly
OneNote for Windows 10           ?unknown                          printonly
OneNote for Windows 10           SONALKAR\Sadiq                    all
OneNote for Windows 10           LOCAL SERVICE                     all
OneNote for Windows 10           SONALKAR\Administrators           all
OneNote for Windows 10           SYSTEM                        o

Microsoft XPS Document Writer    SONALKAR\Sonalkar                 all
Microsoft XPS Document Writer    CREATOR OWNER                     managedocs
Microsoft XPS Document Writer    ALL APPLICATION PACKAGES          printonly
Microsoft XPS Document Writer    Everyone                          printonly
Microsoft XPS Document Writer    SONALKAR\Administrators           all
Microsoft XPS Document Writer    ?unknown                          printonly
Microsoft XPS Document Writer    SYSTEM                        o

Microsoft Print to PDF           SONALKAR\Sonalkar                 all
Microsoft Print to PDF           CREATOR OWNER                     managedocs
Microsoft Print to PDF           ALL APPLICATION PACKAGES          printonly
Microsoft Print to PDF           Everyone                          printonly
Microsoft Print to PDF           SONALKAR\Administrators           all
Microsoft Print to PDF           ?unknown                          printonly
Microsoft Print to PDF           SYSTEM                        o

HP Ink Tank 310 series           SONALKAR\Sadiq                    all
HP Ink Tank 310 series           CREATOR OWNER                     managedocs
HP Ink Tank 310 series           ALL APPLICATION PACKAGES          printonly
HP Ink Tank 310 series           Everyone                          printonly
HP Ink Tank 310 series           SONALKAR\Administrators           all
HP Ink Tank 310 series           ?unknown                          printonly
HP Ink Tank 310 series           SYSTEM                        o

Fax                              SONALKAR\Sonalkar                 all
Fax                              CREATOR OWNER                     managedocs
Fax                              ALL APPLICATION PACKAGES          printonly
Fax                              Everyone                          printonly
Fax                              SONALKAR\Administrators           all
Fax                              ?unknown                          printonly
Fax                              SYSTEM                        o
```

5. Dump Groups: It will dump groups. We can view it in columns as well as tables. We can customise what we want to dump and what not.



Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)
File Edit Search Report View Help
Select Computer...
Refresh F5
Permissions Report Options...
Dump Permissions for File System...
Dump Permissions for Registry...
Dump Permissions for Printers
Dump Permissions for Shares
Dump Permissions for Shared Directory...
Dump Permissions for All Shared Directories
Dump Users as column...
Dump Users as table...
Dump Groups as column...
Dump Groups as table...
Dump Users as table fast (names only)
Dump Policies
Dump Rights
Dump Services...

```
Group
Administrator
   Administra
   Sadiq
   Sonalkar
Device Owners
Distributed C
Event Log Rea
Guests
   Guest
Hyper-V Admin
IIS_IUSRS
Performance L
   Sonalkar
Performance M
Remote Manage
System Manage
   DefaultAcc
Users
   Sadiq
Backup Operat
docker-users
   Sadiq
ORA_ASMADMIN
ORA_ASMDBA
   Sadiq
ORA_ASMOPER
ORA_CLIENT_LISTENERS           ORA_CLIENT_LISTENERS
```



