WinReporter documentation

Table Of Contents

1 General

1.1 WinReporter overview

WinReporter facilitates network management by retrieving all critical data linked to the functioning of your Windows NT/200x network (LAN & WAN), and stores retrieved information in an ODBC type central database.
A getting started guide is available in the start menu (folder WinReporter\Documentation).
Because every table has a field called "id_snapshot", you will be able to store multiple images of your network and get historical analysis as well.
In a first step you can read the WinReporter requirements, in a second step how to use the WinReporter Scanner to start a scan and finally how to display the WinReporter predefined reports. The complete WinReporter database format reference is available for advanced users.

1.1.1

1.1.2 Web site support

Do not hesitate to contact us at info@isdecisions.com to get any sales information or support@isdecisions.com for technical support.
Please check our Frequently Asked Questions before submitting problems to technical support. The FAQ is available on our web site.

1.2 Requirements

For the computer running WinReporter:
Windows NT 4/2000/XP/2003
Service Pack 6 and Internet Explorer 5 or more for Windows NT 4.0
128 Mo physical memory
100 Mo free disk space
For computers being scanned:
Windows NT 4/2000/XP/2003
Windows 95, 98, Me **with Microsoft Remote Administration and Registry service** installed.
Warning! Less information is scanned for these computers.
The Windows 9x remote registry service is available in the remotreg resource kit directory on Windows 9x installation CD. Online installation guide in PDF.

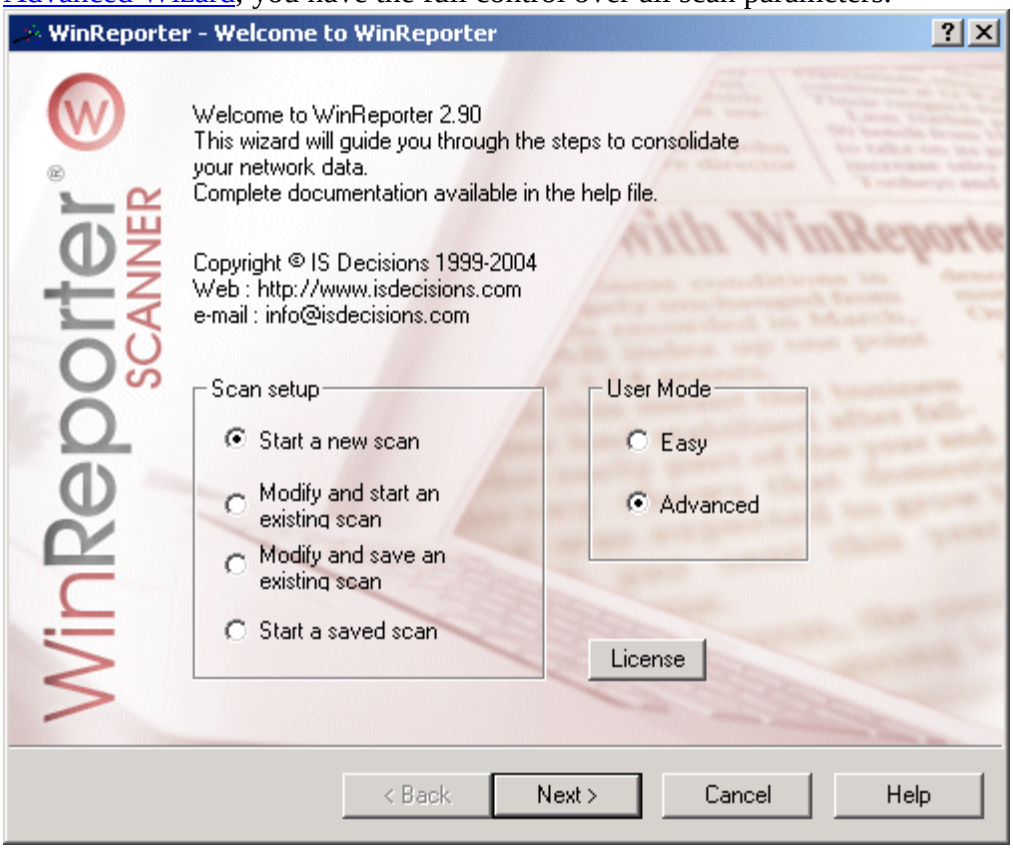
1.3 License

The evaluation version of WinReporter can scan at most 8 workstations and 2 servers during 30 days after the installation. If you need to extend your trial period or increase the number of allowed servers or workstations you can ask for a new evaluation key at:
info@isdecisions.com
If you want to buy WinReporter you can search for a reseller on the following web page:
Locate a reseller
If no reseller is available in your country you can contact us directly: info@isdecisions.com
You can enter you license key or your evaluation key in the Welcome page of the scanner.

2 Scanner

2.1 Welcome to WinReporter

This is the first step of the scan wizard. It introduces you to the core of WinReporter. This step will also allow you to enter your license code.
You can:
Start a new scan
Start and modify (using the wizard) an existing scan (.ntr file)
Modify and save (using the wizard) an existing scan
Start directly an existing scan
Scan setup user mode:
Simplified Wizard, you can only access most important parameters.
Advanced Wizard, you have the full control over all scan parameters.



2.2 Scan requirements

In order to check if a computer can be scanned you can try to access remotely the registry with regedit or regedt32 and access the administrative shares \\computeName\ADMIN$, \\computeName\C$. If this doesn't work please check all hereafter listed points.
In order to successfully scan remote computers the following points should be checked:
- The account running the scanner should own **administrative rights on all computers to scan**. This means that the account should be member of the "domain admins" group or have the same login/password that a local administrator account on remote computers. If this is not the case you need to set impersonation accounts in the advanced scan wizard.
- The server service and the remote registry service should be running on remote computers.

- For Windows 9x/Me computers the Remote registry service should be installed. Windows 9x remote registry service installation guide (on line pdf).
- The scanner should be able to resolve the computer names. If this is not the case you should use IP addresses and IP ranges.
- If the computers to scan are behind a router or a firewall the following protocols should be enabled: NetBIOS (TCP 139), SMB (TCP 445), RPC (TCP 135), ICMP
- For the advanced scan mode (serial numbers, manufacturer, model, memory modules ...) the ADMIN$ administrative share should be accessible (see bellow if you need to enable administrative shares) and DCOM should be enabled (remote computers and local computer). If DCOM is disabled you can enable it with *dcomcnfg*.
- In order to scan partitions the administrative shares C$, D$ (1 share per partition) should be available.

If administrative shares are disabled you should enable them in the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
The two following values (REG_DWORD) should be set to 1: *AutoShareWks*, *AutoShareServer*
If some computers are not scanned please take a look at the Scan errors & warnings report. For some unusual problems you may also take a look in the application log (source WinReporter) in order to get more information about the problem.

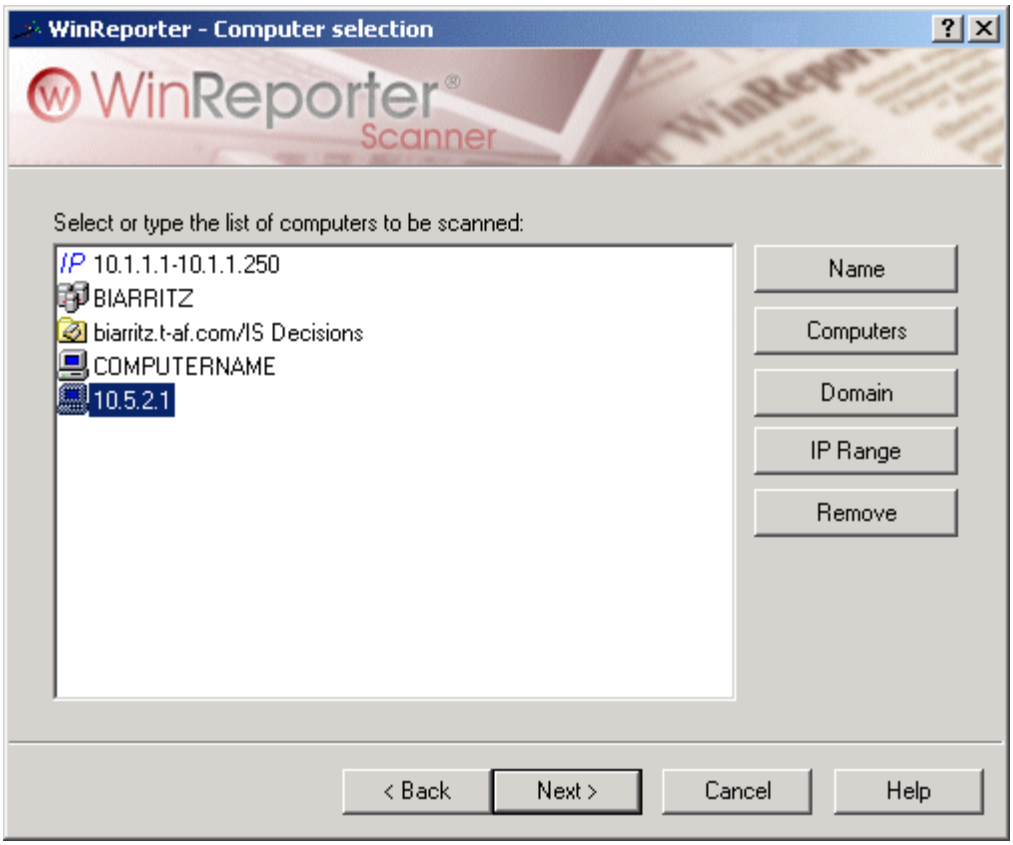
2.3 Simplified Wizard

2.3.1 Simplified Wizard

The simplified wizard is made of the following steps:
Select computers
Validate
Note that the simplified wizard uses the default Microsoft Access database file. This default database is located in the WinReporter program files folder (default installation path is: *c:\Program Files\ISDecisions\WinReporter\WinReporter.mdb*).

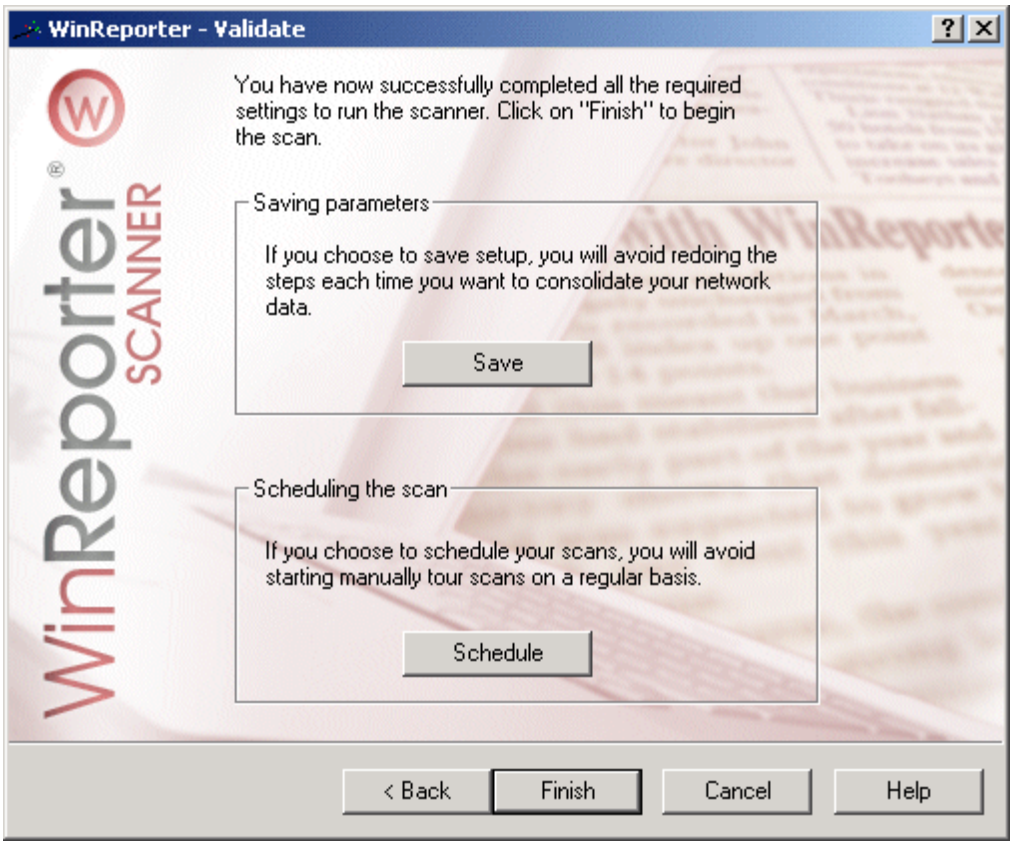
2.3.2 Computer selection

This is the first step of the scan wizard. You have to select all the computers you want to add to your scan either:
By entering a name manually: you will have to type the full hostname or the NetBios name of a computer or of a Windows domain (Select domain as type). You can also enter an IP address of a computer.
By selecting computers in the browser.
By selecting domains or Organization Units in the browser. It is the easiest way to scan all computers in a Windows domain.
By selecting IP range to scan. It provides another way to specify computers to be scanned. It is the easiest way to scan a large array of computers in a network (for example: a DHCP pool). Just click on "Insert" to add a new IP range to the selection through the "IP range edit" dialog box.



2.3.3 Validate

This is the final step of the wizard. You can *save* your configuration in a .NTR file in order to use it later to run WinReporter in a background mode or through the WinReporter Task Scheduler.
You can *schedule* the scan if you want launch it at periodic time.
To start the scan, just click on Finish and the progress window will be displayed.



2.4 Advanced Wizard

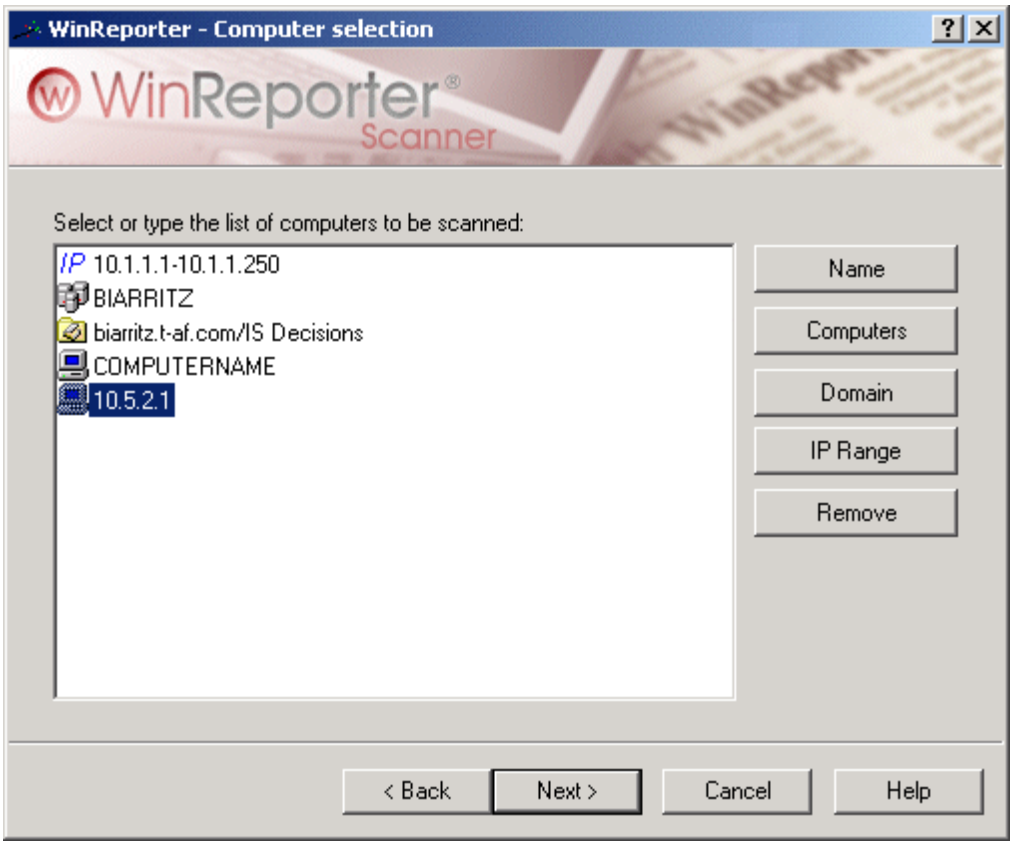
2.4.1 Advanced Wizard

The advanced wizard is made of the following steps:
Select computers and IP ranges
Database configuration
Hardware information to scan
Windows NT information to scan
Software information to scan
Eventlogs scan configuration
Additional parameters
Validate
The default configuration will scan the same information as in simple mode. To run all reports the default configuration is needed at least.

2.4.2 Computer selection

This is the first step of the scan wizard. You have to select all the computers you want to add to your scan either:
By entering a name manually: you will have to type the full hostname or the NetBios name of a computer or of a Windows domain (Select domain as type). You can also enter an IP address of a computer.
By selecting computers in the browser.
By selecting domains or Organization Units in the browser. It is the easiest way to scan all computers in a Windows domain.

By selecting IP range to scan. It provides another way to specify computers to be scanned. It is the easiest way to scan a large array of computers in a network (for example: a DHCP pool). Just click on "Insert" to add a new IP range to the selection through the "IP range edit" dialog box.



2.4.3 Database configuration

You have to specify where the data should be stored. If you don't know how to compose manually an ODBC connection string, you can use the database wizard. The default database is the WinReporter Access database (WinReporter.mdb) in the WinReporter folder. The default installation path is: *c:\Program Files\ISDecisions\WinReporter\WinReporter.mdb.*

2.4.4 Scan Hardware

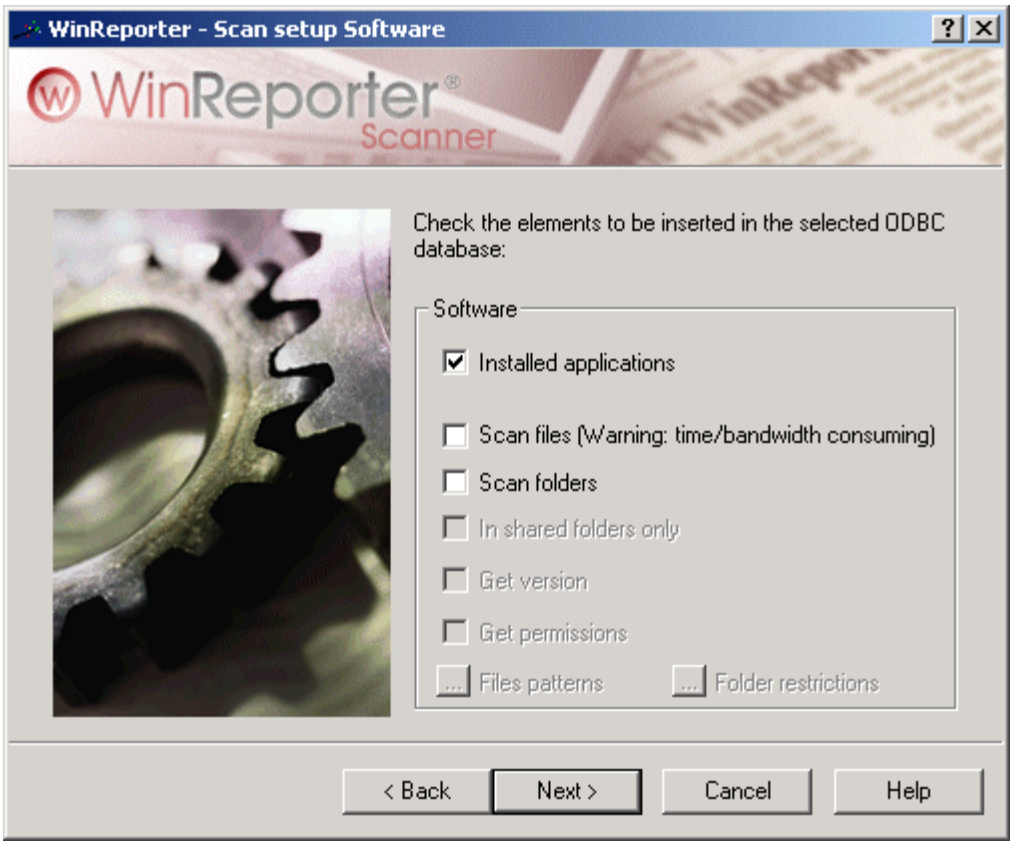
Check here all hardware information you want to retrieve.
CPU: list computers processors in the processors table
Memory: get the computer physical memory in *ram* field from servers table.
BIOS information: get BIOS information in *bios_type*, *bios_date* fields from servers table
Video adapters: list video adapters in the VideoAdapters table
Network adapters: list network adapters in the netcards table
Disks & Partitions: list partitions in the partitions table and physical disks and tapes in the PhysicalDisks table
Printers: list printers in the printers table
Printers permissions: get printers permissions in the aces table and field *account_name* from the printers table.
Manufacturers: Scan the manufacturer, serial number and model for the computer and the motherboard (Fields Manufacturer, Model, Serial, MotherBoard, MBSerial, MBManufacturer of the servers table).
Devices: Scan all devices (from the device manager) and insert them in the devices table.

2.4.5 Scan NT Information

Check here the Windows NT information you want to retrieve.
Hotfixes: list hotfixes in the hotfixes table
SwapFiles: insert swap files in the SwapFiles table.
Scheduler jobs: list jobs in the jobs table
Services: list services in the services table
SAM: list users an groups in users, groups and acc_ownership table
All used domains: scan systematically all PDC of all scanned domains
Shares: get shares information in the shares table
Share permissions: get share permissions in the aces table
DNS servers: Scan Microsoft DNS servers and insert their configuration in the DnsServers table and DNS zones in the DnsZones table.
IIS servers: Scan running IIS services (www, ftp, ...) and insert their state in the IISServers table.
AD servers: Insert Active directory domain controllers' roles in the ADServers table.
Registry values: Add all registry value/key you want to scan. The information is inserted in the RegValues table. You will then be able to analyze this information with the Registry values report.

2.4.6 Scan Software

Check here the software information you want to retrieve.
Installed applications: list installed applications in the software table
Scan files: retrieve files information in the realfiles table.
Scan folders: retrieve folders information in the realfolders table.
Shared folders only: retrieve only files and folders information from shared folders
Get version: get version of files in the versions table
Get permissions: get the file and folder permissions in the aces table
Files patterns: You can add patterns to specify the files to scan. No pattern means that all files will be scanned.
Folders restriction: Select folders if you only want to scan files and folders in specified folders.

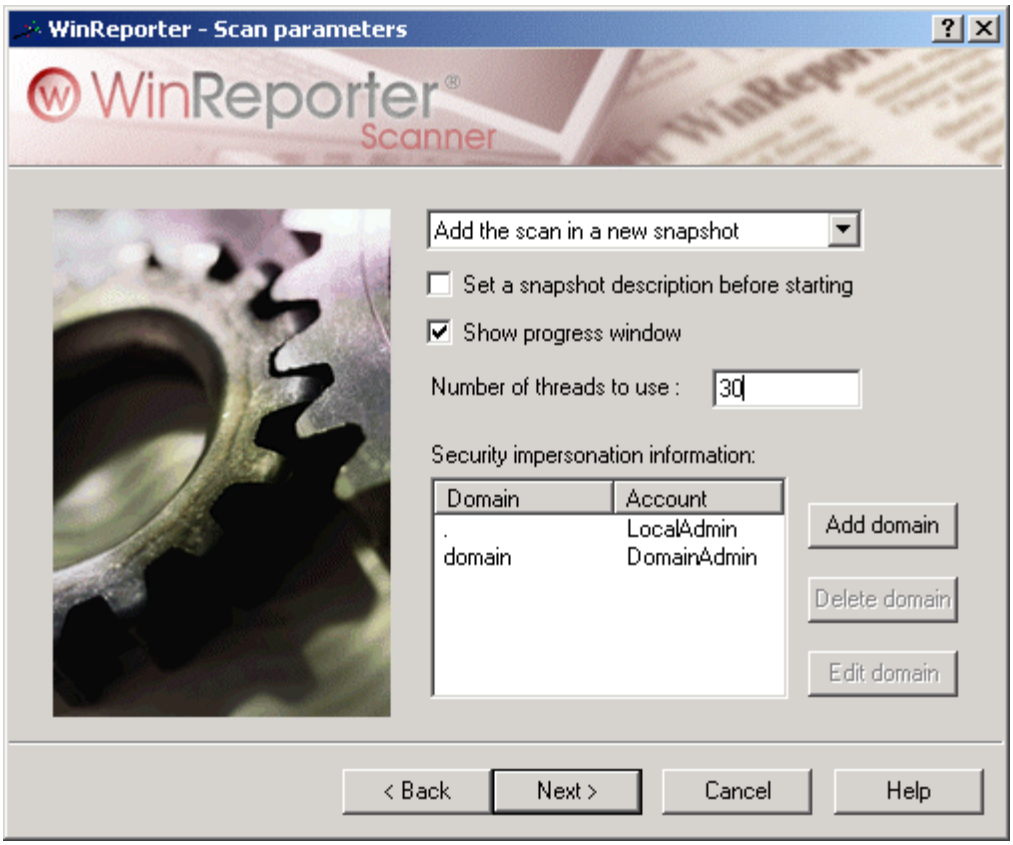


2.4.7 Scan Event Logs

Check here the event logs and the event types you want to insert in the database (tables ET_Events and ET_Params). You can analyze this information with event log reports.

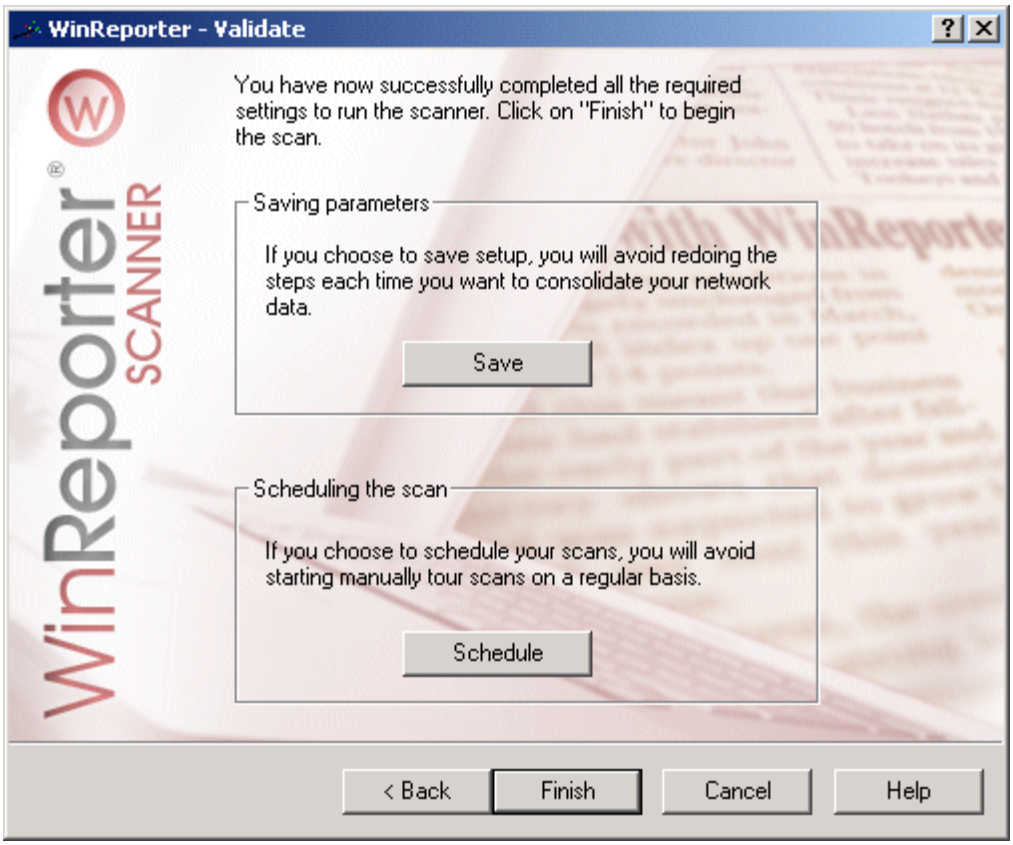
2.4.8 Additional Parameters

Scan mode:
Don't keep older snapshots.
To simplify database management and query designing, you may want not to use snapshots, to do so, simply select this scan mode.
Warning: be aware that not checking this box will result in losing all data from previous snapshots.
Add the scan in a new snapshot
Default mode. The scanner will create a new snapshot and put all scanned computers in it.
Add unscanned computers to the latest snapshot
The scanner will only scan computers unavailable during the latest scan.
Update the latest snapshot
The scanner will do a full scan and update if possible all computers already available in the latest snapshot and add new computers if any. If you want to keep the history rather *Add the scan in a new snapshot* and use later the snapshot manager in order to merge all snapshots in a single snapshot. The result will be the same.
Other options:
The option *Set a snapshot description before starting* will allow you to enter a short description before the scan starts. The description will be displayed in the reporter.
Check box *Show progress window*:
Check this if you want to see the scan progression.
Number of threads to use:
Maximum number of threads that can run at the same time. You can decrease the default number if you want to slow down the scan (minimum value 15). If the scanner doesn't use 100 % of CPU during a scan you can try to speed up the scan by increasing this number.
Domain security information:
If you don't own administrative rights for all domains to scan, you can enter here accounts that have these rights.
You can Add or Edit the security information for a domain.
If you want to use remote computers local administrator account you can enter a dot (.) as domain (e.g. to scan computers in a workgroup or in a Novel network).



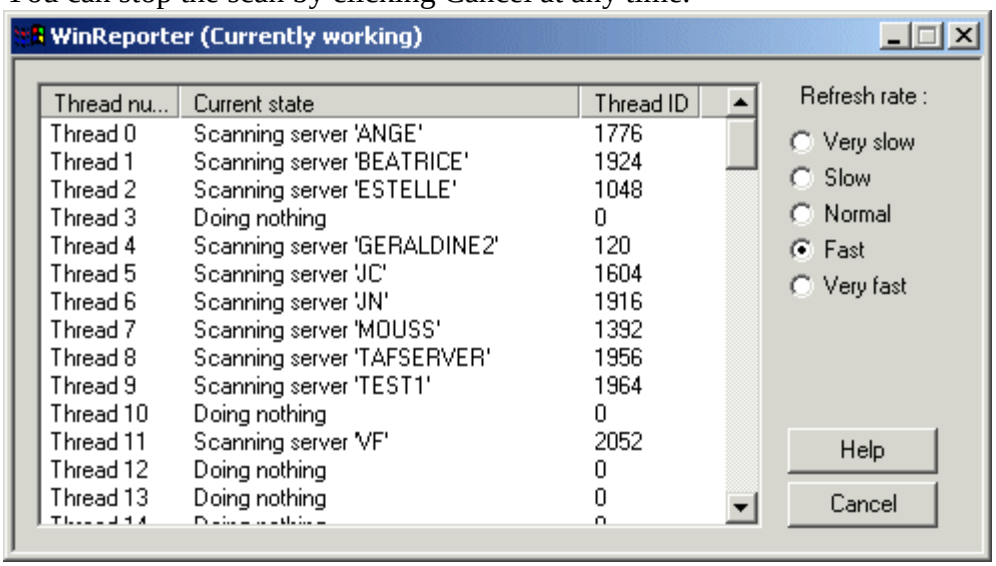
2.4.9 Validate

This is the final step of the wizard. You can *save* your configuration in a .NTR file in order to use it later to run WinReporter in a background mode or through the WinReporter Task Scheduler.
You can *schedule* the scan if you want launch it at periodic time.
To start the scan, just click on Finish and the progress window will be displayed.



2.5 The progress window

This dialog-box lets you visualize the current state of each WinReporter thread.
The refresh rate changes the update speed of the progress window.
You can stop the scan by clicking Cancel at any time.



Add the end of the scan a message box is displayed with the number of successfully scanned computers, failed to scan computers and scan warnings.
If you click O.K. the reporter is displayed and if errors or warnings occurred the Scan errors & warnings report is also automatically displayed.

2.6 Scan errors

If errors or warnings occurred during a scan you will find the required information in order to fix the problem in the Scan errors & warnings report. This report is automatically displayed if needed after a scan.
For unusual errors you may also find explanation events in the *Application* log (Source *WinReporter*).
An *error* means that the computer wasn't scanned and a *warning* means that some information for the specified computer will not be available.

3 Reports

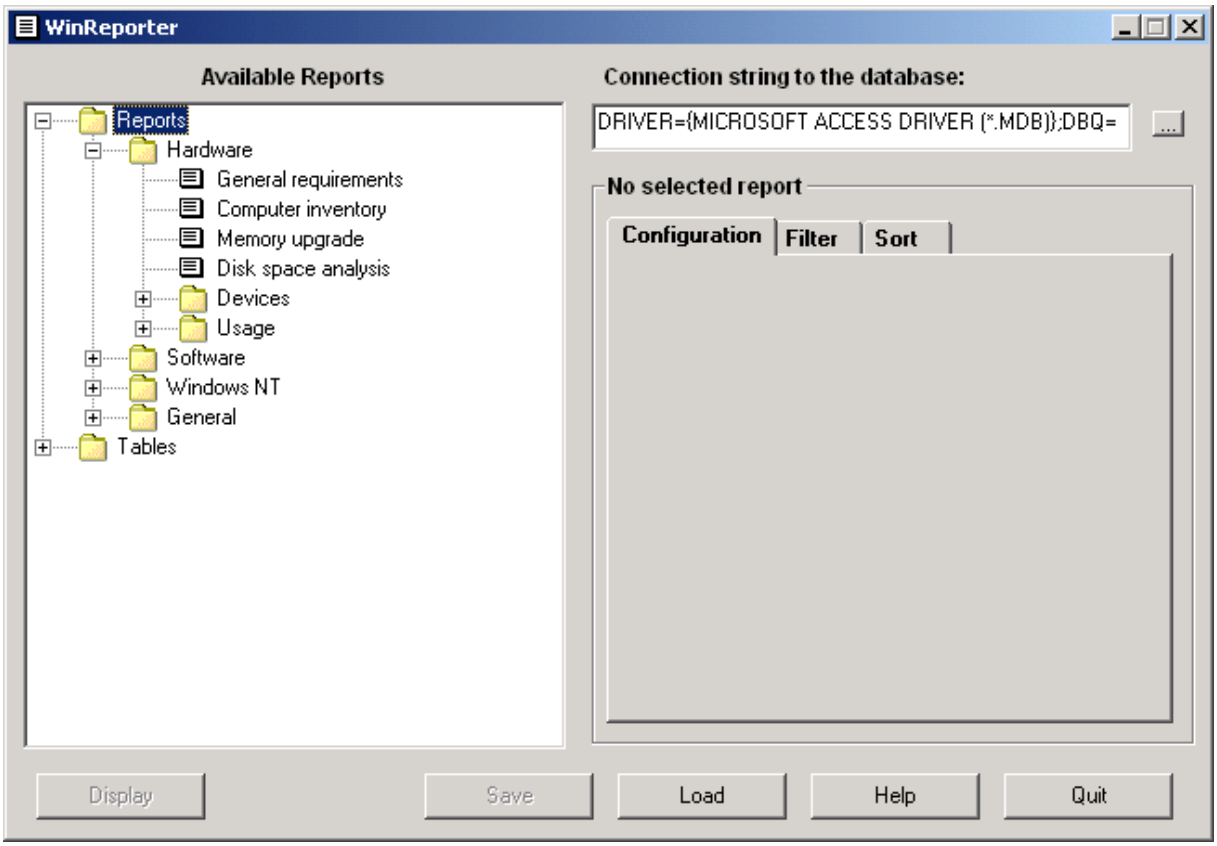
3.1 Report Overview

WinReporter bundles with 29 predefined reports that have been split in four categories: Hardware, Software, Windows NT & General
In order to generate the reports, you need to use the Reporter. Each report is customizable, printable and exportable in several file formats. Also, the report configuration can be saved in order to be used later with a new snapshot or in order to automate the the report generation after a scan through the command line mode.
Additionally you will find 8 event log reports. These reports are based on the Windows NT/2000/XP/2003 event logs that can be scanned with the WinReporter scanner.
You can configure reports in order to display your company logo and a text in the header of all reports.

3.2 Reporter

3.2.1 The Reporter

In order to generate a report with the Reporter, you need to:
Choose the report in the available reports list
Enter the connection string to the database (you can use the database wizard for this)
Choose the snapshot in the available snapshots list.
Choose the report options in the report configuration tab (specific for each report)
Optional. Choose a computer (or user) filter through the filter tab. (Only for selected reports)
Optional. Configure the sort and group options for the report through the Sort tab. (Only for selected reports)
Click *Display* in order to view the report with the report viewer.
A report can be printed and exported in several file formats with the report viewer and its configuration can be saved and reloaded with the *save*/*load* buttons. The report configuration file can also be used to generate automatically reports after a scan using the command line mode.
You can configure the Reporter in order to display your company logo and a text in the header of all reports.
You can also use the Reporter to display raw data from the WinReporter database.



3.2.2 The Report Viewer

With the report viewer you can:

Print your report

Export the report

Explore the report with the table of content (button top - left)

Copy the text contained in the current page in the clipboard

Search for a text sequence in the report

Go in single page mode

Go in multiple page mode

Zoom in

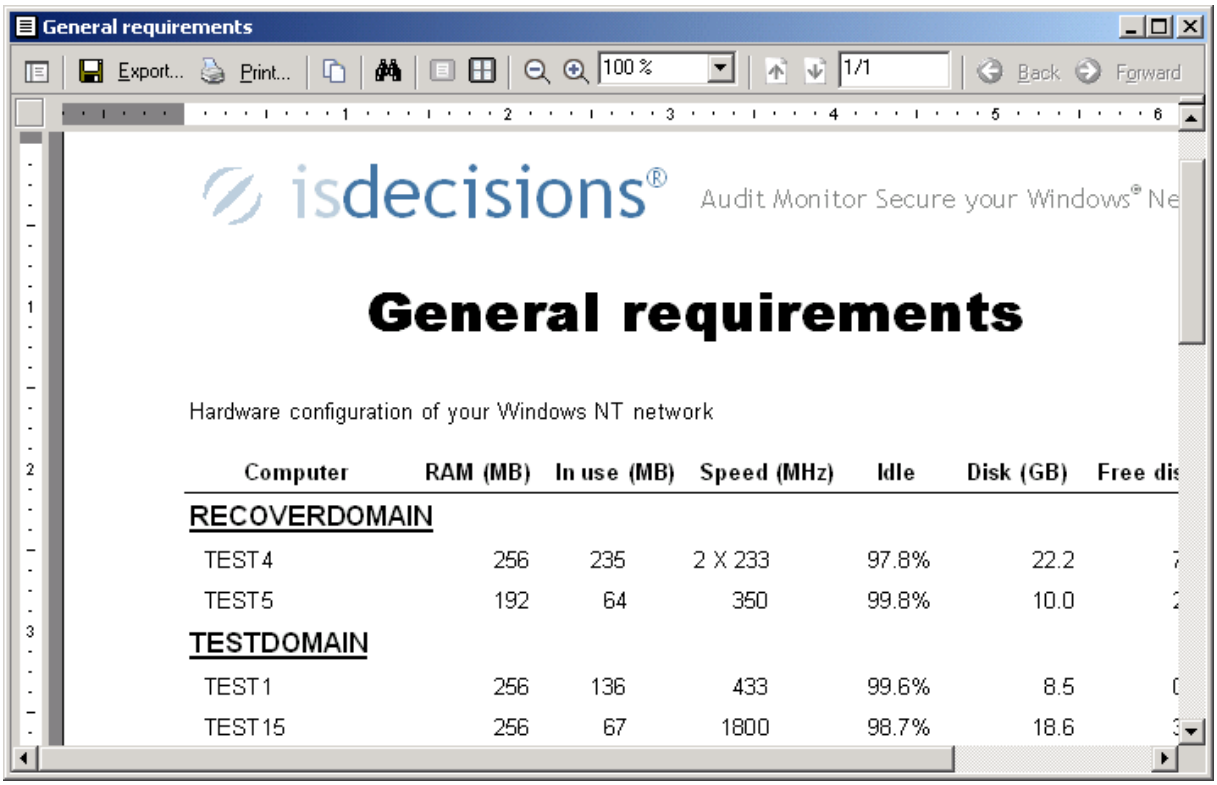
Zoom out

Go to the next page

Go to the previous page

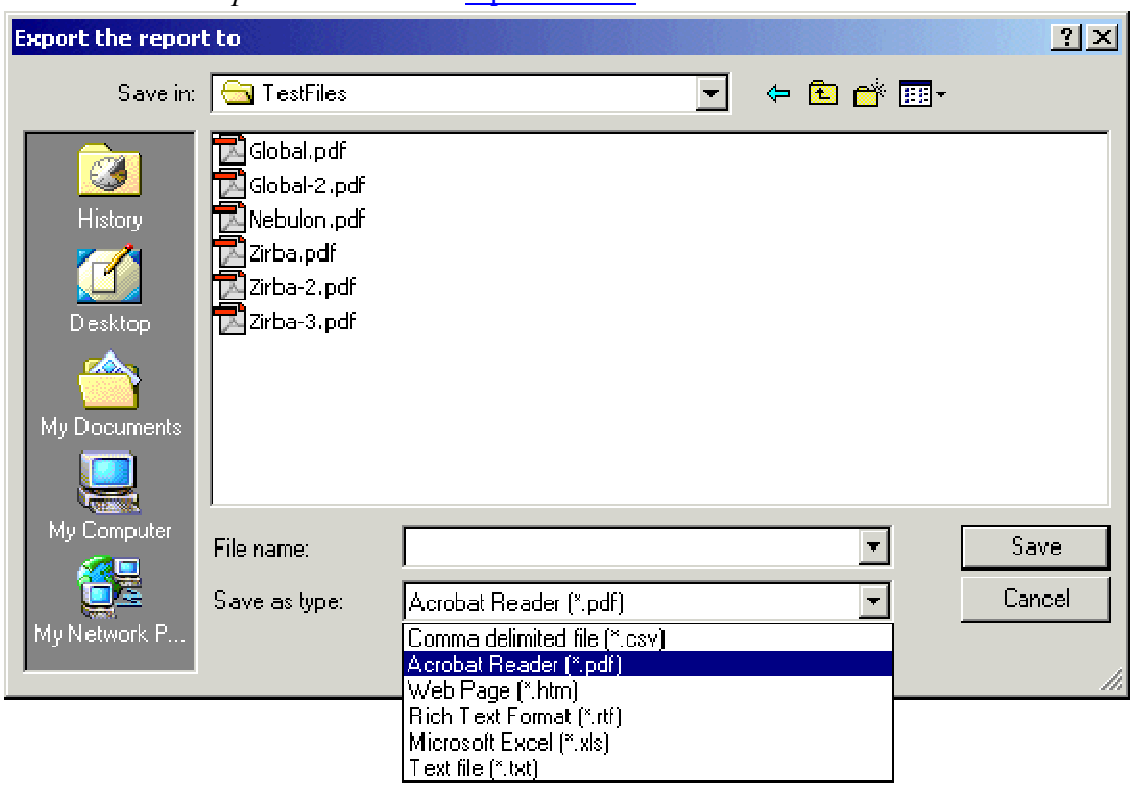
Move backward

Move forward.



3.2.3 Export a report

In order to export a report you need to
1- Click on the *Export* button in the report viewer



2- Choose the export format you are interested in:
Comma delimited file *.csv* (usable with Excel)
Excel document *.xls*

Portable document file *.pdf* (viewable with Acrobat Reader)
Rich text *.rtf* (viewable with Word, WordPad)
Text file *.txt* (viewable with the notepad)
Web page *.htm* (viewable with a web browser)
RemoteExec computer list *.rec* (you can load the computer list in RemoteExec in order run a task on these computers)
3- Choose the file name
4- Click the *Save* button

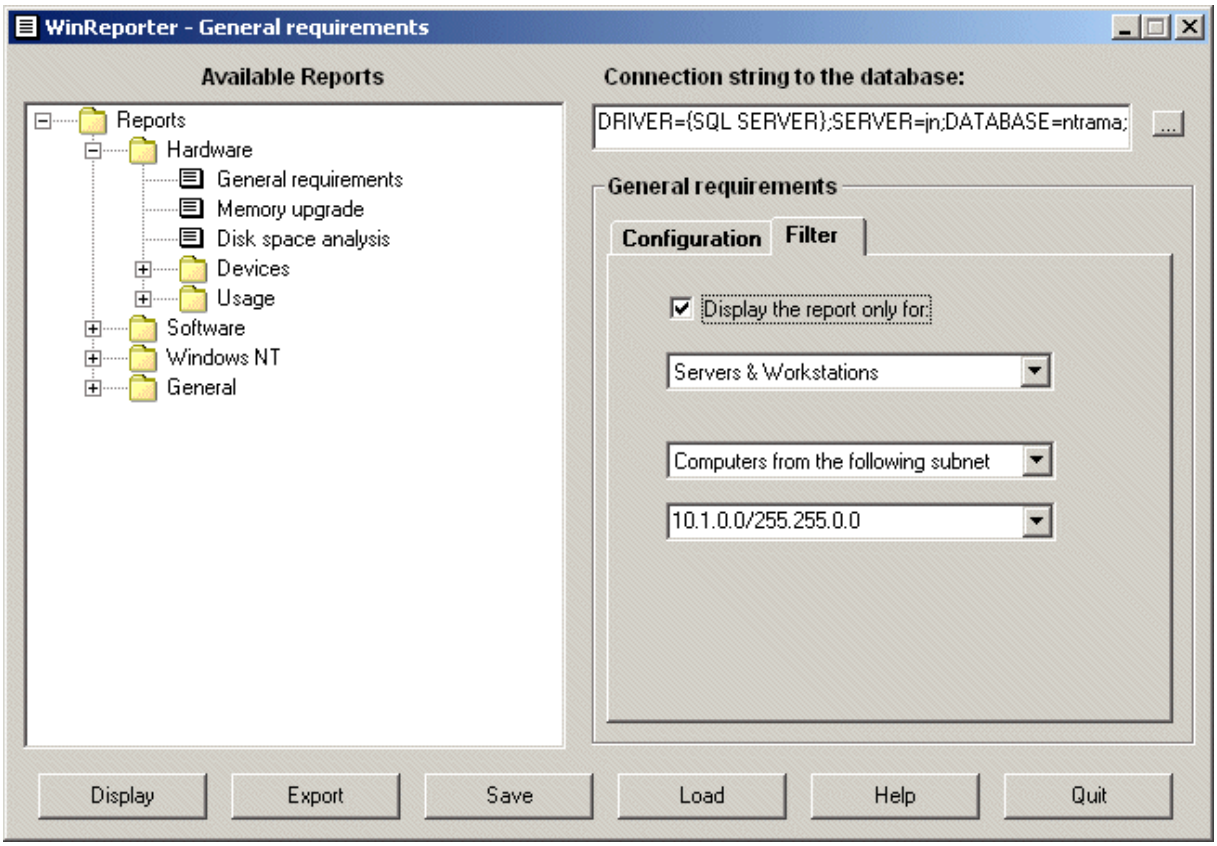
3.2.4 Save/Load a report configuration

If you want to generate a report with specific parameters several times with newer snapshots, you can save the configuration in a *.rcf* file (Report Configuration File) with the *Save* button. The file can then be reloaded later with the *Load* button. The report configuration file can also be used to generate automatically reports after a scan using the command line mode.

3.2.5 Computer/Account Filter

With the filter tab you can set a computer filter for all reports.
The filter can be set on
- The Operating System level: Server/Workstation
- The computers' subnet
- The computers' AD container
- The computers' domain
- The computer's name

This is useful if you want for example display a report on for servers or for a specified subnet.
For the Account logon analysis report you can filter on:
- Domain accounts or local accounts
- The user domain or user computer
- The user AD container



3.2.6 Command line mode

Full reference on Reporter command line mode:
reporter [/AUTOGEN "%ExportedReportFile%"] [/REPORT "%ReportConfigurationFile%"] [/LASTSNAPSHOT] [/SNAPSHOT %SnapshotNumber%] [/DATABASE "%DatabaseConnectionString%"]
/AUTOGEN %ExportedReportName% automatically generates a report in the specified file (*.pdf, *.htm, *.csv, *.txt, *.xls). If used, /AUTOGEN should always be the first argument.
/LASTSNAPSHOT Specify to run reports on the latest snapshot of the database. This is useful to automate an export after a scan.
/SNAPSHOT %SnapshotNumber% Specify the snapshot on which to run reports.
/DATABASE %Connection string% Specify the database on which to run reports. You can copy the connection string from the Scanner or from the Reporter.
/REPORT %ReportConfigurationFile% Specify a report configuration file that will be loaded by the reporter.
For example, you want to generate a report periodically
1- Configure a scan with the WinReporter scanner and save the configuration in a *.ntr* file (%ScanConfigurationFile%)
2- Configure a report with the Report tool and save the configuration in a *.rcf* file (%ReportConfigurationFile%)
3- Create a batch that will launch the scan and the report generation.

"c:\program files\isdecisions\WinReporter\Scanner.exe" "%ScanConfigurationFile%"
"c:\program files\isdecisions\WinReporter\reporter.exe" /AUTOGEN "%ExportedReportFile%" /REPORT "%ReportConfigurationFile%" /LASTSNAPSHOT /DATABASE "%DatabaseConnectionString%"

4- Create a scheduled task that will launch the batch periodically

%ReportConfigurationFile% can be located on a folder located in an intranet web site (.htm or .pdf export) in order to automatically update it.

3.3 Standard reports

3.3.1 Reports List

Hardware
General Requirement
Computer inventory
Disk Space Analysis
Memory upgrade

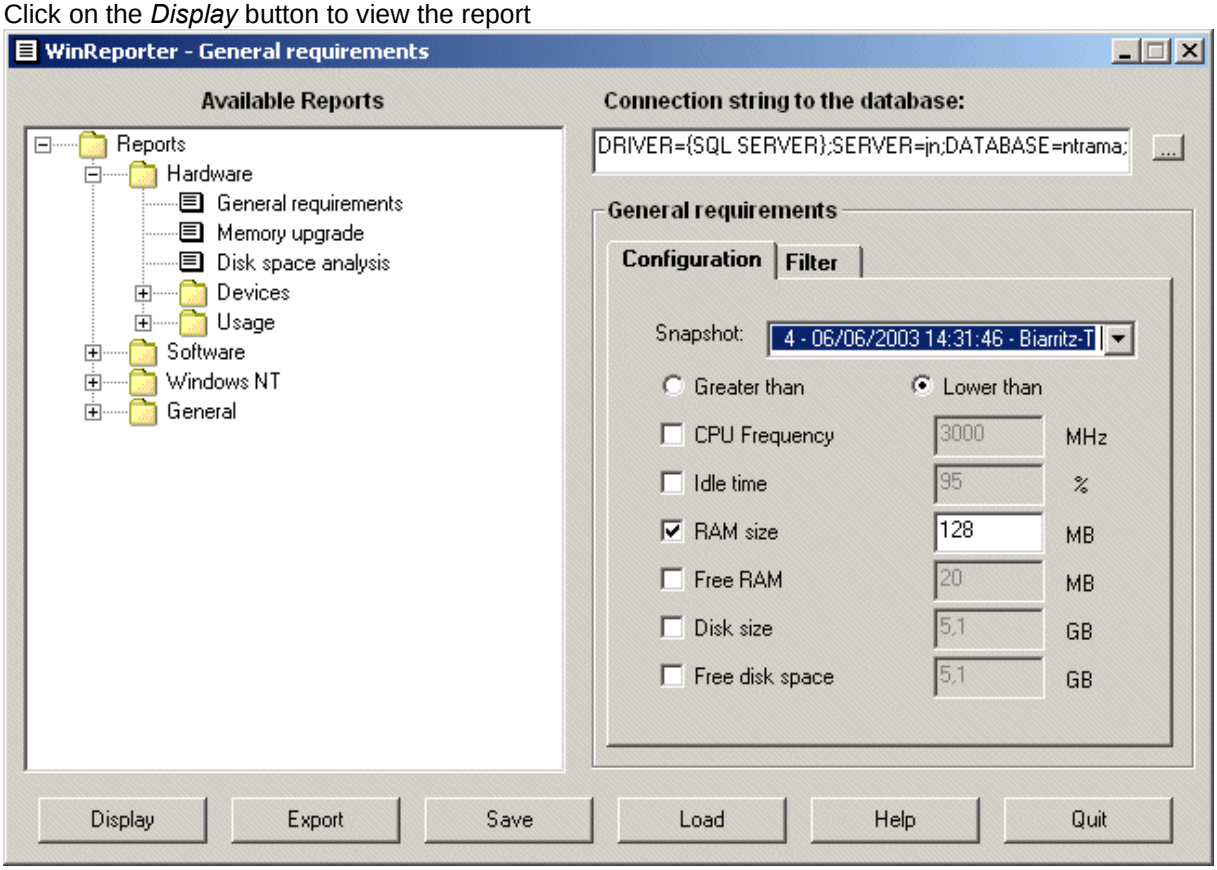
Devices
Printers
Video Configuration

Disk Space Evolution
Memory space evolution
Processor time evolution
Software
Install Statistics
Product Location
Newly installed products
Software analysis
Windows NT
Service Packs and hotfixes
Users in Groups
Services Analysis
Local account analysis
Local administrators analysis
Shares analysis
Share permissions
Account logon analysis
Schedule tasks
Registry values
General
Added/removed computers
Computer changes
Generic query
Scan errors & warnings
Global report

3.3.2 Hardware

3.3.2.1 General hardware requirements

This report allows you to search for computers with specific hardware requirements.
For example, if you want to find & replace oldest computers of your Windows NT network because they can't support a new OS version:
Select *Lower than* as criteria
Select the different fields (processor frequency, memory size, disk size, free disk space) you want to use to select your computers and set their limit.
Click on the *Display* button to view the report



General requirements

List of computers on which:
The physical memory size is lower or equal than 256 MB

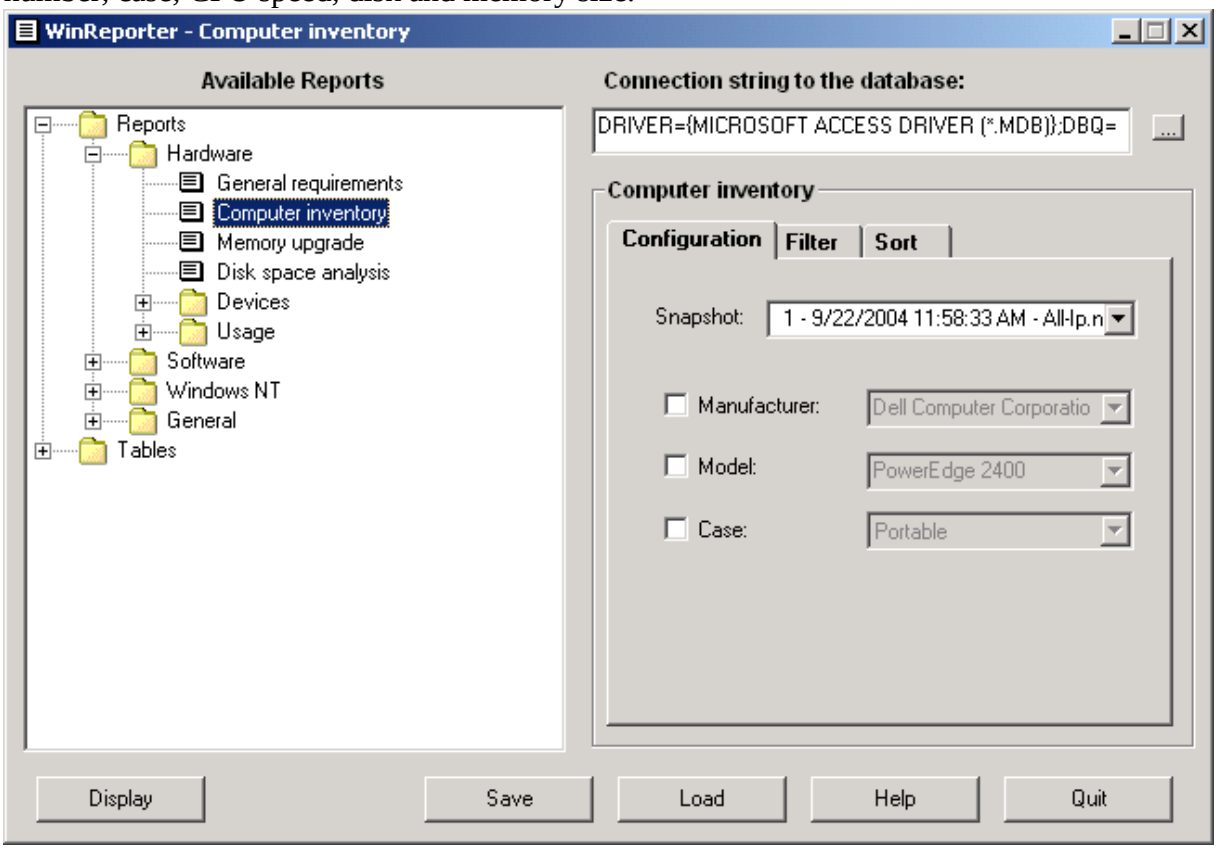
Additional computer filter:
-Only for the domain: TESTDOMAIN

Computer	RAM (MB)	In use (MB)	Speed (MHz)	Idle	Disk (GB)	Free disk (GB)
TESTDOMAIN						
TEST1	256	135	433	99,4%	6,5	0,8
TEST4	256	122	2 X 239	99,5%	7,0	2,1
TEST5	192	59	360	99,6%	4,0	1,0

Selected computers: 3

3.3.2.2 Computer Inventory

The report displays computers according to: manufacturer, model and case (portable or not portable)
The following information is displayed for each computer: model, manufacturer, serial number, case, CPU speed, disk and memory size.