```
nd unrestricted access to all features of Hyper-V.
mation Services.
```

Dump Groups as Table

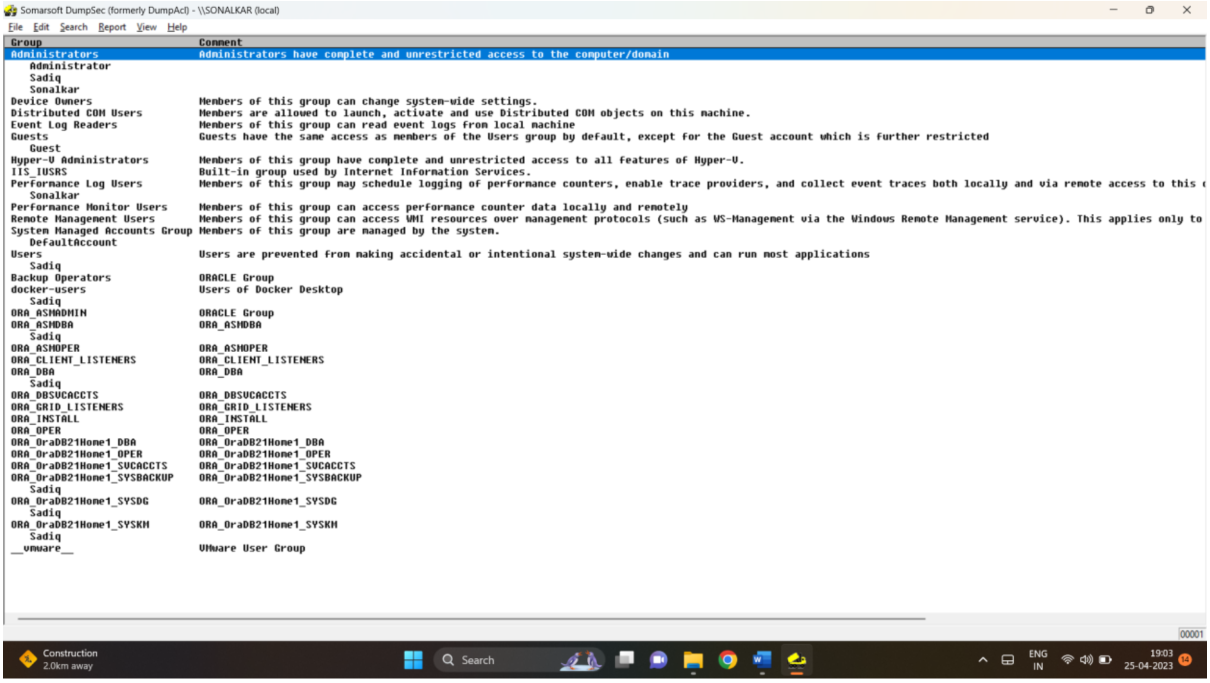
Available fields:

Selected fields (in sort order):
- Group
- Comment
- GroupType
- GroupMember
- MemberType

☑ Show normal user accounts

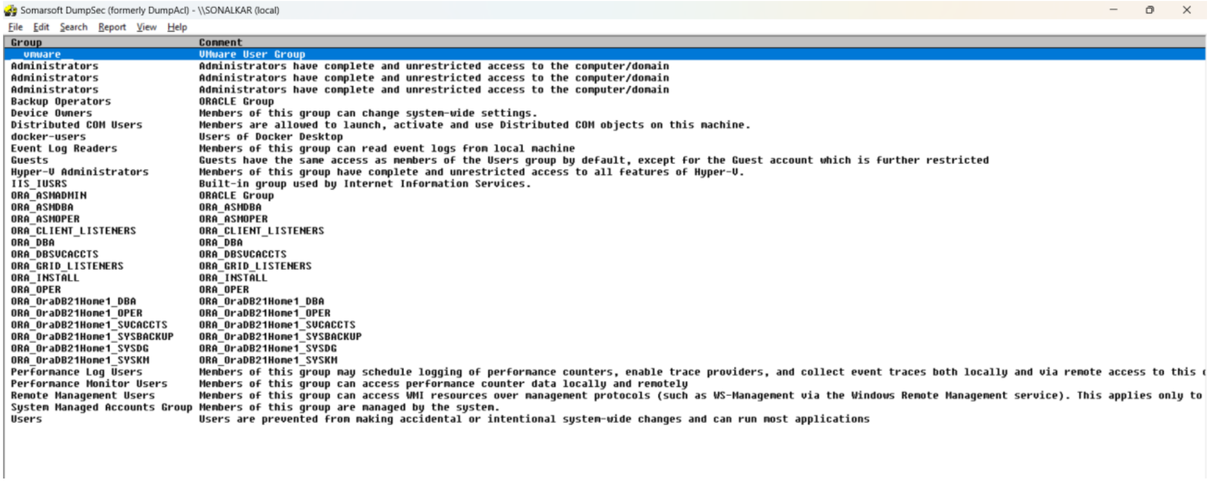
□ Show computer accounts

☑ Fully expand groups (handle case where local group in resource domain includes global group from master domain)



Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)