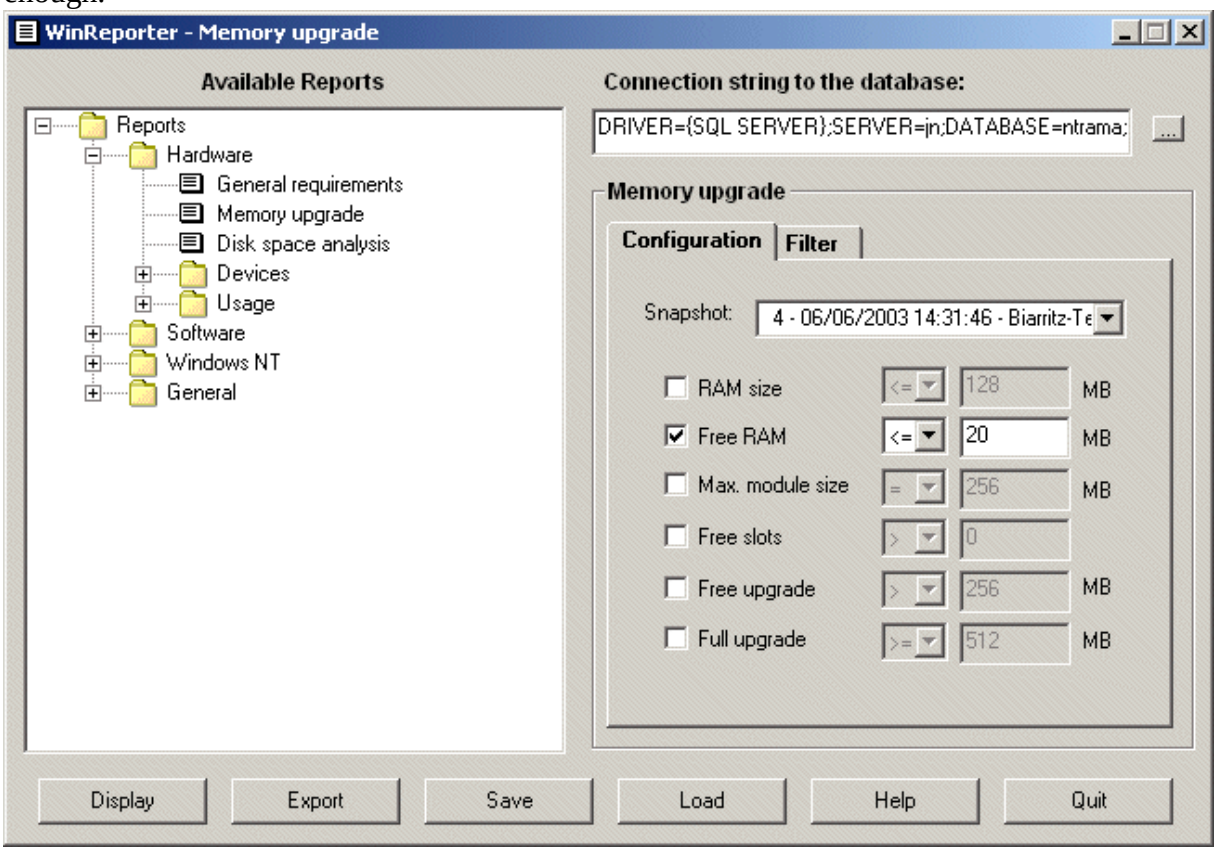
Computer inventory

Computer	Model	Serial	Manufacturer	RAM (MB)	Disk (GB)	Speed (MHz)	Type
RECOVERDOMAIN							
TEST4	Pentium II System			256	22	2 X 233	
TEST5				192	10	350	
TESTDOMAIN							
TEST1	V433	QDYT8	Dell Computer Corporation	256	8	433	
TEST15				256	19	1800	Desktop
TEST16				512	19	1800	
TEST3	System Name	SYS-1234567890	System Manufacturer	64	4	200	

Selected computers: 6

3.3.2.3 Memory upgrade

WinReporter can scan memory slots, the currently installed modules sizes and the maximum allowed module size. Using this information the report displays to how much RAM each computer can be upgraded either using only free slots (Free upgrade) or using all slots (Full upgrade) by replacing current modules with bigger ones.
You can set filter on several fields to find for example all computers that cannot be upgraded enough.



Memory upgrade

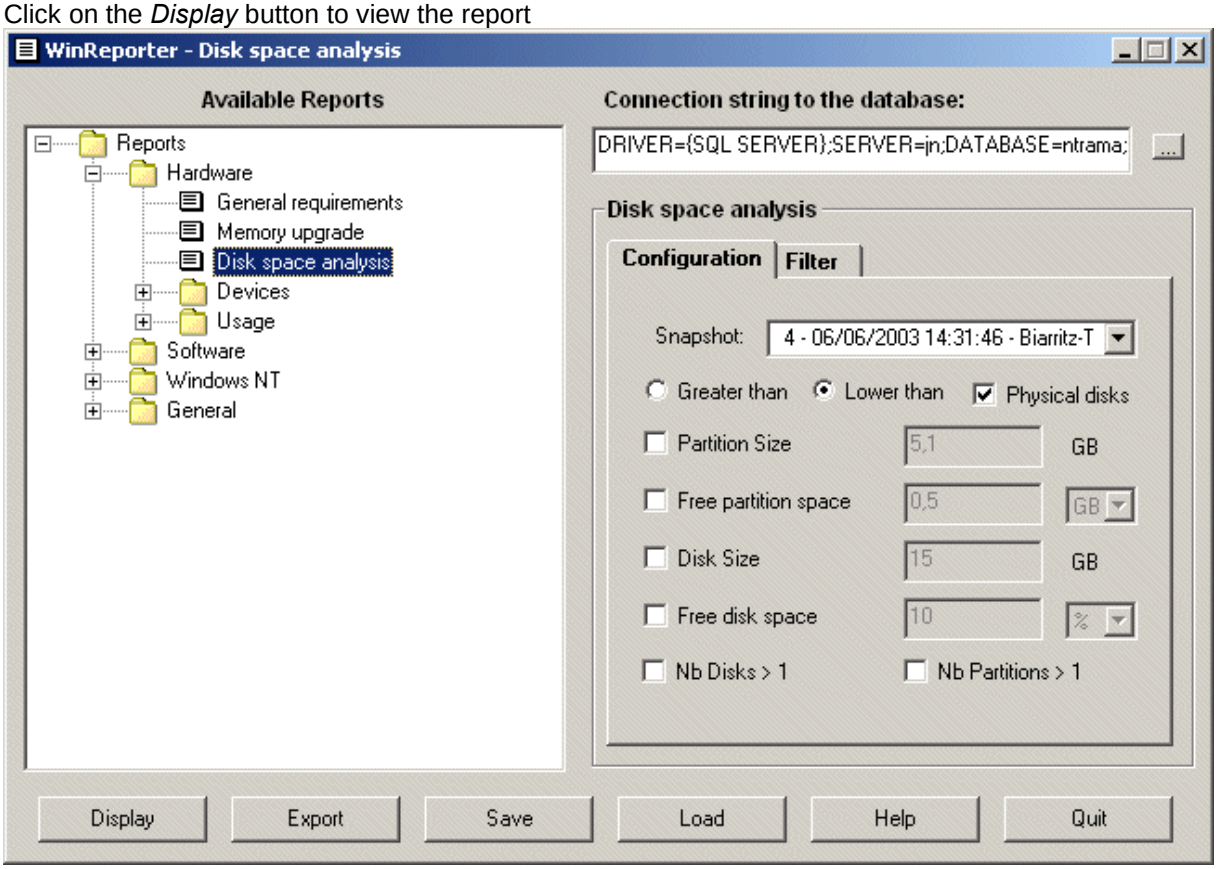
Memory upgrade capabilities of your Windows computers

Additional computer filter:
-Only for the domain: TESTDOMAIN

Computer	RAM	In use	Max. Mod.	Upgradable to	Slots	Free slots
TESTDOMAIN						
TEST1	256	122	256	256 / 768	3	0

3.3.2.4 Disk space analysis

With this report you can monitor the free disk/partition space on your all Windows NT computers.
If you check physical disks you will see them in the report in addition to partitions. In that case the condition *Nb Partitions >1* means partitions in a physical disk rather that partitions on the computer.
For example, you may want to look for all volumes with less than 500 MB free to act before they become full.
Select *Lower than* as criterion
Uncheck *Disk Size*
Check Free disk space
Choose *GB* as free disk space unit
Enter 0.5 as free disk space limit
Click on the *Display* button to view the report



Disk space analysis

List of disk volumes with
On a physical disk with
a free space lower or equal than 25 and

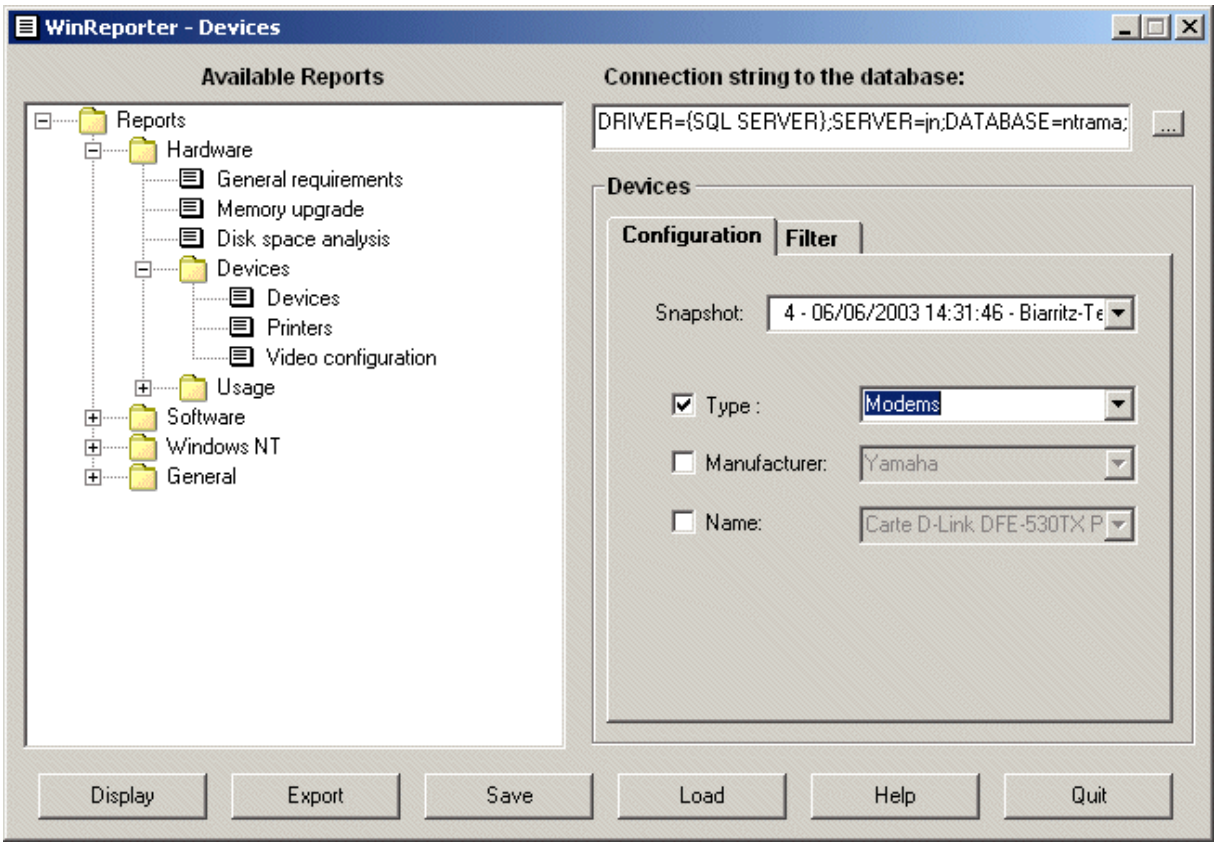
Additional computer filter:
-Only for the domain: TESTDOMAIN

Computer		Volume	Size (GB)	Free space (GB)	Free space (%)
TESTDOMAIN					
TEST1					
Maxtor 90913D4	NAN4	0	6,54	0,82	12,5%
		C	2,93	0,46	15,8%
		D	3,62	0,35	9,8%
TEST4					
FUJITSU MPC3032AT		0	3,01	0,66	21,8%
		C	3,01	0,66	21,8%

3.3.2.5 Devices

3.3.2.5.1 Devices

In this report you can display all devices available in the Windows device manager. You can set a filter on the manufacturer, the device type and the device name.
For example if you want to find all modems on your network you need to:
Check *Type*
Select *Modems* in the combo box (if not available no modems are available)
Uncheck all other filters
Click *Display*



Devices

Computer devices of your Windows network.

Device filter:
-The device belong to the "Monitors" category

Additional computer filter:
-Only for the domain: TESTDOMAIN

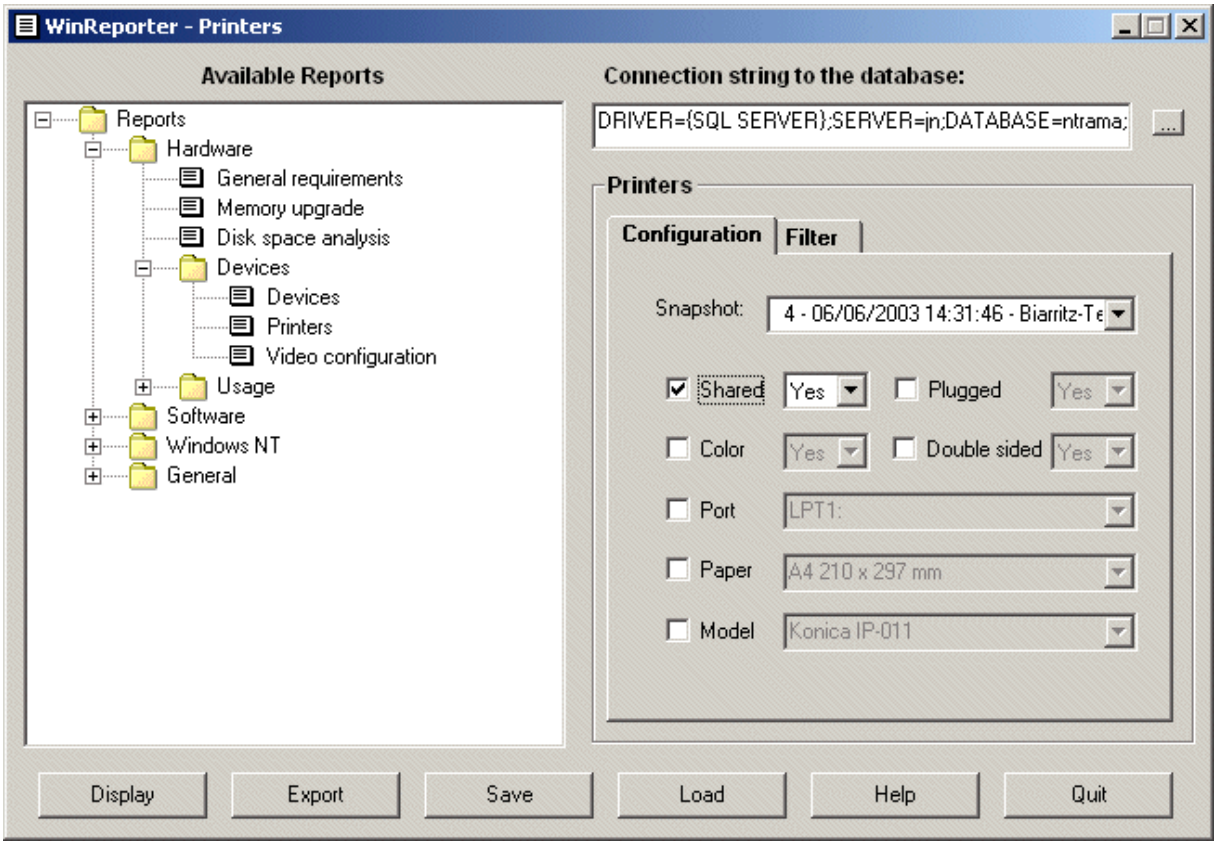
Type	Name	Manufacturer	Location
TESTDOMAIN			
TEST10			
Monitors	Default Monitor	(Standard monitor types)	
TEST4			
Moniteurs	Écran par défaut	(Types d'écrans standard)	

3.3.2.5.2 Printers

This report is designed to list all printers configured on your network. You can set a filter on the following information:
- The printer is shared/not shared
- The printer is plugged (local printers on LPT ports)
- Color printer Yes/No
- Double sided Yes/No
- The port
- The paper format
- The model

For example if you want to display all shared printers
Check shared

Select Yes
Uncheck all other check boxes
Click display



Printers

Printers in your Windows network

Printers filter
-Shared

Additional computer filter:
-Only for the domain: TESTDOMAIN

TESTDOMAIN

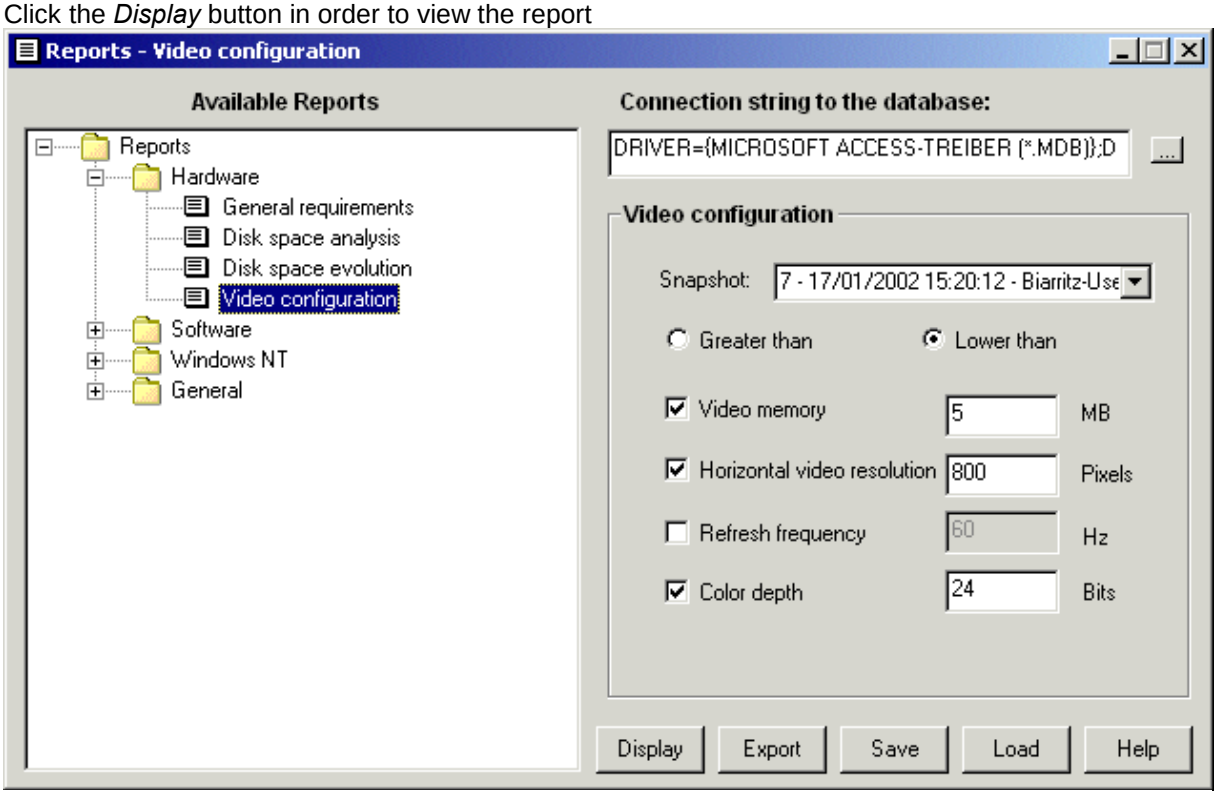
TEST1	Shared	Port	Color	Paper	DPI	Speed
HP LaserJet 4L	1	LPT1:	1	Letter 8 1/2 x 11 in	300	

TEST4	Shared	Port	Color	Paper	DPI	Speed
HP LaserJet 2000	1	LPT1:	0	A4 210 x 297 mm	300	20

3.3.2.5.3 Video configuration

With this report you can find computers with non-optimal video settings or with an outdated video adapter.
For example, it's recommended to set the vertical refresh frequency of a computer monitor to

a value greater than 70 Hz in order to avoid eyestrain. In order to select computer that don't match this rule
Check *Lower than* for criterion
Check only the field *Refresh frequency*
Enter 70 as refresh frequency limit
Click the *Display* button in order to view the report



Video Configuration

Video configuration for computers on which
The video horizontal resolution is lower or equal than 800 pixels

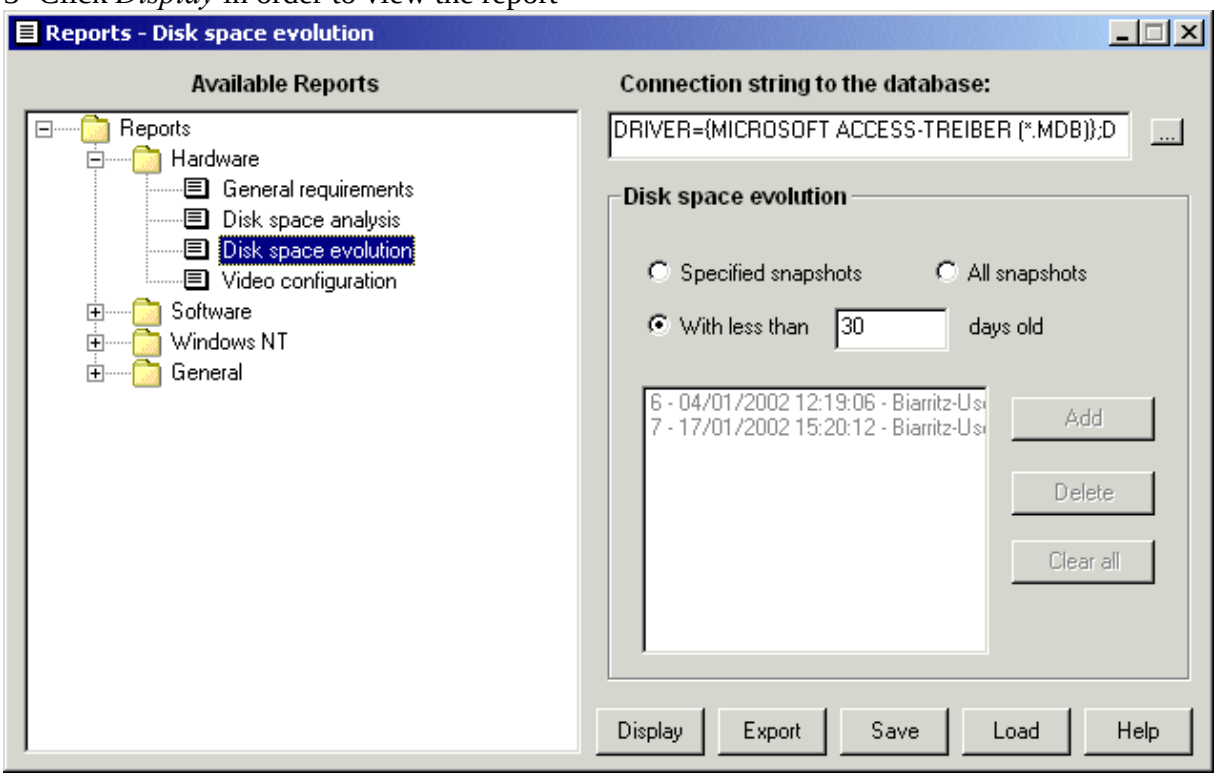
Computer	Memory (MB)	Resolution	Bits	Refresh rate (Hz)
BIARRITZ				
JN	16,0	800 X600	16	75
USERLOCK				
TEST1	8,0	800 X600	16	85
TEST3	2,0	800 X600	16	75

3.3.2.6 Use

3.3.2.6.1 Disk space Evolution

This report allows you to follow the free disk space evolution for all volumes of your Windows NT network.
In order to use this report you need to launch several scans with the "*Use snapshots*" option in order not to always delete the previous snapshots of your network. You can for example schedule a scan each week.
You have three possibilities in order to select the snapshots to use:
- All snapshots
- Snapshots with less than *xx* days (younger than)
- Manually selected snapshots

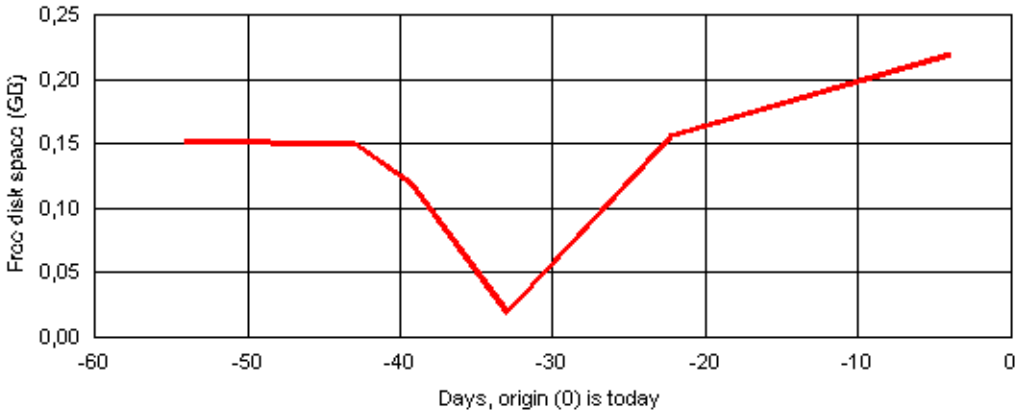
For example you want to see the free disk space evolution over the latest month.
1- Select *With less than*
2- Enter *30* as days count. You see then in the list the snapshots with less than 30 days old.
3- Click *Display* in order to view the report



JN

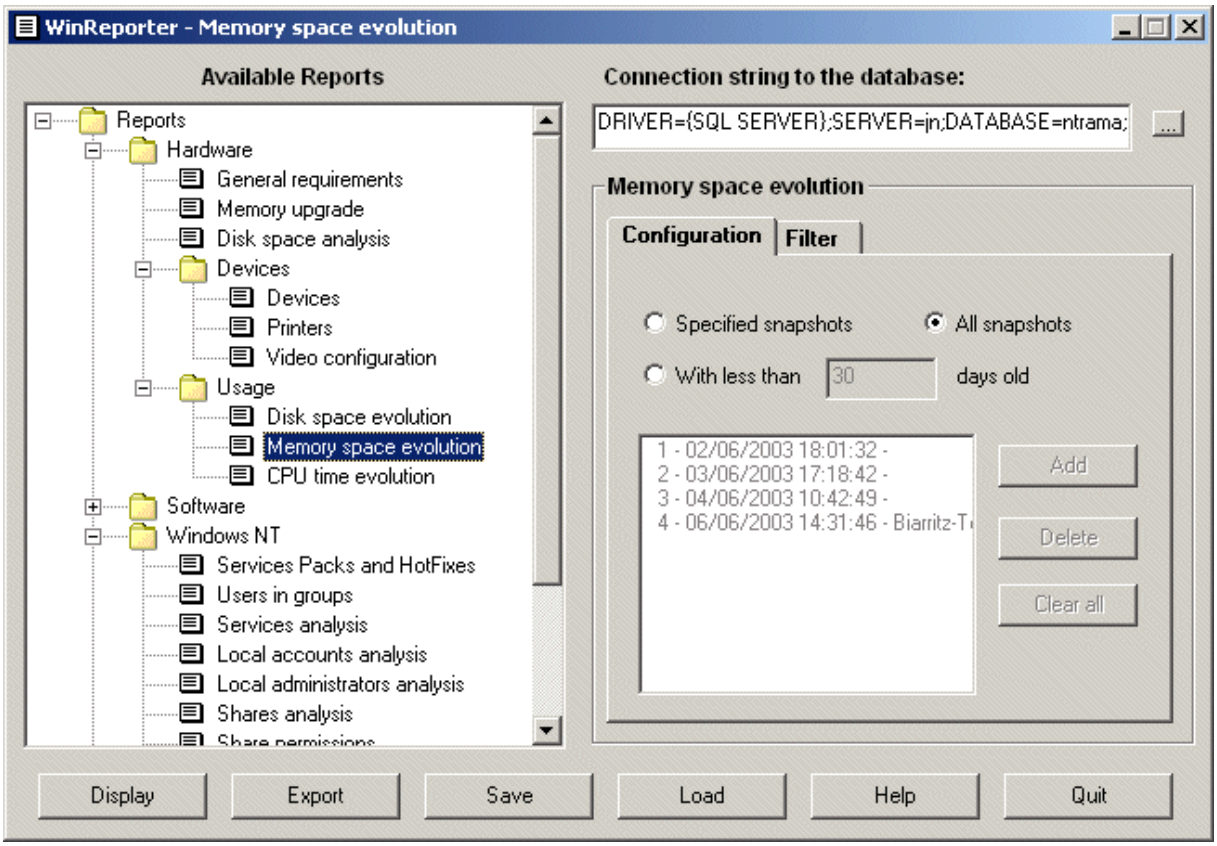
C:

Date	Free space (GB)
15/11/2001 16:53:59	0,15
26/11/2001 17:47:09	0,15
30/11/2001 09:28:31	0,12
06/12/2001 15:07:01	0,02
17/12/2001 09:40:16	0,16
04/01/2002 12:19:06	0,22



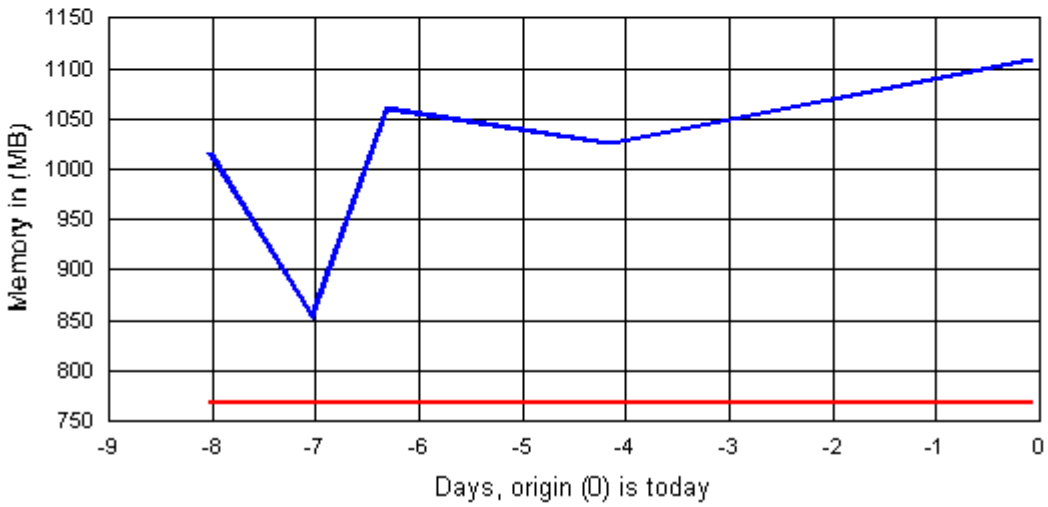
3.3.2.6.2 Memory space evolution

The report allows you to follow the evolution of the memory space in use. The configuration of this report is explained in the Disk space evolution report.
The red trace in the graphic is the physical RAM and the blue trace is the memory in use. If more memory is used as available RAM the computer use swap files as virtual memory.



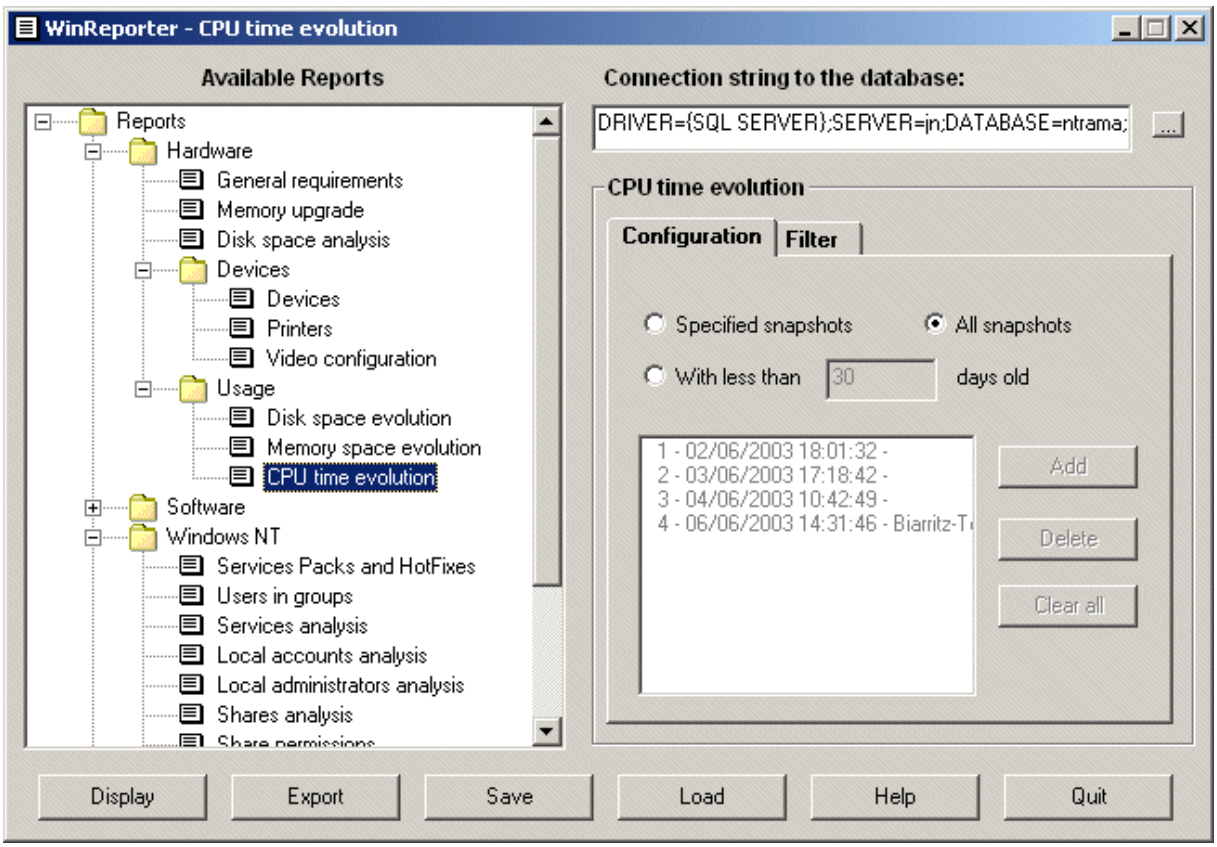
TAFSERVER

Date	RAM (MB)	Memory in use (MB)
02/06/2003 16:01:33	768	1015
03/06/2003 15:18:46	768	855
04/06/2003 08:42:53	768	1061
06/06/2003 12:31:52	768	1026
10/06/2003 14:04:09	768	1109



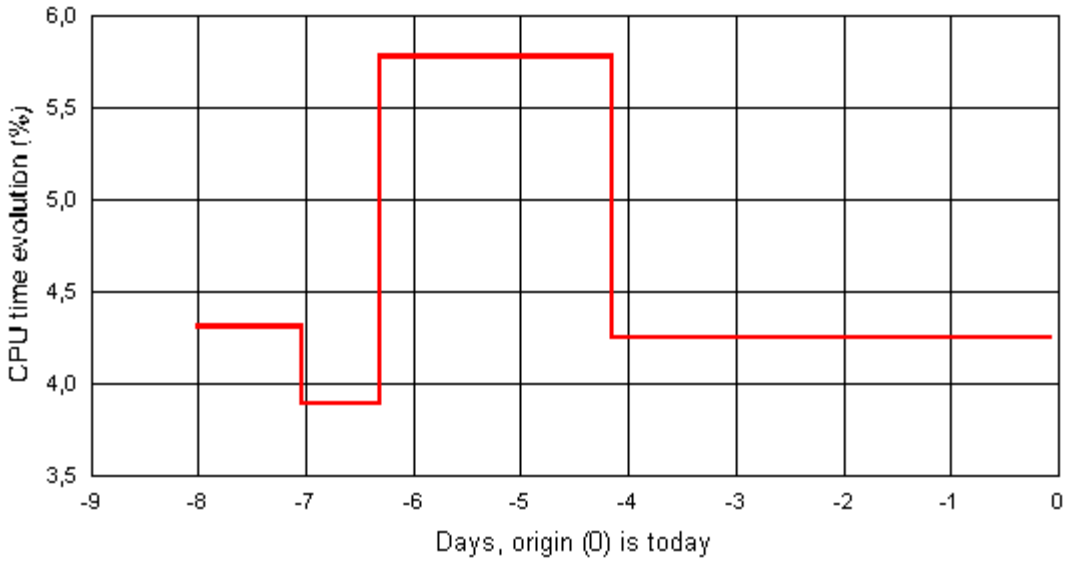
3.3.2.6.3 Processor time evolution

The report allows you to follow the used processor time. Counter to two other evolution reports this report displays an average value between two snapshots rather than an instantaneous value for each snapshot. An oblique line means that the computer rebooted between two snapshots and that in consequence the report cannot set an average value for this time interval.
See the disk space evolution report for the configuration.



TAFSERVER

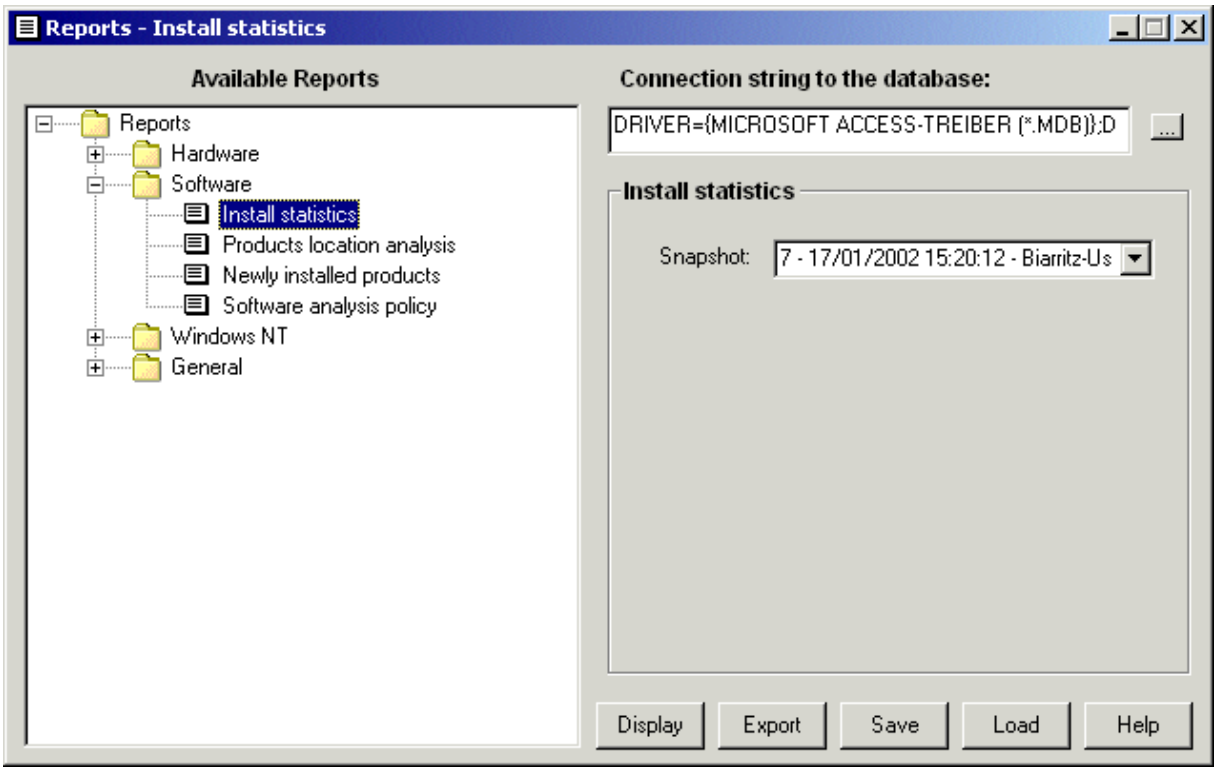
Time interval		Average CPU time
01/05/2003 12:40:28	02/06/2003 16:01:33	7,95%
02/06/2003 16:01:33	03/06/2003 15:18:46	4,31%
03/06/2003 15:18:46	04/06/2003 08:42:53	3,89%
04/06/2003 08:42:53	06/06/2003 12:31:52	5,78%
06/06/2003 12:31:52	10/06/2003 14:04:09	4,25%



3.3.3 Software

3.3.3.1 Install statistics

This report allows you to know on how many computers a product is installed in your network in order to check if you don't exceed the number of bought licenses.


Reports - Install statistics
Available Reports
Reports
Hardware
Software
Install statistics
Products location analysis
Newly installed products
Software analysis policy
Windows NT
General
Connection string to the database:
DRIVER={MICROSOFT ACCESS-TREIBER (*.MDB)};D
...
Install statistics
Snapshot:
7 - 17/01/2002 15:20:12 - Biarritz-Us
Display
Export
Save
Load
Help

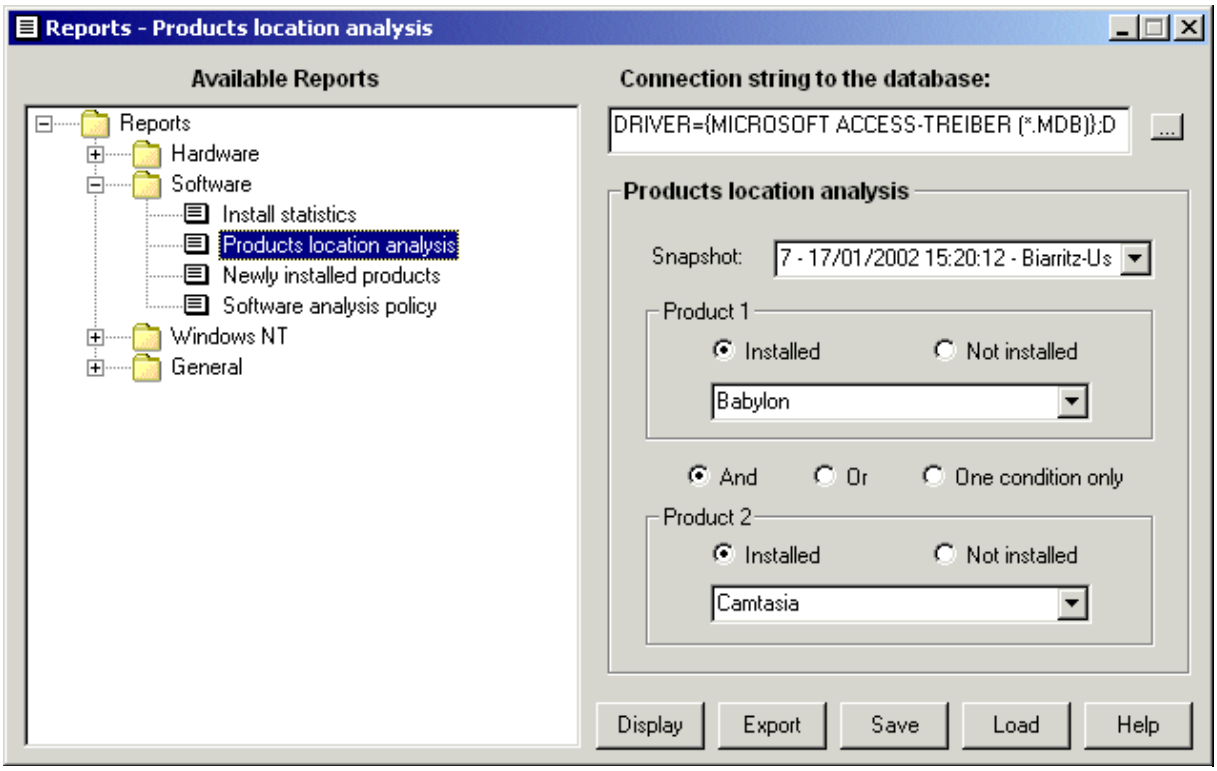
USERLOCK

Adobe Acrobat 5.0	1	25,0%
Chinese (Simplified) Language Support	1	25,0%
Communautest	2	50,0%
CommView	2	50,0%
Dell ResourceCD	1	25,0%
Disk Commander	1	25,0%
ERD Commander 2000	1	25,0%
EvenTrigger	4	100,0%
FAT32 for Windows NT 4.0	1	25,0%
FileAudit	3	75,0%
Find... On the Internet	2	50,0%
MailChecker	1	25,0%
Microsoft Internet Explorer 4.0	1	25,0%
Microsoft Internet Explorer 5.5 and Internet Tools	1	25,0%
Microsoft Internet Explorer 6 and Internet Tools	1	25,0%
Microsoft Music Control	2	50,0%
Microsoft Office 2000 Developer Tools	1	25,0%
Microsoft Office 2000 SR-1 Premium	1	25,0%
Microsoft Outlook Express	1	25,0%
Microsoft Outlook Express 5	1	25,0%
Microsoft Outlook Express 6	1	25,0%
Microsoft Visual Studio 6.0 Enterprise Edition	1	25,0%
Microsoft Wallet	2	50,0%
Microsoft Web Publishing Wizard 1.53	2	50,0%
Microsoft Windows Media Player 6.4	2	50,0%
Microsoft XML Parser	1	25,0%
MonitorMagic	1	25,0%
MSDE	1	25,0%
MSN Messenger Service 3.0	2	50,0%
NetMeeting 3.01	1	25,0%
NTRama	3	75,0%

Install Statistics - 19/12/2001 11:32:57 - 2 / 3

3.3.3.2 Products location analysis

This report is designed to locate computers on which a specified product is installed or not installed.
If you use the second condition you can define a more complex filter. For example, you can display the computers on which a product1 is installed and a product2 is not installed.
For example, to display computers on which the product *FileAudit* is not installed:
Choose the snapshot
Check *Not Installed* in the *Product 1* frame
Choose *FileAudit* in the available products list in the *Product 1* frame.
Check *One condition only*
Click the *Display* button



Products location

Computers on which the product "UserLock 2000" is not installed

BIARRITZ

JN

USERLOCK

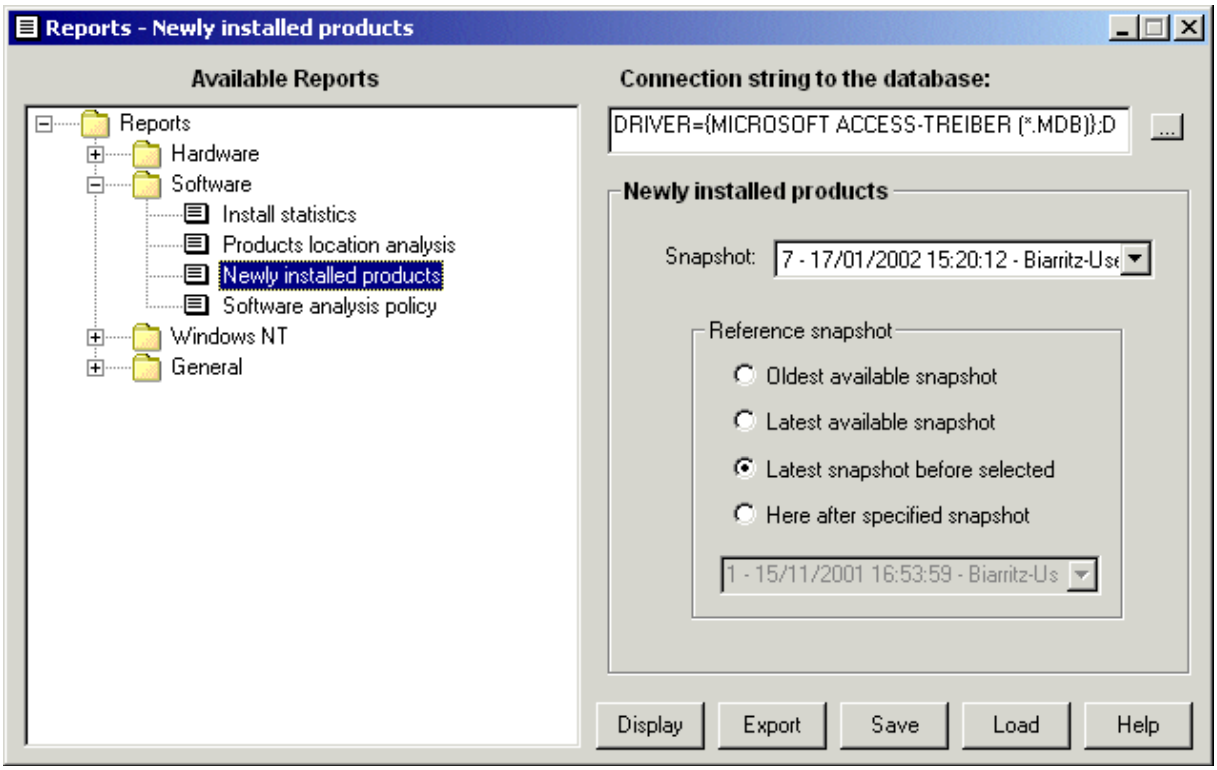
TEST3 TEST4

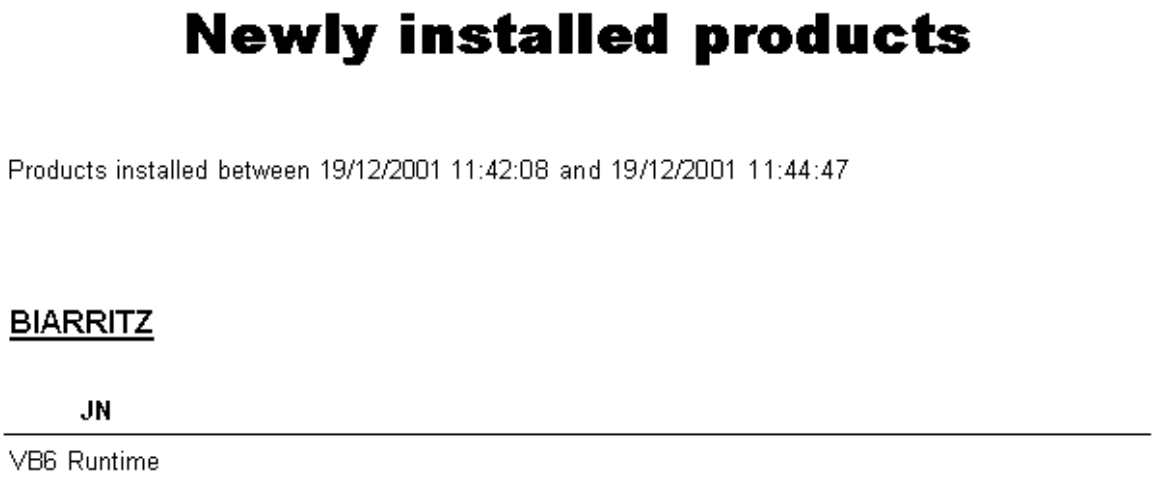
TEST5

3.3.3.3 Newly installed products

With this report you are able to monitor the evolution of installed software on your network. You can find all products installed between two dates (dates of two snapshots). In order to do this you need to select the actual snapshot and a reference snapshot.
The reference snapshot can be chosen automatically in three manners:
- The oldest available snapshot in your database
- The latest snapshot available in your database
- The previous snapshot to the currently selected

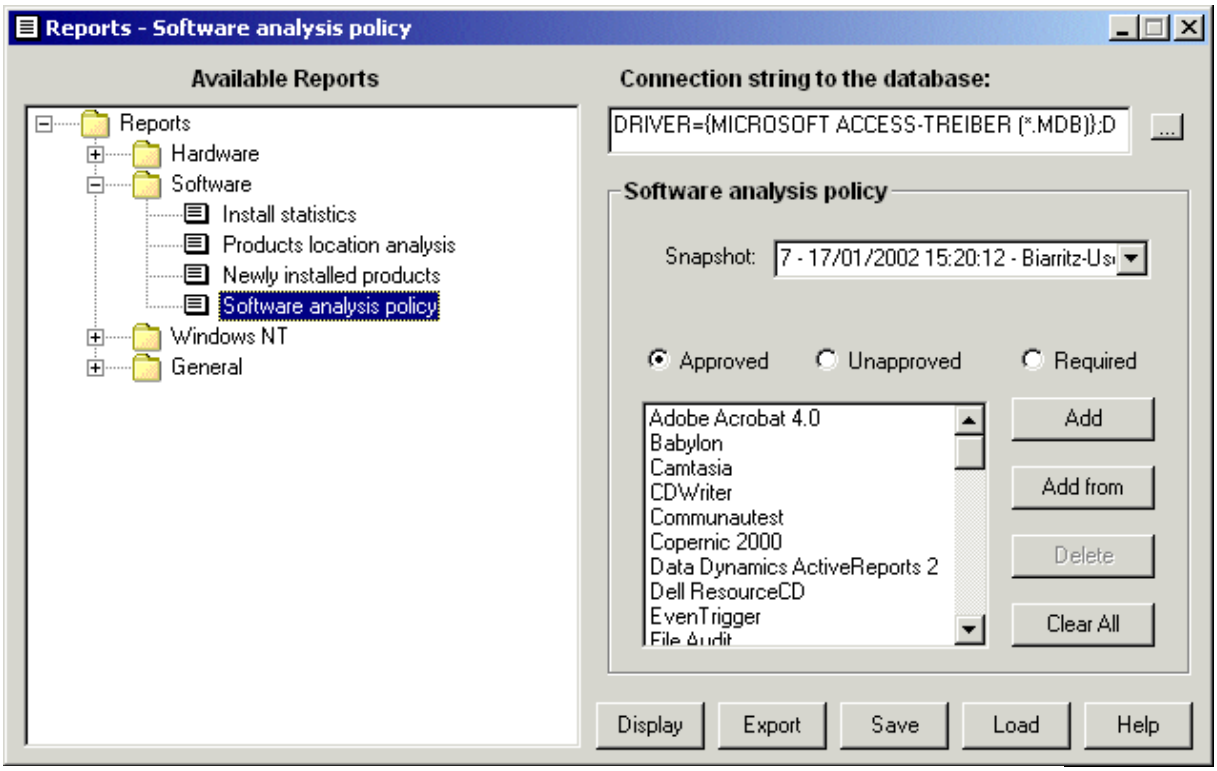
The reference snapshot can even be manually selected





3.3.3.4 Software analysis policy

With this report you can find computers with unapproved products installed. You have two ways to find them.
- You can specify all approved products in the list *(Approved* must be checked). You can easily complete the list with the *Add from* button. This button allows you to add all products installed on a clean computer.
- You can specify all unapproved products in the list (*Unapproved* must be checked)
You can even find with this report computers with missing required products. To do this, check *Required* and add the required products in the list and click *Display* to view the report.