```
Group                        Comment
Administrators               Administrators have complete and unrestricted access to the computer/domain
   Administrator
   Sadiq
   Sonalkar
Device Owners                Members of this group can change system-wide settings.
Distributed COM Users        Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers            Members of this group can read event logs from local machine
Guests                       Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
   Guest
Hyper-V Administrators       Members of this group have complete and unrestricted access to all features of Hyper-V.
IIS_IUSRS                    Built-in group used by Internet Information Services.
Performance Log Users        Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this c
   Sonalkar
Performance Monitor Users    Members of this group can access performance counter data locally and remotely
Remote Management Users      Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to
System Managed Accounts Group Members of this group are managed by the system.
   DefaultAccount
Users                        Users are prevented from making accidental or intentional system-wide changes and can run most applications
   Sadiq
Backup Operators             ORACLE Group
docker-users                 Users of Docker Desktop
   Sadiq
ORA_ASMADMIN                 ORACLE Group
ORA_ASMDBA                   ORA_ASMDBA
   Sadiq
ORA_ASMOPER                  ORA_ASMOPER
ORA_CLIENT_LISTENERS         ORA_CLIENT_LISTENERS
ORA_DBA                      ORA_DBA
   Sadiq
ORA_DBSVCACCTS               ORA_DBSVCACCTS
ORA_GRID_LISTENERS           ORA_GRID_LISTENERS
ORA_INSTALL                  ORA_INSTALL
ORA_OPER                     ORA_OPER
ORA_OraDB21Home1_DBA         ORA_OraDB21Home1_DBA
ORA_OraDB21Home1_OPER        ORA_OraDB21Home1_OPER
ORA_OraDB21Home1_SVCACCTS    ORA_OraDB21Home1_SVCACCTS
ORA_OraDB21Home1_SYSBACKUP   ORA_OraDB21Home1_SYSBACKUP
   Sadiq
ORA_OraDB21Home1_SYSDG       ORA_OraDB21Home1_SYSDG
   Sadiq
ORA_OraDB21Home1_SYSKM       ORA_OraDB21Home1_SYSKM
   Sadiq
__vmware__                   VMware User Group
```



Somarsoft DumpSec (formerly DumpAcl) - \\SONALKAR (local)

```
Group                        Comment
  vmware                     VMware User Group
Administrators               Administrators have complete and unrestricted access to the computer/domain
Administrators               Administrators have complete and unrestricted access to the computer/domain
Administrators               Administrators have complete and unrestricted access to the computer/domain
Backup Operators             ORACLE Group
Device Owners                Members of this group can change system-wide settings.
Distributed COM Users        Members are allowed to launch, activate and use Distributed COM objects on this machine.
docker-users                 Users of Docker Desktop
Event Log Readers            Members of this group can read event logs from local machine
Guests                       Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Hyper-V Administrators       Members of this group have complete and unrestricted access to all features of Hyper-V.
IIS_IUSRS                    Built-in group used by Internet Information Services.
ORA_ASMADMIN                 ORACLE Group
ORA_ASMDBA                   ORA_ASMDBA
ORA_ASMOPER                  ORA_ASMOPER
ORA_CLIENT_LISTENERS         ORA_CLIENT_LISTENERS
ORA_DBA                      ORA_DBA
ORA_DBSVCACCTS               ORA_DBSVCACCTS
ORA_GRID_LISTENERS           ORA_GRID_LISTENERS
ORA_INSTALL                  ORA_INSTALL
ORA_OPER                     ORA_OPER
ORA_OraDB21Home1_DBA         ORA_OraDB21Home1_DBA
ORA_OraDB21Home1_OPER        ORA_OraDB21Home1_OPER
ORA_OraDB21Home1_SVCACCTS    ORA_OraDB21Home1_SVCACCTS
ORA_OraDB21Home1_SYSBACKUP   ORA_OraDB21Home1_SYSBACKUP
ORA_OraDB21Home1_SYSDG       ORA_OraDB21Home1_SYSDG
ORA_OraDB21Home1_SYSKM       ORA_OraDB21Home1_SYSKM
Performance Log Users        Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this c
Performance Monitor Users    Members of this group can access performance counter data locally and remotely
Remote Management Users      Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to
System Managed Accounts Group Members of this group are managed by the system.
Users                        Users are prevented from making accidental or intentional system-wide changes and can run most applications
```