Software analysis

List of computers with unapproved products

BIARRITZ

JN

Babylon
Camtasia
WinZip
Babylon Translator
DivX Codec 3.1alpha release

USERLOCK

TEST1

Disk Commander
WinZip

TEST3

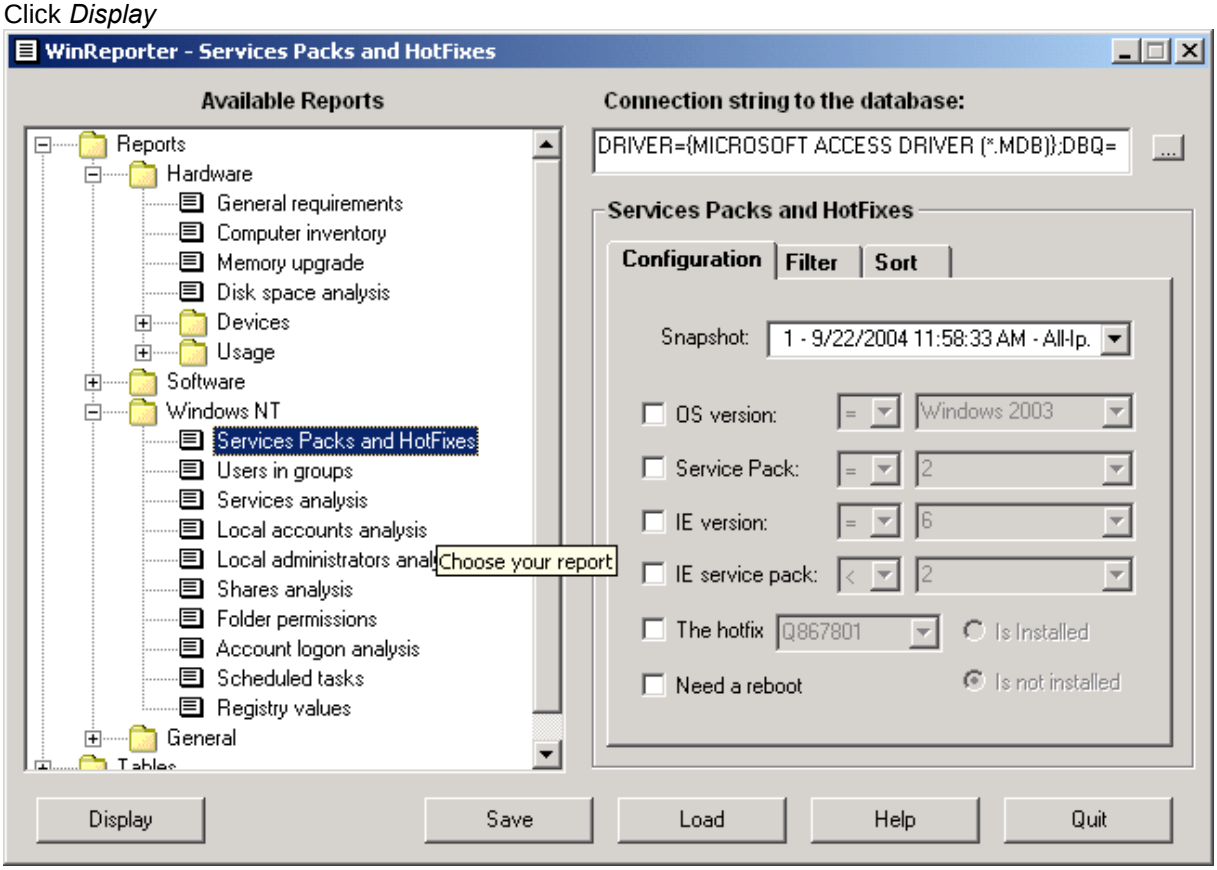
WinZip

3.3.4 Windows NT

3.3.4.1 Services Packs and HotFixes

This report is designed to search computers that are not up to date concerning Microsoft services packs, Internet Explorer versions and hot fixes.

The report also show when computers need a reboot and can filter them on this state. A computer needs a reboot when file updates are scheduled for the next reboot. So updates may not be effective on computers in this state.
For example if you want to find all computers under windows 2000 with a service pack lower or equal than 2 and without a specific preSP3 hot fix installed:
Choose the snapshot
Check *Operating System* and select *Windows 2000*
Check *Service Pack Number lower than* and select 3
Check *The hot fix* and select the hot fix in the available hot fixes list
Check *Is not Installed*
Click *Display*



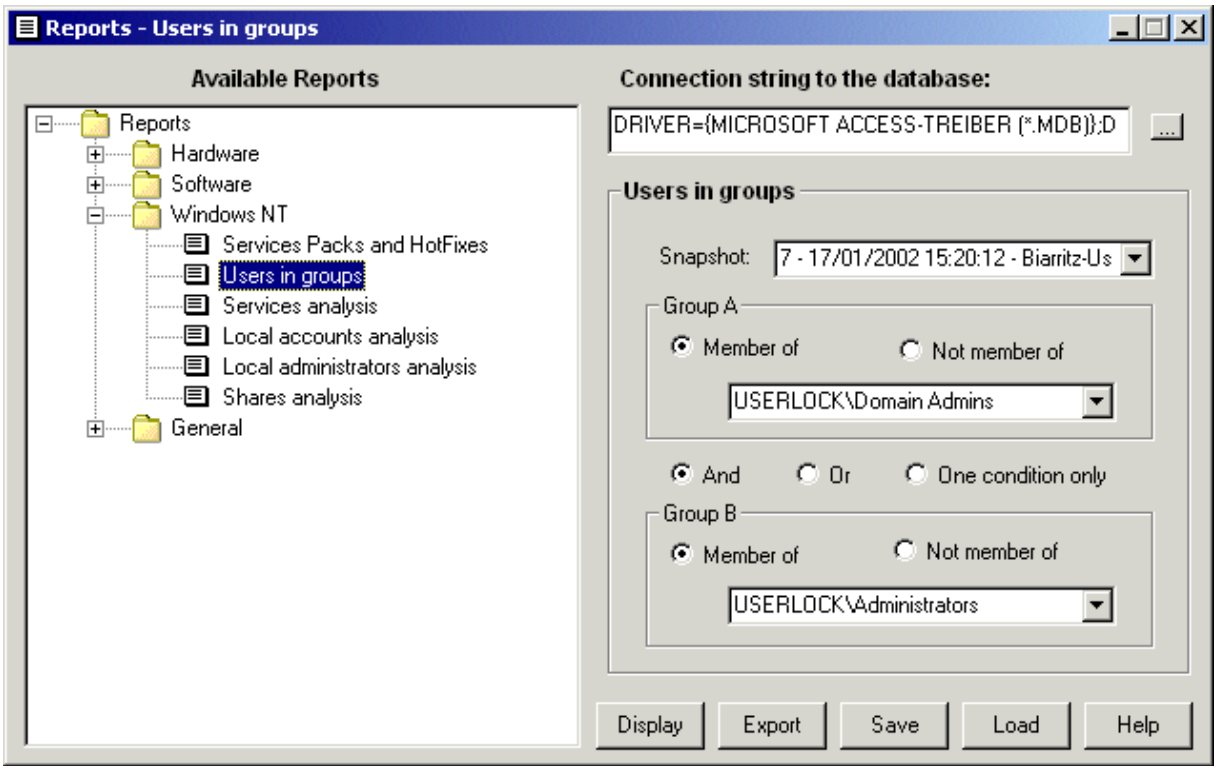
Services Packs and HotFixes

Computer	Operating system	Service Pack	Internet Explorer
RECOVERDOMAIN			
TEST4	Windows 2000	Service Pack 4	6.0 SP1
TEST5	Windows 2000		5.0
TESTDOMAIN			
TEST1	Windows NT 4	Service Pack 6	5.5 SP1
TEST15	Windows XP	Service Pack 2	6.0 SP2
TEST16*	Windows XP	Service Pack 2	6.0 SP2
TEST3	Windows NT 4	Service Pack 6	5.0 SP2

Selected computers: 6

3.3.4.2 Users in groups

This report allows you to list:
Users member of a specific group
Users member of two specified groups
Users member of a first group but not member of a second group
And other combination
For example, if you want to list users member of both group *users* and *domain admins*:
Choose the snapshot
In the *Group A* frame, check *Member of* and select the group *MYDOMAIN\users*
Check *And*
In the *Group B* frame, check *Member of* and select the group *MYDOMAIN\Domain Admins*
Click Display



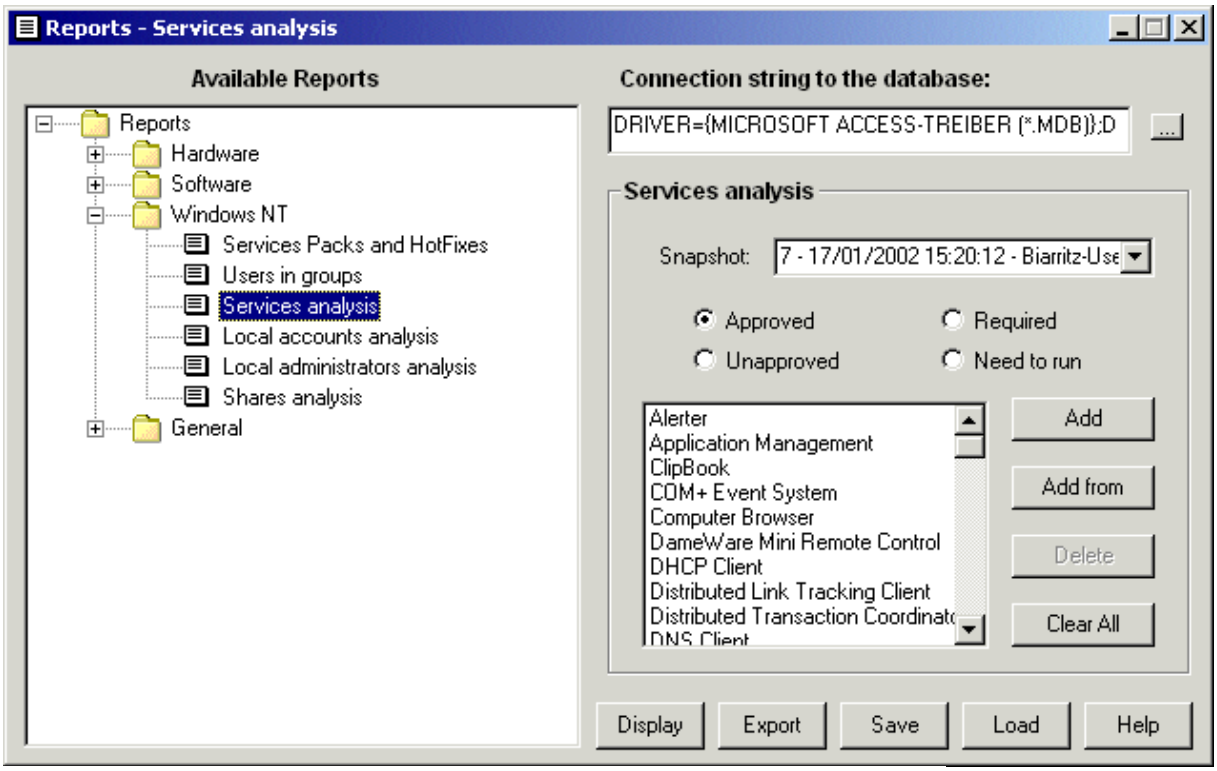
Users in Groups

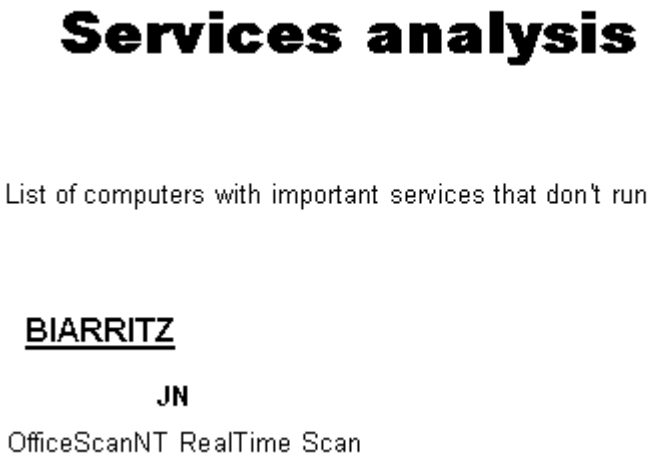
List of users member of the group "USERLOCK\Domain Admins" and member of the group "USERLOCK\Administrators"

USERLOCK\aa	USERLOCK\administrator
USERLOCK\jnh	

3.3.4.3 Services analysis

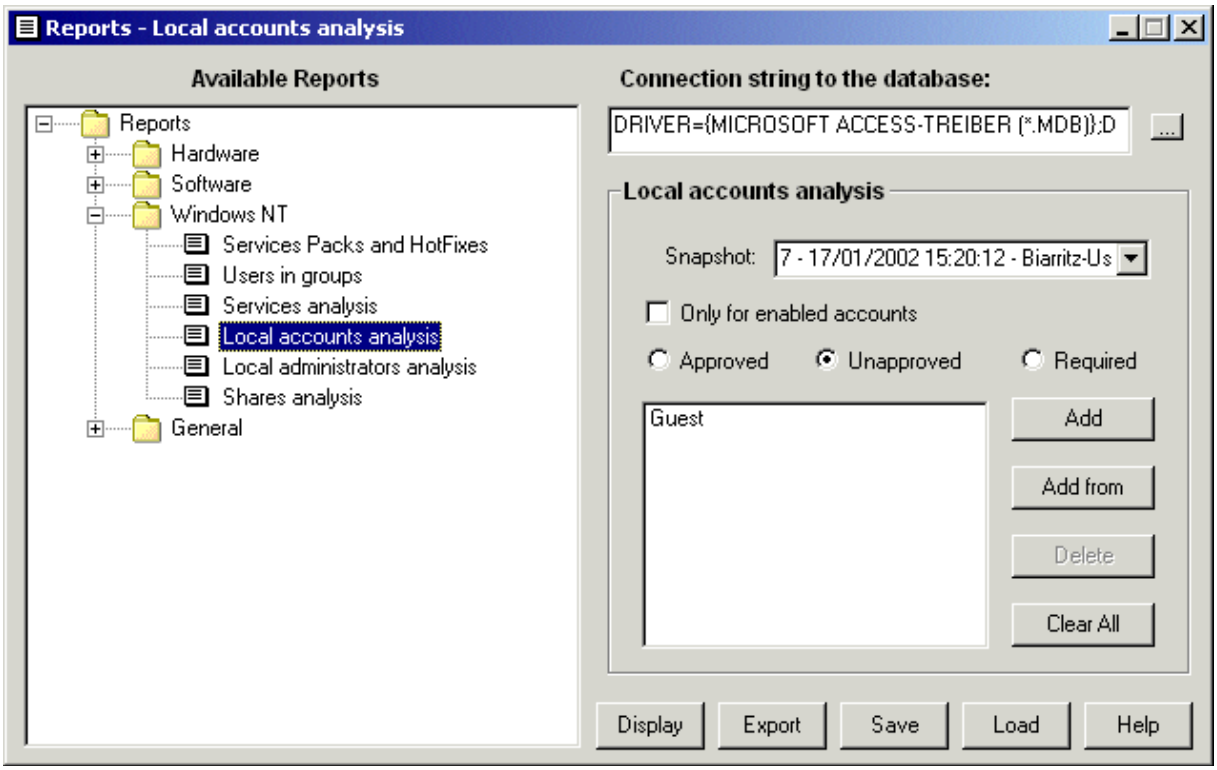
This report allows you to search for unapproved Windows NT services, missing required Windows NT services or stopped services needing to run. The configuration of this report is similar to the report Software analysis.
For example to check if your real-time antivirus is running on your all workstation.
Choose the snapshot
Select *Need to run*
Click *Add* after empty the service list
Select the service name of your real-time antivirus and click *Ok*
Click *Display*





3.3.4.4 Local accounts analysis

This report is designed to find computers with unapproved local accounts or with missing required local accounts. The configuration is similar as the report Software analysis.
If you check *Only enabled accounts*, then disabled accounts won't appear in the report.
For example, if you want to list computers with the *Guest* account enabled:
Choose the snapshot
Select *Unapproved*
Check *Only for enabled account*
Click the *Add* button
Select the *Guest* account and click *Ok*
Click *Display*



Local Accounts analysis

Computers with an unapproved local account.

BIARRITZ

JN

Guest

USERLOCK

TEST4

Guest

3.3.4.5 Local administrators analysis

This report is designed to find computers with unapproved local administrators or missing required local administrators. The configuration of the report is similar to the report Software analysis.

The local accounts names are listed using the generic name LOCAL\LocalAccountName and the domain accounts are listed under *DOMAIN\UserName*.

For example, you may suspect that the user *MyUser* of the domain *MyDomain* has obtained the administrative rights of several workstations. To find the concerned workstations:

Select the snapshot

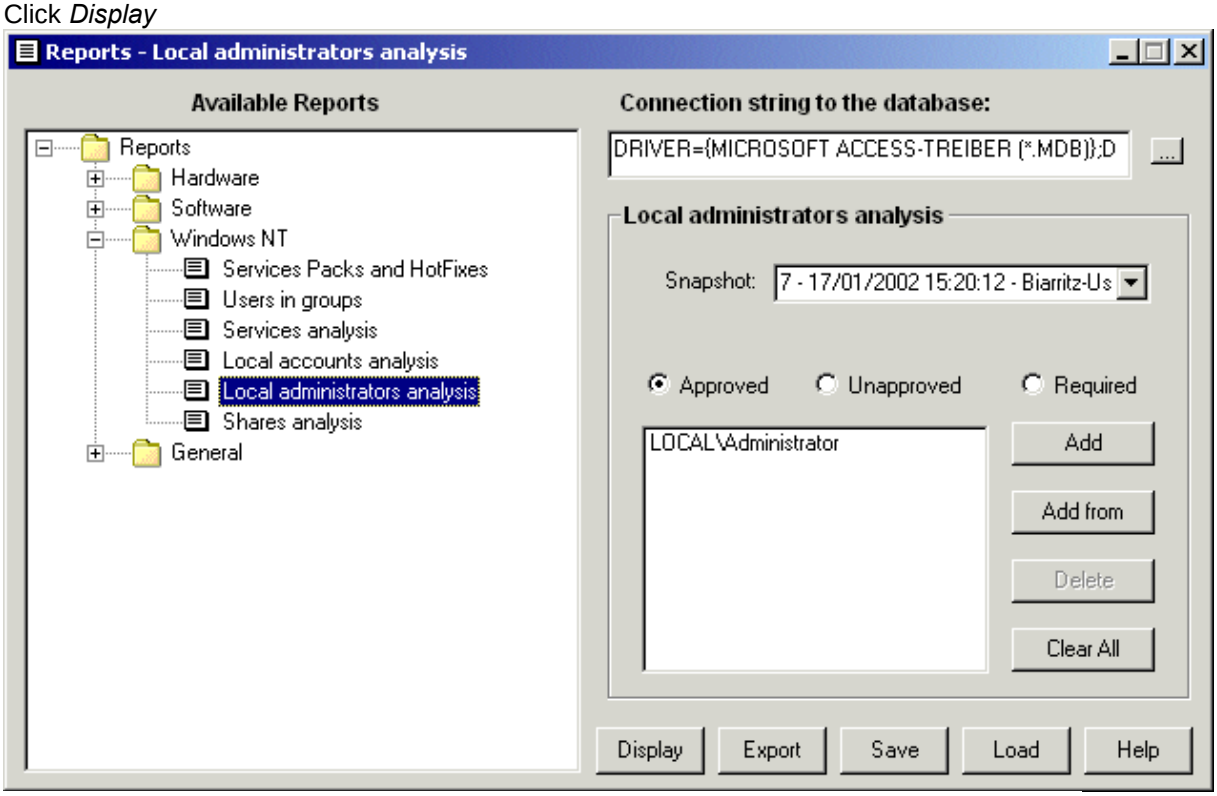
Check *Unapproved*

Click *Add*

Select the user *MYDOMAIN\MyUser* in the available account list and click *Ok*

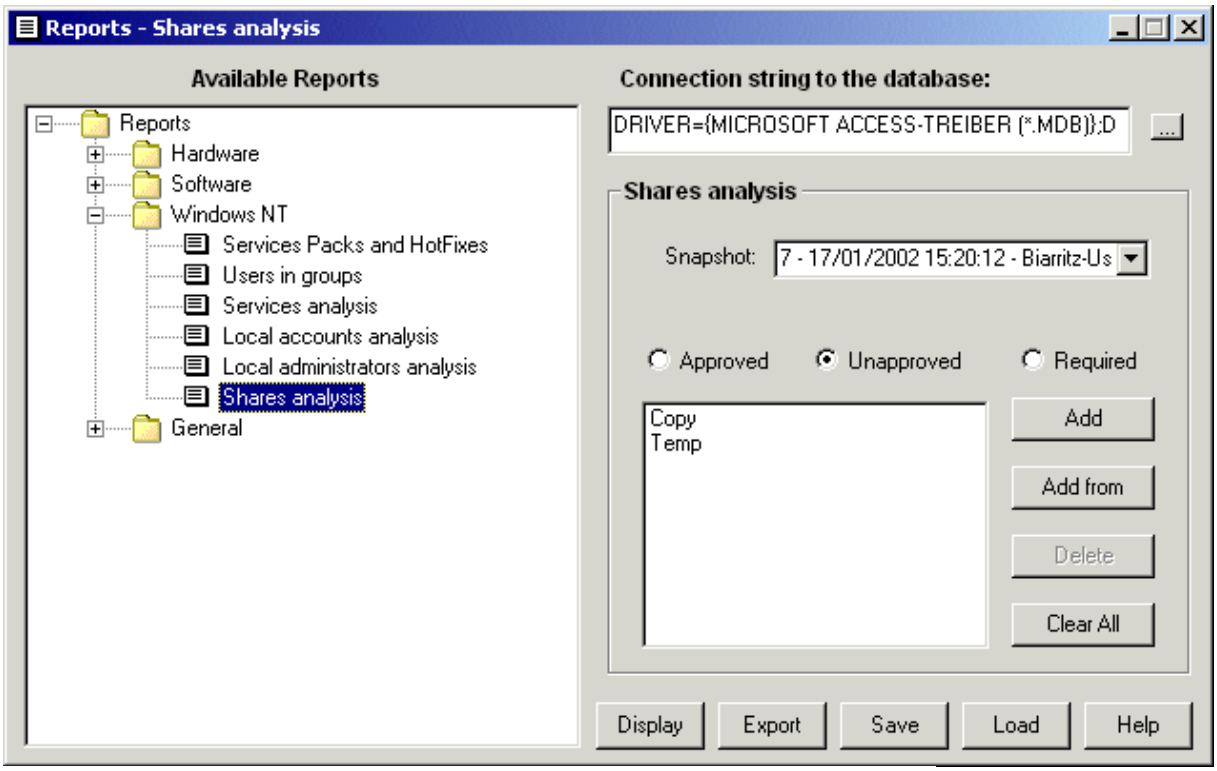
Click *Display*

Other example you want only the default administrator account as administrator on your all workstations:
Select the snapshot
Check *Approved*
Click *Add*
Select *LOCAL\Administrator* in the available account list and click *Ok*
Click *Display*



3.3.4.6 Shares analysis

This report is designed to list computers with unapproved shares or missing required shares. The configuration of the report is similar that the report Software analysis.



Shares analysis

Computers with unapproved shares.

BIARRITZ

JN

Copy

USERLOCK

TEST1

Copy

TEST3

Copy

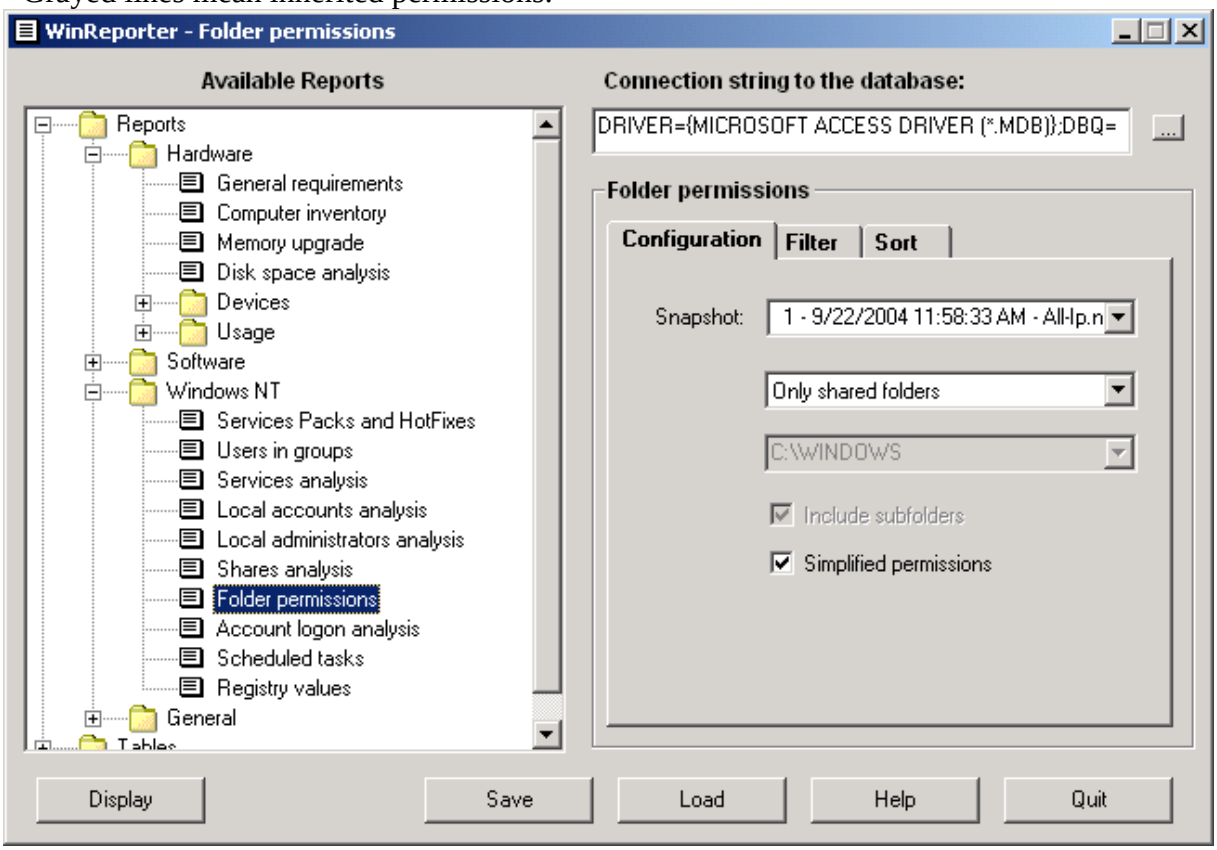
TEST5

Temp

3.3.4.7 Folder Permissions

This report displays NTFS permissions of all scanned folders.

In a standard scan only the root of shared folders are scanned. If you want to display permissions on other folders you need to start a scan with the advanced wizard; in the software step, check "Scan folders", "Get permissions" and specify "Folder restrictions" or check "In shared folders only" if you don't want to scan all folders.
You can display permissions only for shared folders, for all scanned folders or for a specified folder with/without its subfolders.
- In order to minimize the report, All subfolders with same permissions as their parent folder are not displayed.
- You can choose to display simplified permissions (RWXD).
- You will find the explanation of all permissions at the end of the report.
- Grayed lines mean inherited permissions.



TEST5

ADMIN$

Owner: TEST5\Administrators
Local path: C:\WINNT

		R	W	X	D	DF	CP	TO
\CREATOR OWNER	Allow	☑	☑	☑	☑	☑	☑	☑
\Everyone	Allow	☑	☐	☑	☐	☐	☐	☐
NT AUTHORITY\SYSTEM	Allow	☑	☑	☑	☑	☑	☑	☑
TEST5\Administrators	Allow	☑	☑	☑	☑	☑	☑	☑
TEST5\Power Users	Allow	☑	☑	☑	☑	☐	☐	☐
TEST5\Users	Allow	☑	☐	☑	☐	☐	☐	☐

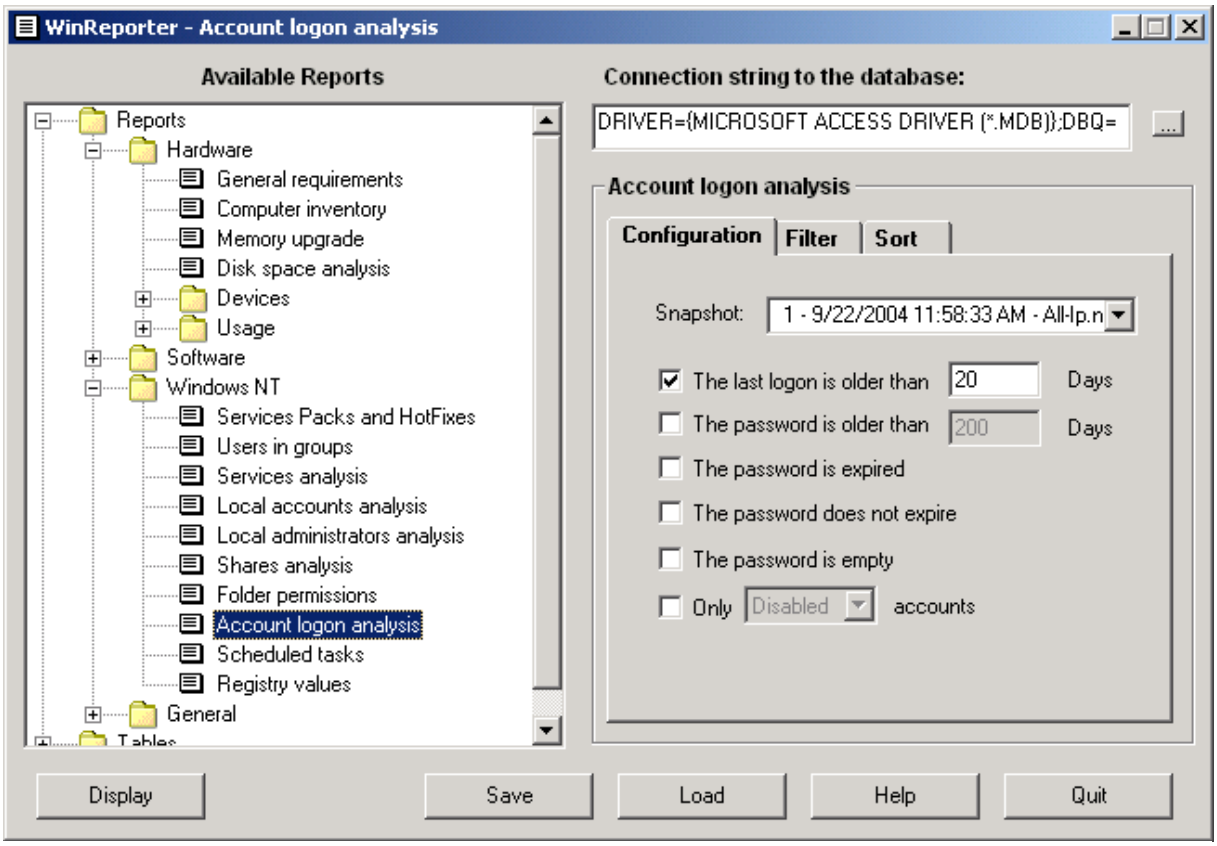
C$

Owner: TEST5\Administrators
Local path: C:\

		R	W	X	D	DF	CP	TO
\Everyone	Allow	☑	☑	☑	☑	☑	☑	☑

3.3.4.8 Account logon analysis

The report allows you to display user accounts according to: Latest logon time, passwords age, empty passwords, expired passwords, permanent passwords and account status (enabled/disabled).
Warning! Empty passwords are only scanned for domain accounts. Additionally if you launch the scan from a Windows XP workstation empty password should be allowed for network logon in the local security policy.



Account logon analysis

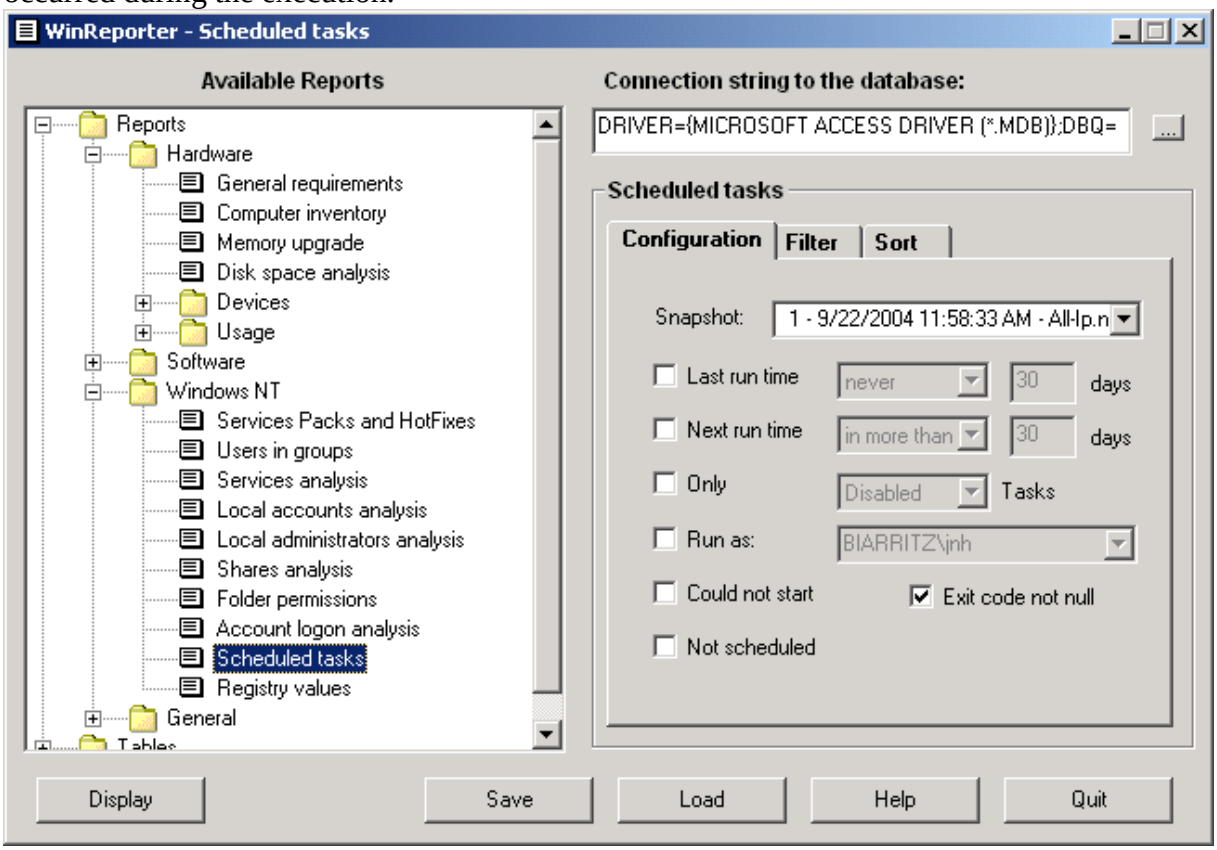
Account filter:
- Last logon is older than 20 days

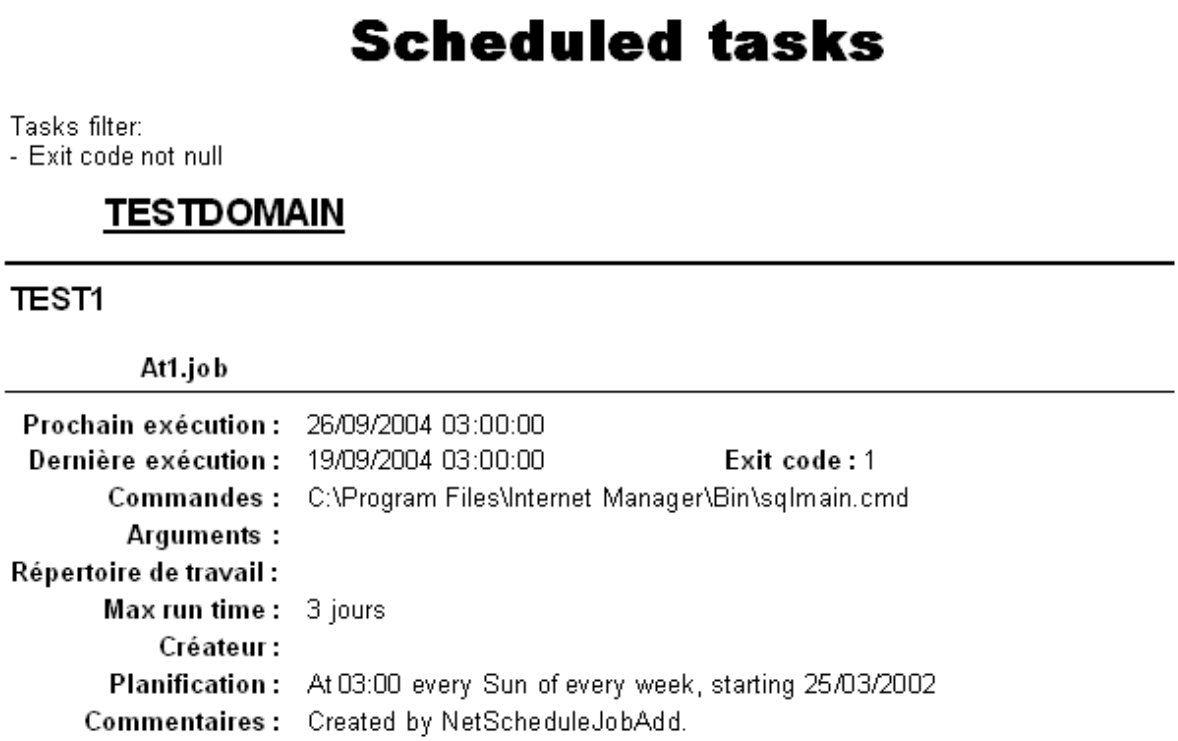
Additional computer filter:
-Only for the domain: TESTDOMAIN

Account			Password		
Name	Last logon	Disabled	Age (days)	Empty	Expired	Never expire
TESTDOMAIN						
aurélie	18/09/2002 16:18:56	☐	735		☑	☐
AutoAdmin	07/07/2004 12:00:28	☐	391		☐	☑
gf	20/09/2004 18:30:36	☐	2		☐	☐
Guest		☑	0		☐	☑
help	12/06/2003 12:18:38	☐	468		☑	☐
kl	13/11/2002 17:27:12	☐	687		☑	☐
testeur	05/08/2004 16:12:08	☐	194		☐	☑
testeur1	08/03/2004 17:16:34	☐	296		☐	☑
testeur2	05/03/2004 11:10:07	☐	219		☑	☐
testeur3	13/02/2004 21:43:09	☐	222		☑	☐
titi	30/04/2003 15:32:42	☐	513		☑	☐

3.3.4.9 Scheduled Tasks

The report displays all tasks according to: last run time, next run time, task status (enabled/disabled), execution account, task startup status, task error code (returned by the process) or if the task is not scheduled.
In addition to the previously listed elements, the report also displays for each task: the command line, the working folder, the maximum run time and the schedule.
With this report you will be able to easily list all tasks that did not start or for which errors occurred during the execution.





Scheduled tasks

Tasks filter:
- Exit code not null

TESTDOMAIN

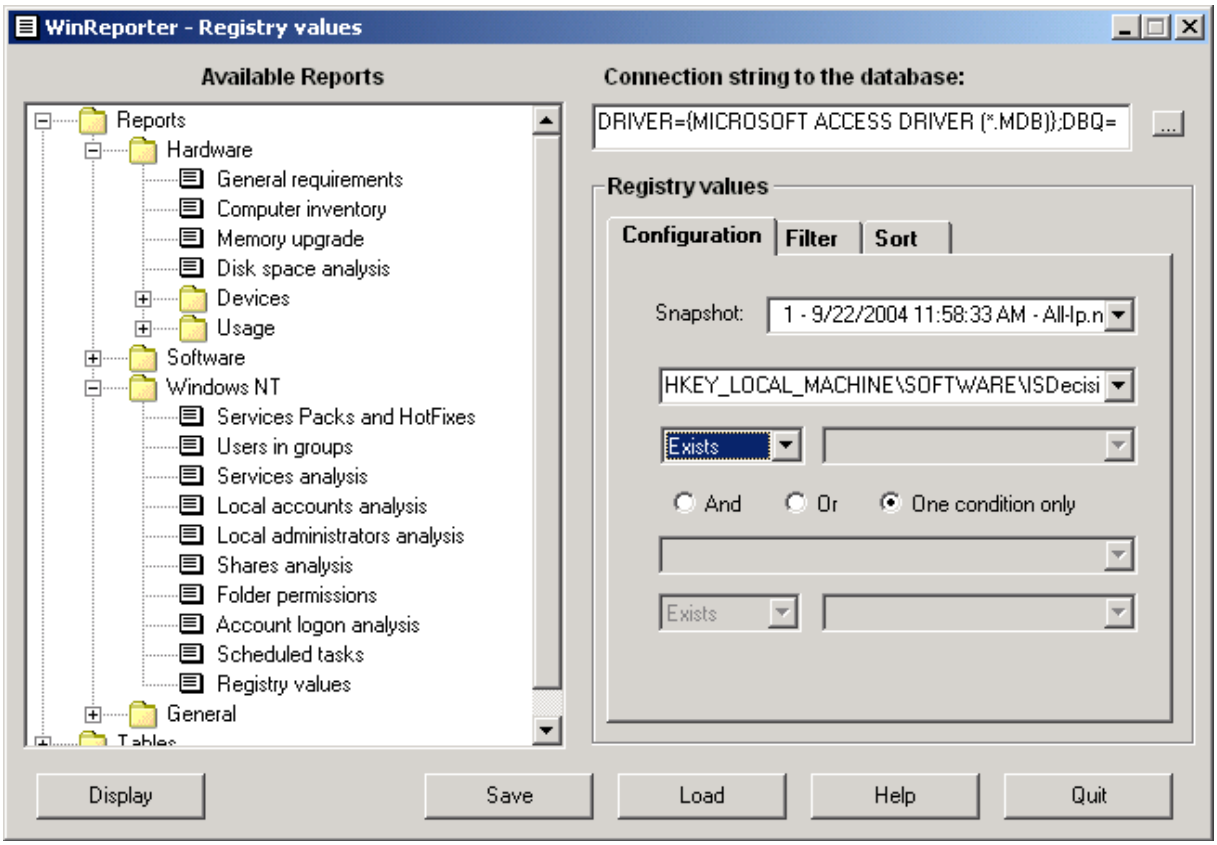
TEST1

At1.job

Prochain exécution :	26/09/2004 03:00:00
Dernière exécution :	19/09/2004 03:00:00 **Exit code :** 1
Commandes :	C:\Program Files\Internet Manager\Bin\sqlmain.cmd
Arguments :	
Répertoire de travail :	
Max run time :	3 jours
Créateur :	
Planification :	At 03:00 every Sun of every week, starting 25/03/2002
Commentaires :	Created by NetScheduleJobAdd.

3.3.4.10 Registry Values

To use this report you need to start the scan with the advanced scan wizard (Windows NT step) and specify the registry values you want to scan. To do this, copy for each value, the path and the name from regedit and merge them as follows: %pathname%\%ValueName%. The report allows you to list computers according to a filter on one or two registry values. Allowed conditions are: exists, doesn't exist, is equal, is different, is lower, is greater, is lower or equal, is greater or equal, contains, and doesn't contain a specified value.



Registry values

HKEY_LOCAL_MACHINE\SOFTWARE\ISDecisions\WinReporter\LicenseKey

TESTDOMAIN

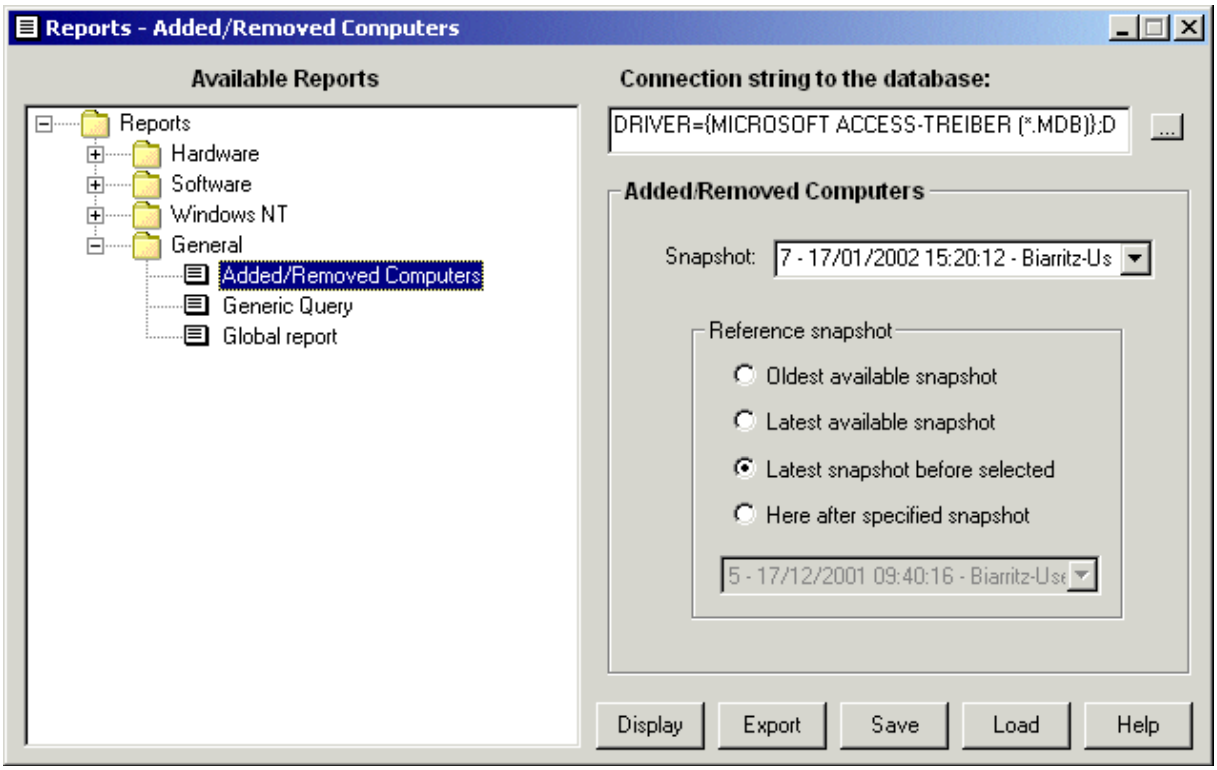
The value or the key doesn't exist!

TEST15	TEST16

3.3.5 General

3.3.5.1 Added/removed computers

With this report you can list all newly added or removed Windows NT computers (between two snapshots). The configuration of this report is almost similar to the *New Products* report. For example, you may want to print each month the list of the added/removed computers. Schedule a scan for each month with the "Use snapshots" option in order to always keep the old snapshots.
When the monthly snapshot is completed select it in the available snapshots list
Select *Latest snapshot before selected* as reference snapshot
Click *Display*



Added/Removed Computers

List of added and supressed computers in the following period: 13/12/2001 17:22:47 to 19/12/2001 11:32:57

List of added computers

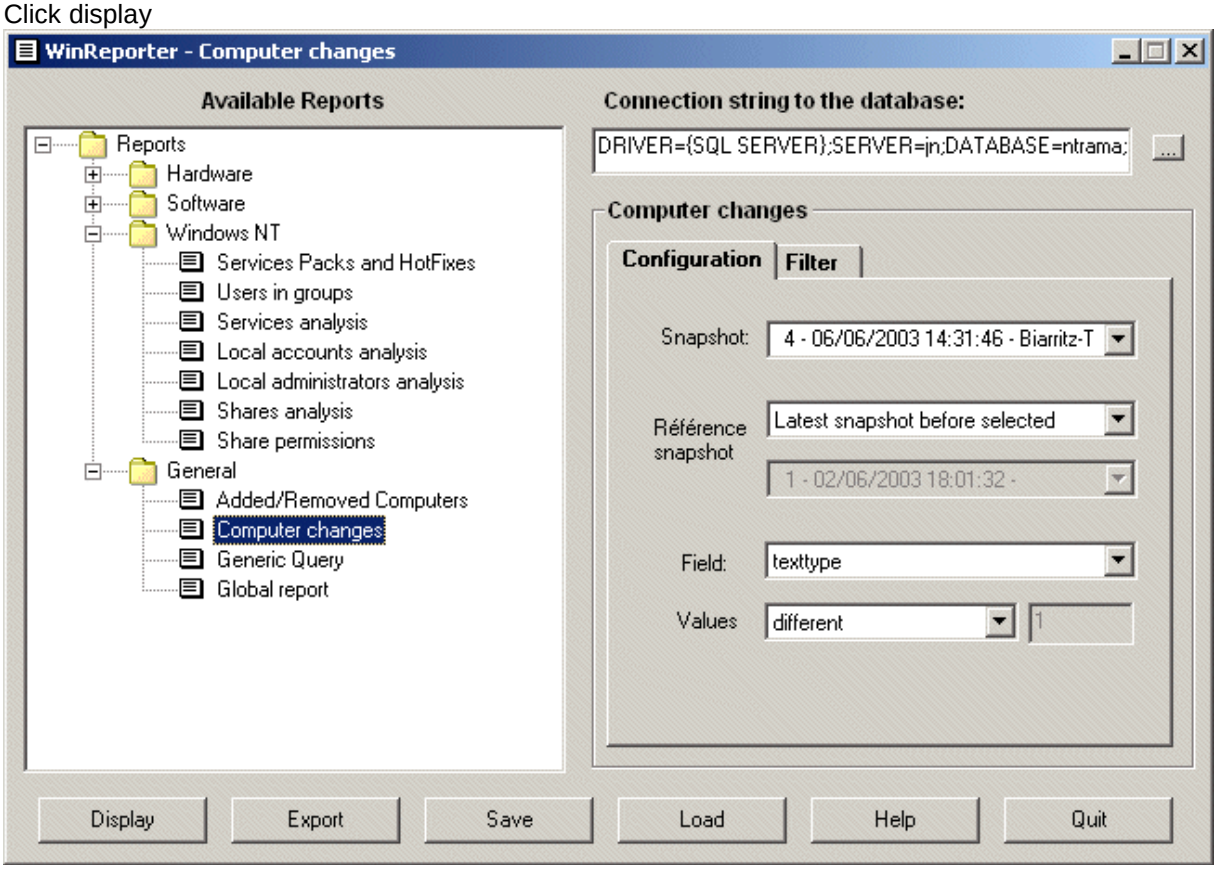
USERLOCK

TEST1	TEST3
TEST4	TEST5

3.3.5.2 Computer changes

In this report you will be able to find computers on which settings have changed. The old and the new value are displayed and for numeric values the difference is displayed too. For example if you want to list all computers on which you made a memory upgraded. You need to:
Launch a scan before your intervention on computers
Launch a scan after the intervention
In the report configuration select the second snapshot
Select latest snapshot before selected
Select *Memory* as information
Select different for Values

Click display



Computer changes

List of computers on which the field "ramUsed"
Is different beetween 02/06/2003 18:01:32 and 10/06/2003 16:04:06

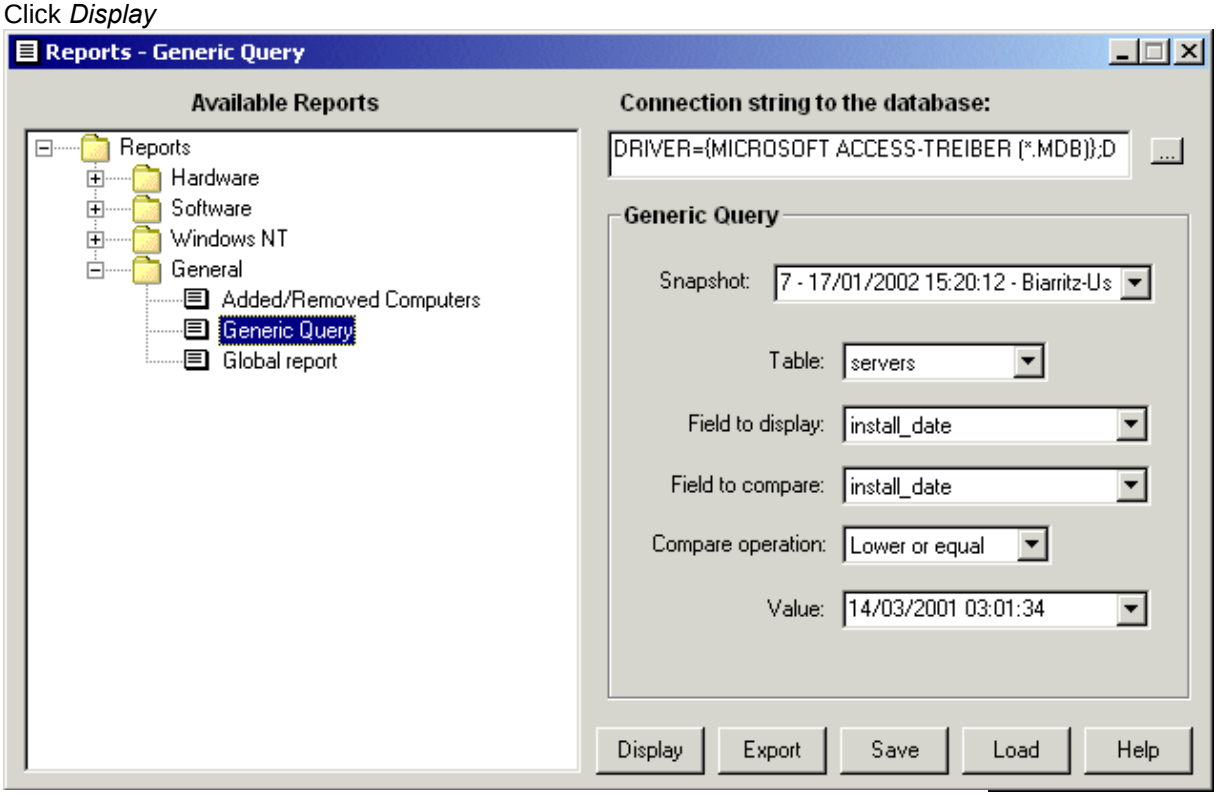
Additional computer filter:
-Only for the domain: TESTDOMAIN

Computer	Reference	Current	Difference
TESTDOMAIN			
TEST1	122	142	20
TEST4	112	109	-3
TEST5	44	46	2

3.3.5.3 Generic Query

This report allows the user to make a customized query over the database.
In order to do this you need to:
Select the snapshot
Select the Table
Select the field of the table that will be displayed in the report
Select the field of the table that will be used for the comparison
Select the compare operator (Equal, Different, Greater....)
Enter the value that will be used in the comparison
Click *Display*
You can find information about all tables of the database and their fields in the database reference.

Only the tables directly linked to the *servers* table can be used in the report because the result is grouped by computers.
Example: you want to display all computers with "x86 Family 6 Model 5 Stepping 2" as processor:
Choose the snapshot
Select *processors* as table
Select *model* as field to display
Select *model* as field for the comparison
Select *Equal* as comparison operator
Enter "*x86 Family 6 Model 5 Stepping 2*" as value
Click *Display*



Generic Query

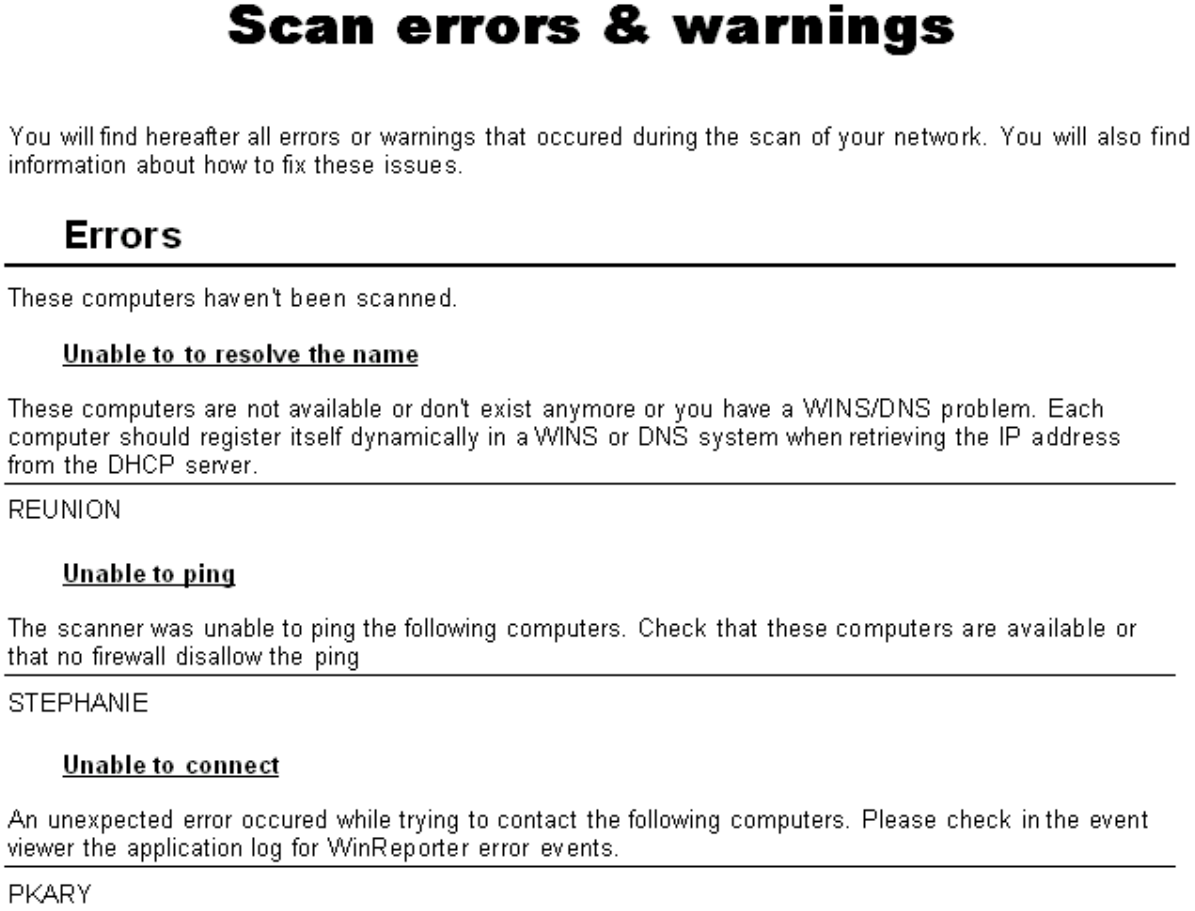
Table: processors
Displayed Field: model
Compare Field: model
Compare operation: equal
Compare value: x86 Family 6 Model 5 Stepping 2

TEST4
x86 Family 6 Model 5 Stepping 2

TEST5
x86 Family 6 Model 5 Stepping 2

3.3.5.4 Scan errors & warnings

This report will help you to fix most common scan problems and will also help you to find all out of date computer accounts that need to be removed from the domain.



Scan errors & warnings

You will find hereafter all errors or warnings that occured during the scan of your network. You will also find information about how to fix these issues.

Errors

These computers haven't been scanned.

Unable to to resolve the name

These computers are not available or don't exist anymore or you have a WINS/DNS problem. Each computer should register itself dynamically in a WINS or DNS system when retrieving the IP address from the DHCP server.

REUNION

Unable to ping

The scanner was unable to ping the following computers. Check that these computers are available or that no firewall disallow the ping

STEPHANIE

Unable to connect

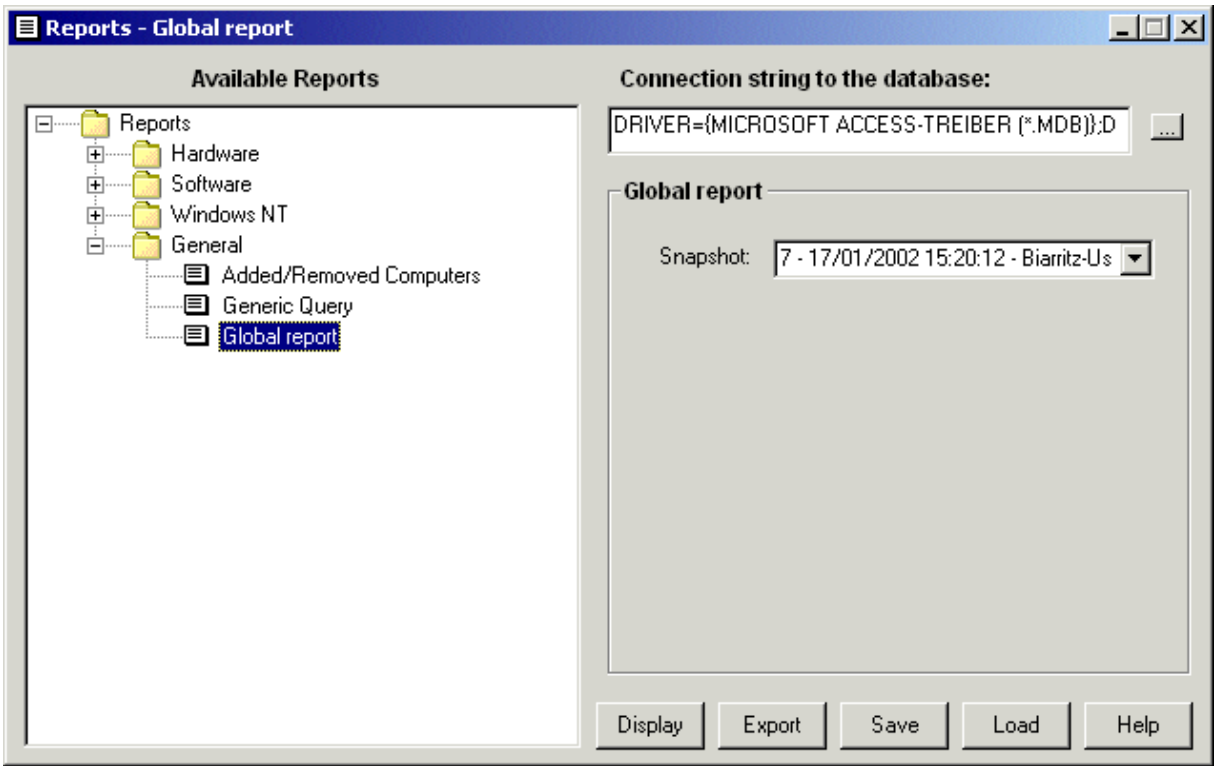
An unexpected error occured while trying to contact the following computers. Please check in the event viewer the application log for WinReporter error events.

PKARY

3.3.5.5 Global report

The global report allows you to have an exhaustive view about all computers, users and groups of your Windows NT network.
Warning! The global report may take a long time to be generated. To see the progression you can look at the window title of the report tool.
For each computer the following information is listed:
Type
Operating system
Language
Service pack
Internet Explorer version and service pack
Installation date
Last boot date
Last user
Registered user
Registered organization
System folder
Program files folder
Common folder
BIOS type

BIOS date
Model
Manufacturer
Serial number
Motherboard (Model, Manufacturer, Serial number)
List of services (internal name, display name, start mode)
Local users list (SID, account, full name, comment, last logon, last logoff, privilege)
List of local groups with the list of the members
Shares list (UNC, local path, description)
List of installed hot fixes
List of installed products (name, version, install date)
Network adapters
Disk partitions (volume, size, free space, file system, volume name)
Physical disks: Name, type disk/floppy/CD-ROM/tape, Volume, cable, position (SCSI ID or IDE master:0/slave:1)
Video configuration: Adapter model, Video memory size, horizontal/vertical resolution,
Processors: Model, manufacturer, frequency, bus frequency, caches
Memory: total RAM, in use
Swap files: Path, Minimum size, Maximum size, Current size, usage (%), Usage peak (%)
Memory slots: Slot name, installed size, maximum module size, type (SDRAM, DDR, RAMBUS...), Speed (MHz)
Local & Shared printers: Printer name, paper size, port, resolution (DPI), speed (ppm)
Scheduled tasks
Scanned registry values
For each domain user the following information is listed:
SID
Account
Full name
Comment
Last logon
Last logoff
Privilege
The password age
The password never expires
For each domain group the following information is displayed
The account name of the group
The list of members (groups included) (account name, full name)



TEST1

Type :	Windows NT Server, Primary Domain Controler, Server sharing print queue, running the master Browser service		
Operating System:	Windows NT 4	**Langage:**	English
Service Pack:	Service Pack 6		
Internet Explorer:	5.5 SP 1		
Installation date:	21/03/2002 01:06:39	**Last boot date:**	15/05/2003 07:34:42
Last User:	TESTDOMAIN\administrator		
Registered User:	jnh		
Registered Organization:	isd		
System folder:	C:\WINNT		
Program files folder:	C:\Program Files		
Common folder:	C:\Program Files\Common Files		
BIOS Type:	PhoenixBIOS 4.0 Release 6.0		
BIOS Date:	03/15/99		
Model:	V433		
Manufacturer:	Dell Computer Corporation		
Serial:	QDYT8		
Motherboard:	AR440BX		
Motherboard manufacturer:	Intel Corporation		
Motherboard serial:	0007328C1246193F01QL		

Services

Internal Name	Display Name	Start Mode
Alerter	Alerter	Automatic
ClipSrv	ClipBook Server	Manual
EventSystem	COM+ Event System	Manual
Browser	Computer Browser	Automatic
DHCP	DHCP Client	Disabled

Shares

\\TEST1\ADMIN$	C:\WINNT	Remote Admin
\\TEST1\backup	D:\backup	
\\TEST1\C$	C:\	Default share
\\TEST1\Copy	C:\Copy	
\\TEST1\copy2	D:\copy	
\\TEST1\D$	D:\	Default share
\\TEST1\E	E:\	
\\TEST1\HP4L	HP LaserJet 4L,LocalsplOnly	HP LaserJet 4L
\\TEST1\IPC$		Remote IPC
\\TEST1\NETLOGON	C:\WINNT\system32\Repl\Import\Scripts	Logon server share
\\TEST1\OfficeXPus	C:\OfficeXPus	
\\TEST1\PC_NT_DB	C:\Program Files\Northern\PrintControl	Common share for administrative tasks
\\TEST1\print$	C:\WINNT\system32\spool\drivers	Printer Drivers
\\TEST1\ServerBoss	C:\Program Files\ServerBoss	

Hot fixes

Q147222	Q246009	Q305399
Q314147		

Software

Product name	Version	Installed
Administrator's Pak		04/16/02
CConnect		06/10/03
CConnect Administrator		06/10/03
Communautest	1.00.0000	01/17/03
CommView	2.3	10/07/02
Directory Service Client (Remove only)		03/18/03
EMCO Remote CmdLine - Trial 1.1	1.1	03/27/02

Disk Partitions

Volume	Size (GB)	Free space (GB)	File system	Volume name
C	2,93	0,42	NTFS	
D	3,62	0,35	NTFS	

Storage Name	Type	Volume	Cable	Position
Floppy Device	Floppy	A		
Maxtor 90913D4 NAN4	Disk	C D	0	0
TOSHIBA CD-ROM XM-6402B 1008	CD-ROM		1	0

Video configuration

Type	Memory (MB)	Colors	Resolution (H)	Resolution (V)
	0,00	4	640	480

Processors

CPU idle time: 99,27 %

Model	Vendor	Frequency (MHz)	Bus (MHz)	L1 (KB)	L2 (KB)	L3 (KB)
Celeron	Intel	433	66	32	128	

Memory

RAM: 256 MB **In use:** 142 MB

Swap file Path	Min size (Mo)	Max size (Mo)	Size (Mo)	Usage (%)	Usage Peak (%)
C:\pagefile.sys	256	256	256	1,0	1,7

Memory Slot	Installed (MB)	Max (MB)	Type	Speed (MHz)
J6J1	128	256	DRAM	
J6J2	64	256	DRAM	

3.4 Event log reports

3.4.1 Event log reports

The eventlog based reports are common between the two IS Decisions product WinReporter and EvenTrigger

WinReporter is designed to insert events in the database manually or at scheduled times where EvenTrigger is designed to insert events in real time.

Before using these reports you need to either start a WinReporter scan with the eventlog scan selected (with the advanced mode) or configure a trigger in EvenTrigger with a database insertion as action.

Eventlog reports list

3.4.2 Files Access Report

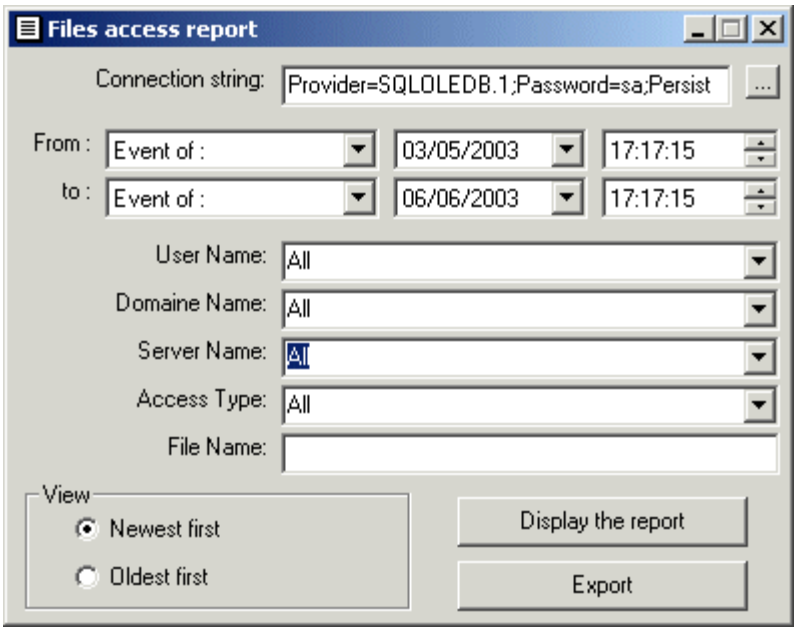
The files accesses report display the following information for each access.

Access time	Computer	File path	Access	Type	User name	Domain

In order to use the report you need to:
1- Activate the files access audit on your server
Windows NT 4: *Administrative Tools> User Manager for domain > Policy > Audit*
Check *Audit these events*
Check *Success* and *Failure* for *Files and objects access*

Windows 2000/XP/2003: *Administrative Tools> Local security policy > Local policies > Audit policy > Audit object access*
Check *Success* and *Failure*
Warning! The audit needs some times a long time to be effective. In order to accelerate this, you can execute the following command line: *secedit /refreshpolicy machine_policy* on Windows 2000 or *gpupdate* on Windows XP/2003.
Warning! If defined the domain security policy and the domain controller security policy override the local policy.

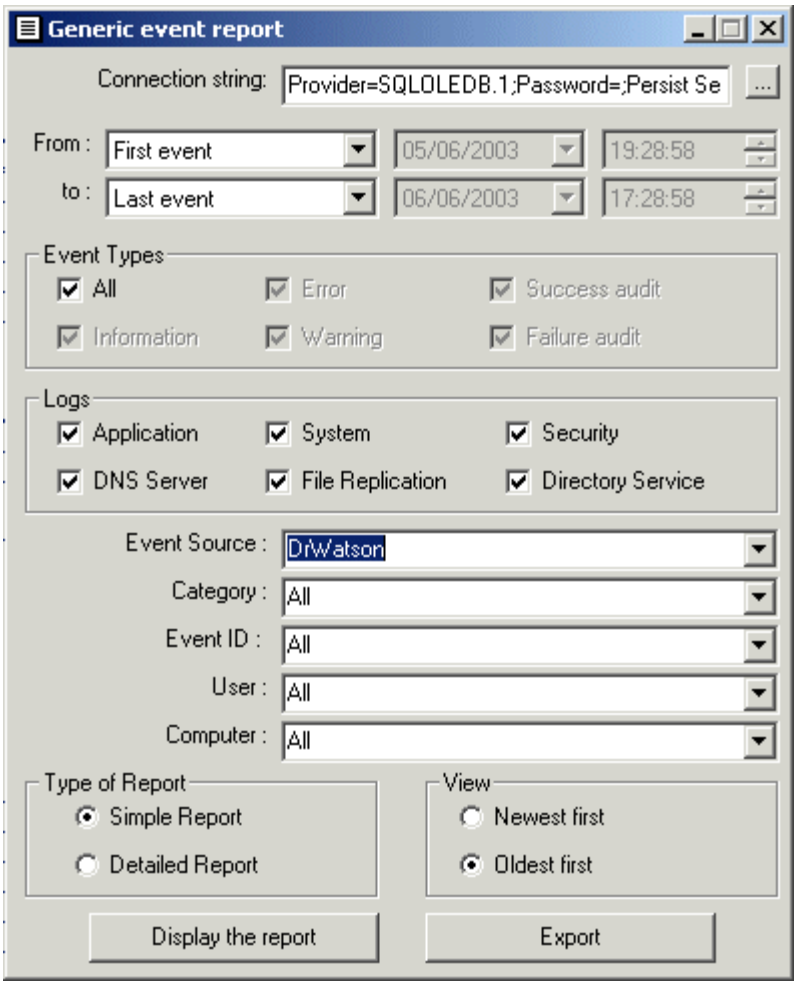
2- Activate the audit on the folder/file you want to monitor
Context menu of the folder/file: *Properties > Security > Advanced > Auditing > Add* to add an audit
Choose the users or groups to monitor and choose the files operations to monitor
3- Scan the security log of the computers to audit
To do this you need to use the advanced scan wizard after the monitoring period, check *Scan eventlogs*, check the *security* log, check *success audit* and *failure audit* as event types and start the scan.
3- Start the report File Accesses (available in the start menu, program group: WinReporter\Eventlog reports)
4- Configure the *connection string* to the database with the database wizard. (WinReporter default database path c:\program files\isdecisions\WinReporter.mdb)
5- Configure the filter. For example if you want to see accesses for a specified user or if you want to see accesses on a specified file.
The combo boxes display a list of all available field values in the database according the other conditions. You can even choose the report period with the *From* and *To* fields.
6- Click *Display* to see the report.



Additional information:
The file access report use the events 560 (file open)
Dynamic parameters:
2: Object type = File
3: File path
7: User name
8: Domain name
14: Access type
15: Privilege

3.4.3 Generic event report

This report will allow you to displays events according filters on standard event fields. You will for example be able to list all error or warning events or all events from a specified source.
If you want to display event descriptions you can select *Detailed report*.
To use the report you need to:
1- Scan the event logs of the computers you want to audit
To do this you need to use the advanced scan wizard, check *Scan eventlogs*, check the logs and event types you are interested in and start the scan.
2- Start the report Generic event report (available in the start menu, program group: WinReporter\Eventlog reports).
3- Configure the *connection string* to the database with the database wizard. (WinReporter default database located in c:\program files\isdecisions\WinReporter.mdb)
4- Configure the filter. The combo boxes display a list of all available field values in the database according the other conditions. You can even choose the report period with the *From* and *To* fields.
5- Click Display to view the report



3.4.4 Logon/Logoff report

The Logon/Logoff reports display the following information for each logon session.

Logon time	Logoff time	User name	Domain	Logon type	Server	Workstation

In order to use the report you need to:

1- Activate the logon/logoff audit

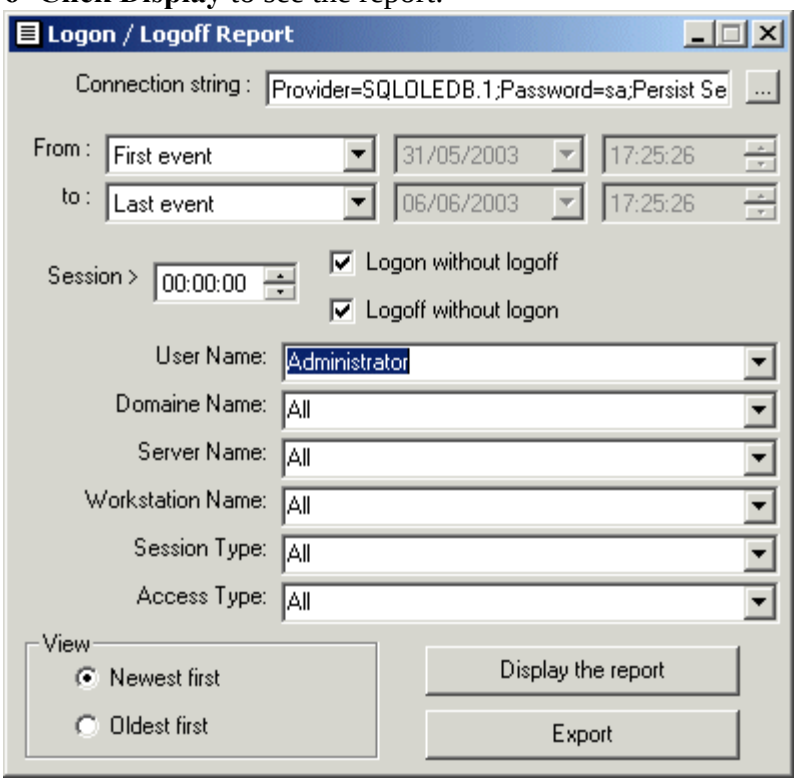
Windows NT 4: *Administrative Tools> User Manager for domain > Policy > Audit*
Check *Audit these events*
Check *Success* for *Logon and Logoff*

Windows 2000/XP: *Administrative Tools> Local security policy > Local policies > Audit policy > Audit logon events*
Check *Success*
Warning! The audit needs some times a long time to be effective. In order to accelerate this, you can execute the following command line: *secedit /refreshpolicy machine_policy* on Windows 2000 or *gpupdate* on Windows XP/2003
Warning! If defined the domain security policy and the domain controller security policy override the local policy.

2- Scan the security log of the computers to audit

To do this you need to use the advanced scan wizard after the monitoring period, check *Scan*

eventlogs, check the *security* log, check *success audit* and *failure audit* as event types and start the scan.
3- Start the report User sessions (available in the start menu, program group: WinReporter\Eventlog reports)
4- Configure the *connection string* to the database with the database wizard. (WinReporter default path c:\program files\isdecisions\WinReporter.mdb)
5- Configure the filter if needed. You can choose the report period with the *From* and *To* fields.
6- Click Display to see the report.



You can define the report time period with the *Begin date* and *End date* fields
You can choose to don't display sessions shorter than a time length specified in the *Session>* field.
The check box *Logoff without logon* allow to display logoff events without a corresponding logon event
The check box *Logon without logoff* allow to display logon events without a corresponding logoff event
Warning!
- The report may require a long time to execute the query. In order to accelerate the process you can deactivate *Logoff without logon* and *Logon without logoff.*

Advice
The report is interesting on Windows NT 4 computers or on Windows 2000/XP workstations (local logon). On Windows 2000 domain controllers the system generate to many Logon/Logoff events and it's very difficult to analyze them.

Additional information:
The logon/Logoff report use the events 528,540 (Logon) and 538 (Logoff)
The session information is located in the dynamic parameters:
1 : User name

2 : Domain
3 : Session Identifier
4 : Logon Type (Network = 3, Local = 2, Unlock workstation = 7)
7 : Workstation name

3.4.5 Printing Report

You can display three printing reports.
1- The listing of all printed documents. The following fields are available.

Print Time	Document name	Pages	Size (KB)	User Name	Print server	Printer

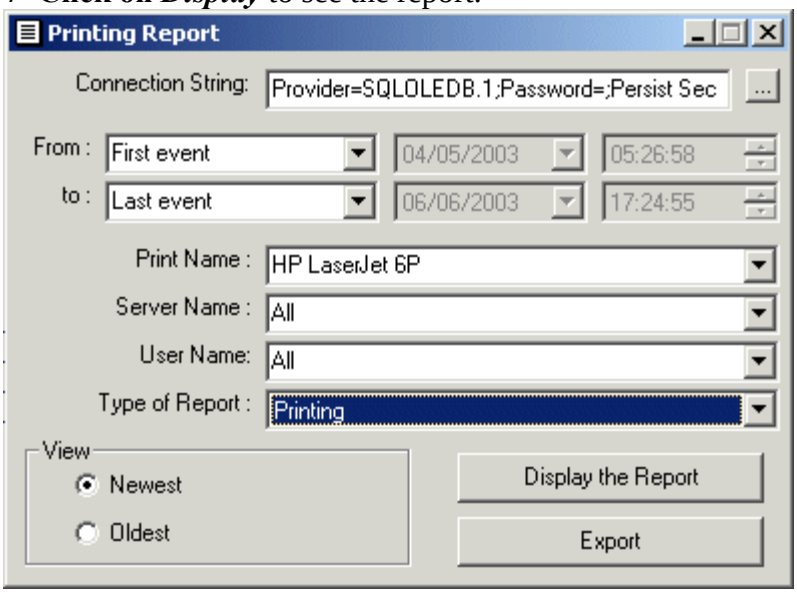
2- User print statistics. The following fields are available.

User name	Pages	Size (MB)	Number of documents

3- Daily print statistics. The following fields are available.

Date	Pages	Size (MB)	Number of documents

In order to use the *Printing report* you need to:
1- Activate the spooler audit.
Printers Server properties *(Start > Settings > Printers > Files > Server Properties > Advanced Settings* menu). Check
"*log spooler information*".
2- Scan the system log of the print servers to audit
To do this you need to use the advanced scan wizard after the monitoring period, check *Scan eventlogs*, select *system* log, check *Information* as event types and start the scan.
3- Start the report Printing Report (available in the start menu, program group: WinReporter\Eventlog reports)
4- Configure the *connection string* to the database with the database wizard. (WinReporter default path c:\program files\isdecisions\WinReporter.mdb)
5- Choose the report type: Printing/User statistics/Daily statistics
6- Configure the filter. For example to see only print notifications for a specified user. You can even choose the report period with the *From* and *To* fields.
7- Click on *Display* to see the report.



Additional information:

The printing report is based on the event *10* from the source *Printer* in the *system* log.
The printing information is located in the dynamic parameters:
1: Document number
2: Document name
3: User name
4: Printer name
5: Size of the document in bytes
6: Number of pages of the document

3.4.6 Process Tracking

This report displays the following fields for each process starting.

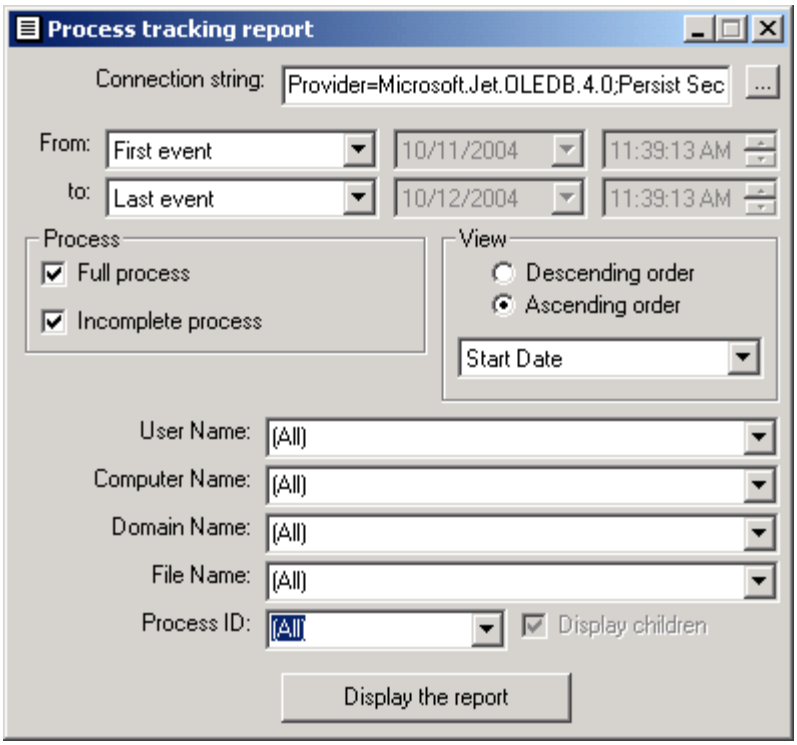
Start time	Process Id/ Parent Id	Path to the executable	Computer	User	Domain

In order to use it you need to:
1- Activate the Process tracking audit

Windows NT 4: *Administrative Tools> User Manager for domain > Policy > Audit*
Check *Audit these events*
Check *Success* for *Process tracking*

Windows 2000/XP: *Administrative Tools> Local security policy > Local policies > Audit policy > Audit process tracking*
Check *Success*
Warning! The audit needs some times a long time to be effective. In order to accelerate this, you can execute the following command line: *secedit /refreshpolicy machine_policy* on Windows 2000 or *gpupdate* on Windows XP/2003
Warning! If defined the domain security policy and the domain controller security policy override the local policy.

2- Scan the security log of the computers to audit
To do this you need to use the advanced scan wizard after the monitoring period, check *Scan eventlogs*, check the *security* log, check *success audit* and *failure audit* as event types and start the scan.
3- Start the report Process tracking (available in the start menu program group WinReporter\Eventlog reports)
4- Configure the *connection string* to the database with the database wizard. (WinReporter default path c:\program files\isdecisions\WinReporter.mdb)
5- Configure the filter, for example to list all processes started by a specified user. You can even choose the report period with the *From* and *To* fields.
6- Click *Display* to view the report



3.4.7 Service errors

When a service doesn't start or stop unexpectedly the *Service Control Manager* insert an error in the system log. This report will allow you to display easily all service errors notified by the Service Control Manager. Three kinds of errors are listed: Start, Stop and timeout problems. The report display the following information for each error:

Error time	Service	Category	Comment	Computer

In order to use this report you need to:

1- Scan the system log of the computers to audit

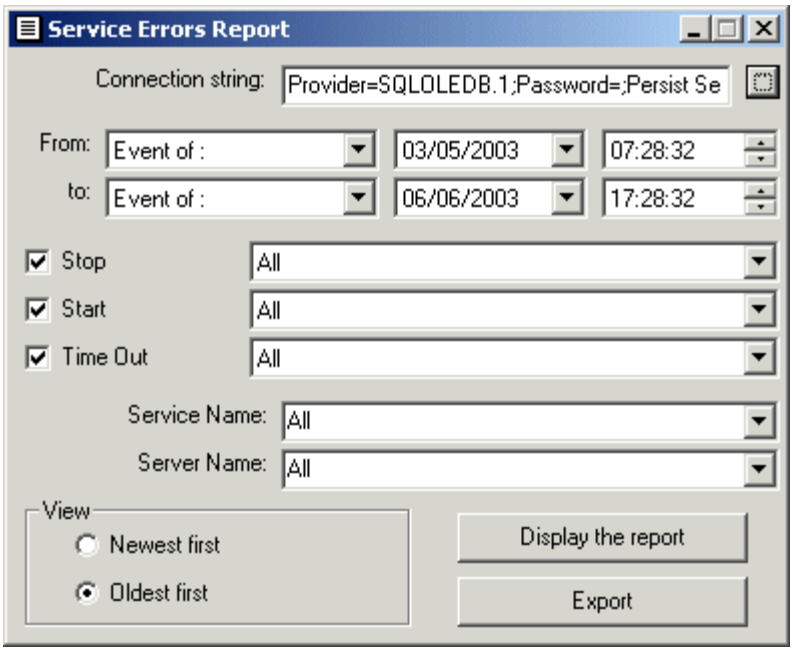
To do this you need to use the advanced scan wizard after the monitoring period, check *Scan eventlogs*, select *system* log, check *Information* as event types and start the scan.

2- Start the report *Service Errors*.

3- Configure the *connection string* to the database with the database wizard. (WinReporter default database located in c:\program files\isdecisions\WinReporter.mdb)

4- Configure the filter. You can choose the report period with the *From* and *To* fields.

5- Click Display to view the report

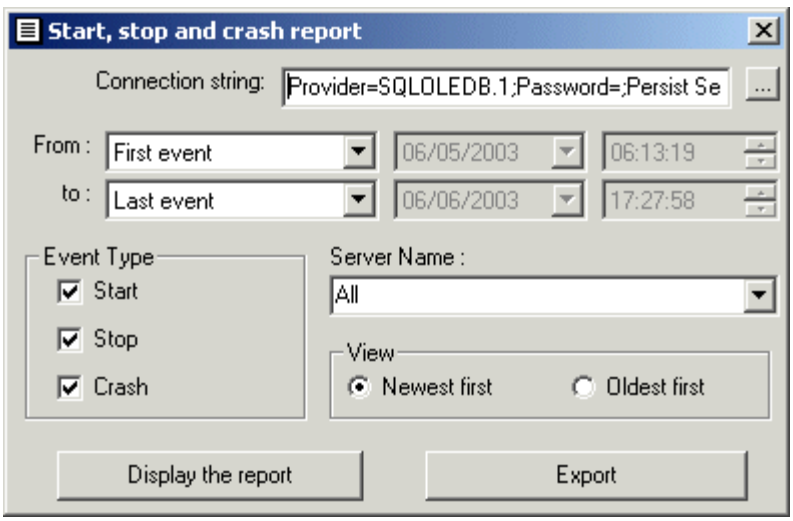


3.4.8 Computers starts and shutdowns

When a computer starts or stops, the eventlog service inserts specified events in the system log. This report use these events to track all computer shutdowns and reboots.
The following information is displayed for each start/shutdown event.

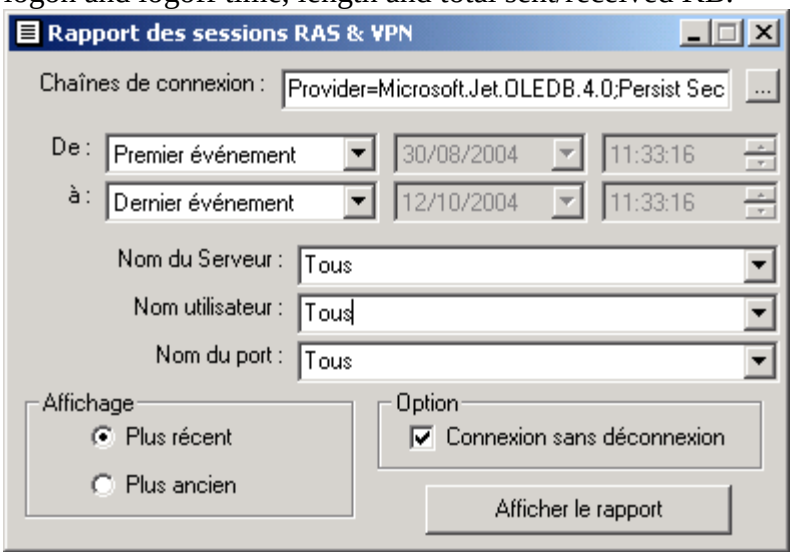
Type (start/stop/crash)	Date	Event type	Computer

In order to use the report you need to:
1- Scan the system log of the computers you want to audit
To do this you need to use the advanced scan wizard, check *Scan eventlogs*, select *system* log, check *Information* as event types and start the scan.
2- Start the report Computers starts & shutdowns (available in the start menu program group WinReporter\Eventlog reports).
3- Configure the *connection string* to the database with the database wizard. (WinReporter default database located in c:\program files\isdecisions\WinReporter.mdb)
4- Configure the filter. You can choose the report period with the *From* and *To* fields.
5- Click Display to view the report



3.4.9 RAS & VPN connections

To use this report you need to enable the full audit on your Remote access server. To do this, open your RRAS console and check *Record all events* in the *log* tab of the server properties. After a while you will be able to retrieve in the database the remote access events by scanning the system log of the RRAS server and you will be able launch the report on the database.
The report displays remote access sessions according to: username, server name and port name. In addition to the previously listed information the report also displays for each session: logon and logoff time, length and total sent/received KB.



Rapport des sessions RAS & VPN

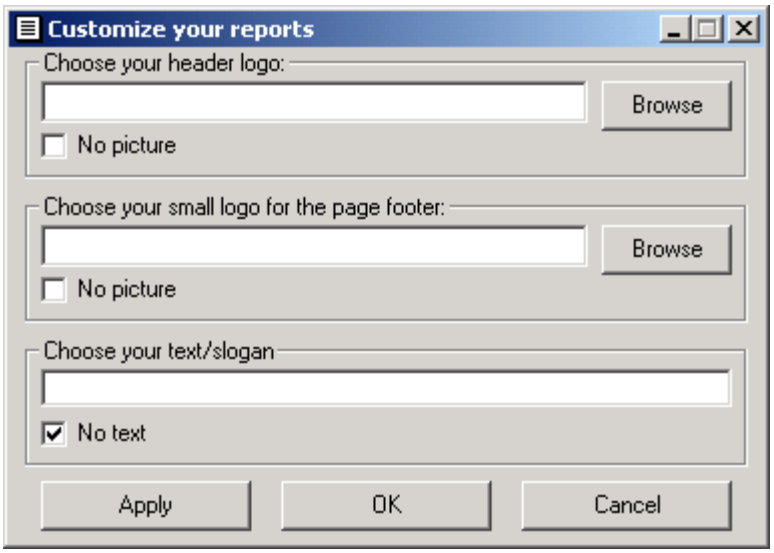
Période du Rapport : Du 19/05/2004 21:25:06 au 21/06/2004 22:24:14

Nom du Serveur : Tous **Nom utilisateur :** BIARRITZ\jnh **Nom du port :** Tous

Heure de connexion	Heure de déconnexion	Durée	Utilisateur	Serveur	Port	Envoyés (Ko)	Reçus (Ko)
21/06/2004 21:36:21	21/06/2004 22:24:14	00:47:53	BIARRITZ\jnh	TAFSERVER	VPN5-4	2962	1496117
21/06/2004 20:48:24	21/06/2004 20:55:48	00:07:24	BIARRITZ\jnh	TAFSERVER	VPN5-4	1691	603235
19/06/2004 18:17:40	19/06/2004 18:37:34	00:19:54	BIARRITZ\jnh	TAFSERVER	VPN5-4	199	94627
19/06/2004 10:45:47	19/06/2004 11:39:15	00:53:28	BIARRITZ\jnh	TAFSERVER	VPN5-4	3247	1606471
18/06/2004 23:35:34	19/06/2004 01:39:00	02:03:26	BIARRITZ\jnh	TAFSERVER	VPN5-4	4852	3142936

3.5 Configure your company logo

In order to configure the logo displayed in the header of all reports you can use the *Logo configuration* tool available in the start menu *WinReporter\Tools*.
You can even configure a *text/slogan* and a *small logo* for the report footer.
If you don't want any logo you can check *No picture*.

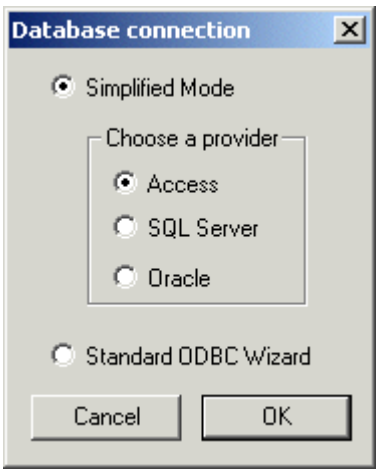

Customize your reports
Choose your header logo:
Browse
No picture
Choose your small logo for the page footer:
Browse
No picture
Choose your text/slogan
No text
Apply
OK
Cancel

4 Tools

4.1 Database Wizard

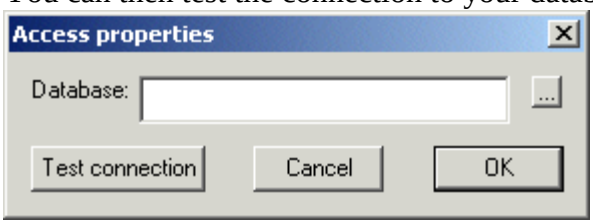
4.1.1 Database Wizard

This is a simplified wizard designed to help you creating the connection string to the database. You can choose between three providers supported by WinReporter : Access, SQL Server, and Oracle. If you need more options or use an existing DSN you can use the *standard ODBC wizard*.
This wizard can be called on all WinReporter tools needing a connection to a database.



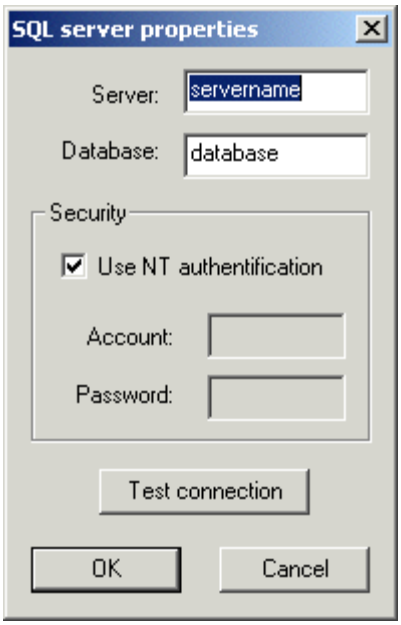
4.1.2 Database Wizard with Access

Enter here the path to your Microsoft Access database file (.MDB extension) or use the browse button.
You can then test the connection to your database with the *test* button.



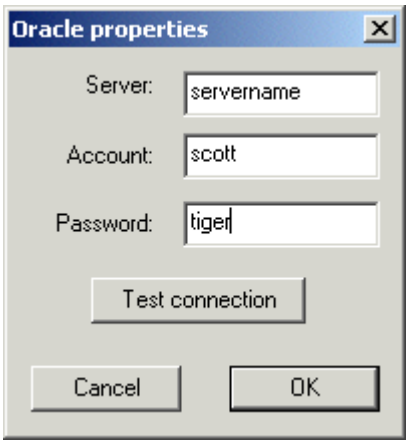
4.1.3 Database Wizard with SQL Server

Enter the SQL server name (leaving blank means localhost)
Enter the Database name (leaving blank means using the default database)
Security
You can use the NT authentication if your NT account has the required rights on the SQL server and this SQL Server support NT authentication (SQL Server 7 or more). If not checked, enter a SQL server user account and its password.



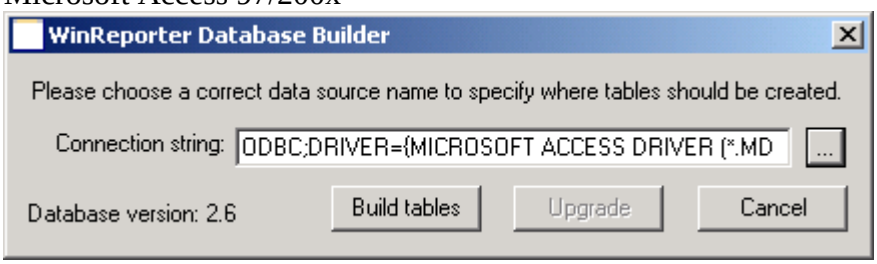
4.1.4 Database Wizard with Oracle

Enter the Oracle *server* name, the *security account* and its *password*.
You can then test the connection to your database with the *test* button.



4.2 WinReporter database builder

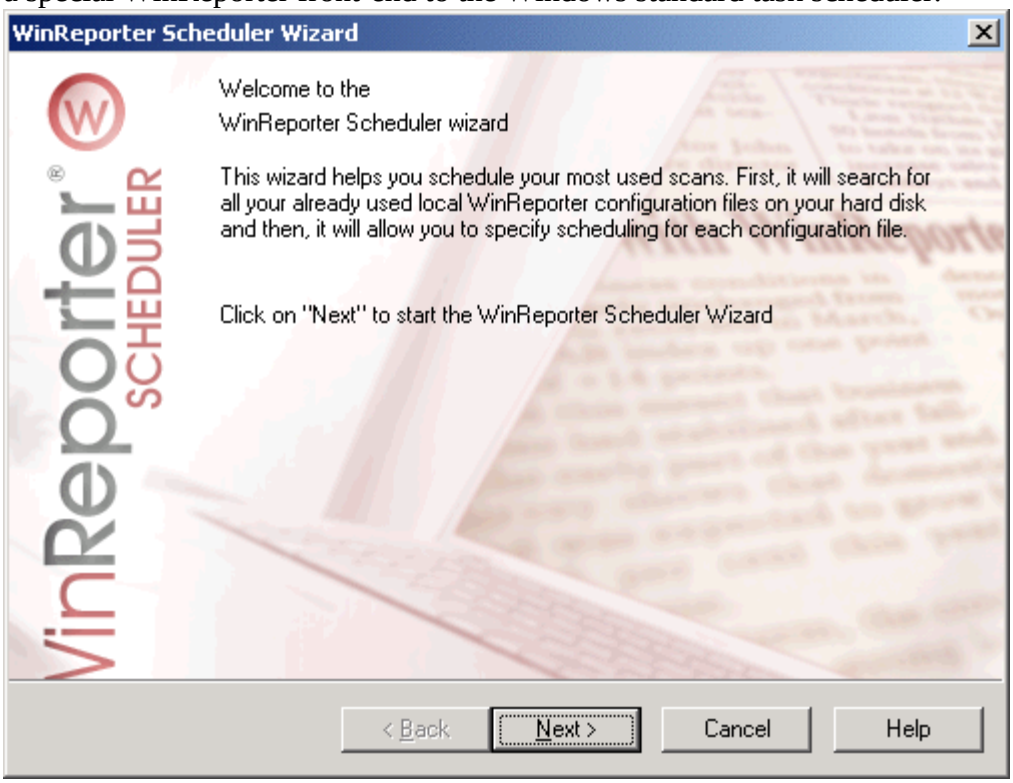
This tool creates automatically the tables related to WinReporter in the ODBC data source you've specified with the database wizard by clicking on the "..." button.
The tables are created by sending SQL queries of type *CREATE TABLE xxx (...)*.
You can also upgrade a database from a previous version of WinReporter by clicking *Upgrade*.
The following databases formats are supported:
Microsoft SQL Server 6.5/7.0/2000
Oracle 7/8
Microsoft Access 97/200x



4.3 WinReporter Scheduler Wizard

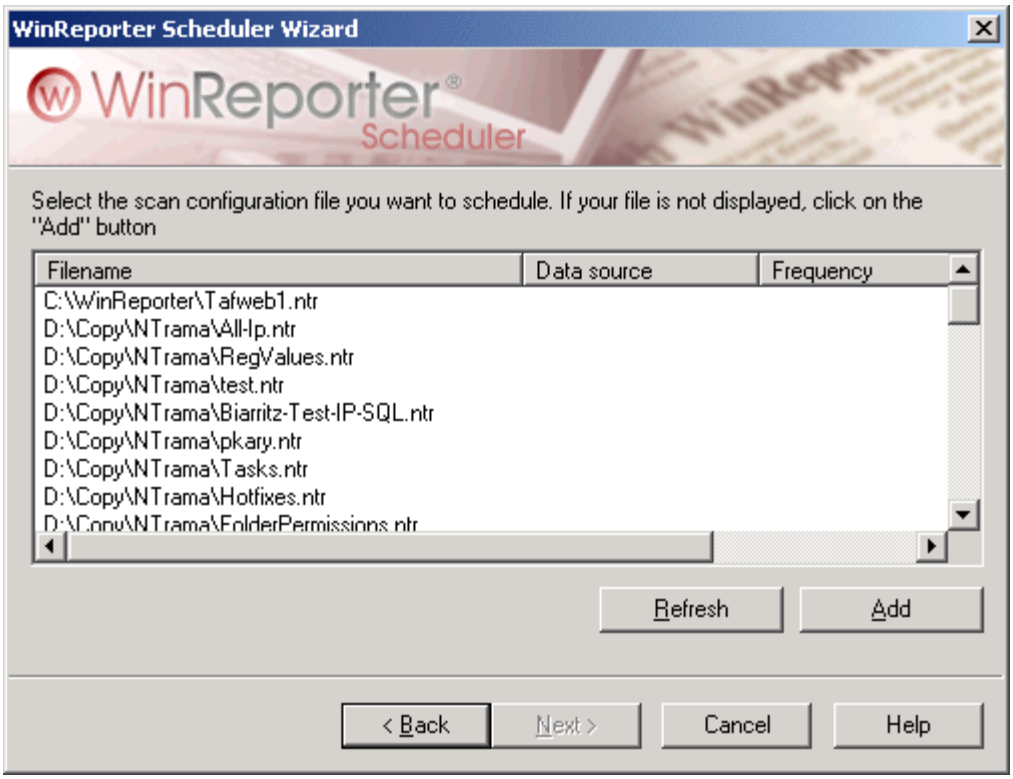
4.3.1 Welcome page

This is the first step of the wizard. It indroduces you to the scheduler. The scheduler is simply a special WinReporter front-end to the Windows standard task scheduler.



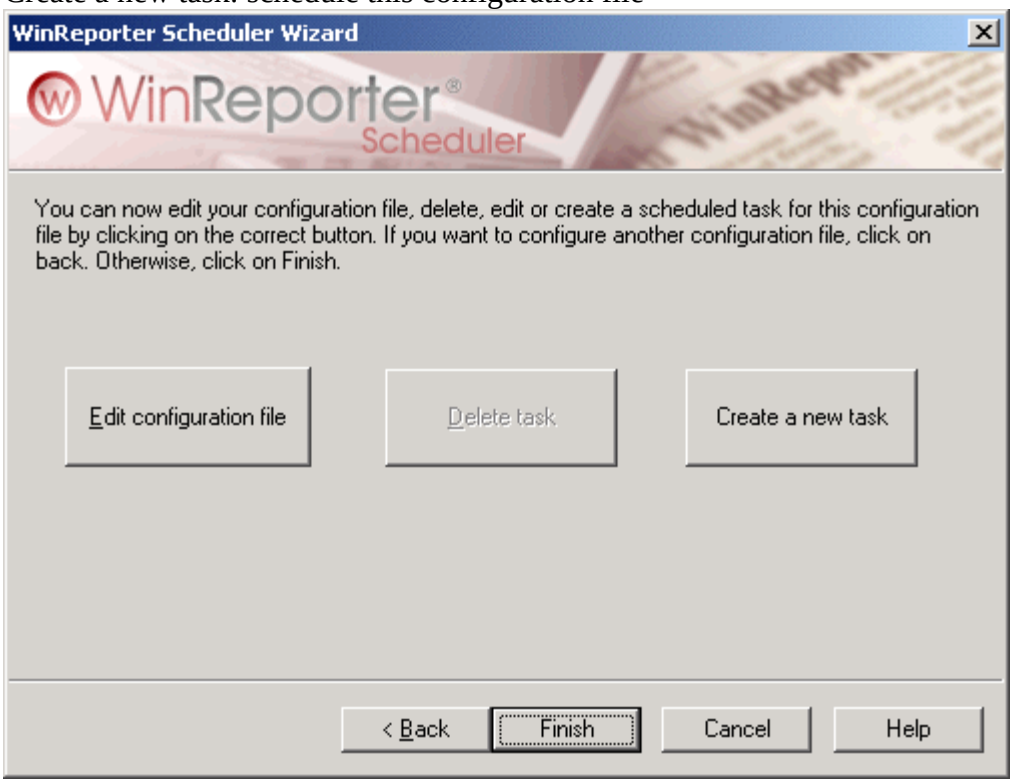
4.3.2 Configuration file selection

You may select your file from the list of the configuration files you have already used with the scanner. If the file you want to use is not in the list, click on "Add" and select manually the file to add it to the list.



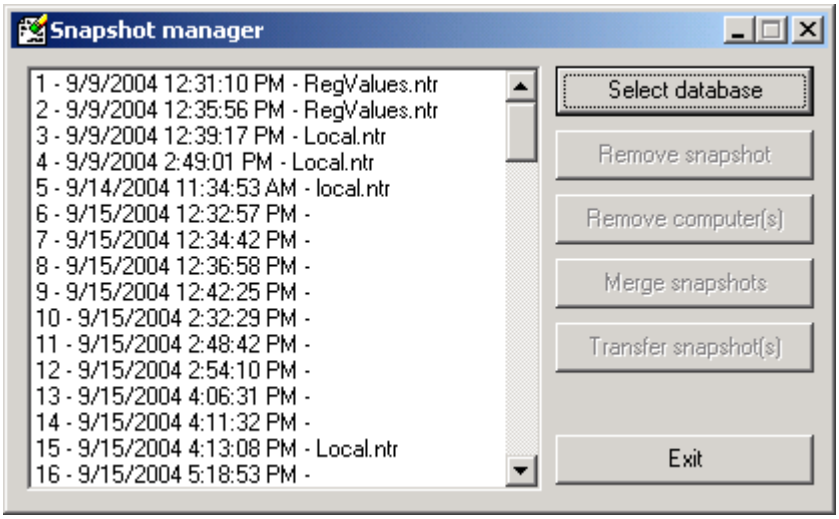
4.3.3 Action page

The final step of the wizard enables you to:
Edit configuration file: opens the notepad to edit the .NTR file (previously created with the WinReporter scanner)
Delete task: deletes all scheduled works for this configuration
Create a new task: schedule this configuration file



4.4 Snapshot manager

The snapshot manager allows you to:
Delete snapshots in a WinReporter database in order to free disk space
Remove computers from a WinReporter snapshot
Merge several snapshots in a new snapshot. The merged snapshot will contain the most recent version of all computers available in those snapshots. This is useful if you want to scan a network in several times or if many computers are regularly unavailable.
Transfer snapshots in another database
For example if you want to scan a world wide network in several times:
Each administrator scans its own network zone in an MS Access database
The world wide administrator centralize all MS Access databases and transfer all snapshots contained in these databases in a single database (one database with several snapshots) using the Snapshot manager.
The world wide administrator merges all snapshots from this database in a new snapshot in a final database.



5 Database format

5.1 Database format Overview

A typical WinReporter database is composed of many tables each one presenting a different type of information. The most important one is the table called "servers". This table lists all the servers that have been scanned.
The complete list of tables used by WinReporter is available here and the relationship diagram between all tables is available here.

5.1.1 Snapshots

WinReporter allows you to store your information from a? historical point of view, so that you can retrieve the state of your network from the dates of your snapshots. Each snapshot is identified by a value called **id_snapshot**. All the snapshots are listed in the snapshots table. Every WinReporter table has a field named id_snapshot indicating when the information was valid.

5.2 Creating a new database

The steps in order to create a WinReporter database are:
Create a database with your database manager (MS SQL Server, Oracle, MS Access)
Run the WinReporter database builder
Select the just created database with the database wizard
Click on "*Build tables*"
The tables will then be created and you will be able to fill in the database with the WinReporter scanner.

5.3 Tables

5.3.1 Tables list

Alphabetical order
AccountPolicy
acc_ownership
aces
ADServers
devices
DnsServers
DnsZones
ET_Events
ET_Params
groups
hotfixes
IISServers
MemSlots
netcards
NetComponents
partitions
PhysicalDisks
printers

5.3.2 servers

5.3.2.1 Description

This table describes the list of computers specifying their name, type, comments and service pack.

5.3.2.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
domain_name	string	Name of the domain (or the workgroup) to which the servers belongs.
type	number	Number composed of a bit mask describing the type of the server (see Appendix 1).
texttype	string	A comprehensible text string describing the preceding type value.
comments	string	Comments of the server.
maxusers	number	Maximal number of concurrent connected users. If this value equals -1, it means that there is no limit.
userspath	string	This string contains the path to user directories.
sp	string	Describes the actual Windows NT Service Pack installed.
install_date	date	Date when the operating system has been installed.
bios_type	string	Description of the Bios.
bios_date	string	Bios date (useful for Y2K tests).
os	string	Active operating system.
OSLevel		0 = workstation/ 1 = server/ 2 advanced server
wmi	number	Equals 1 if Windows Management Instrumentation is active on the computer. Otherwise, it is equals to 0.
ram	number	Amount of physical memory (MB).
ramUsed	number	Memory in use (MB)

dns_hostname	string	
dns_domain_name	string	
dns_suffixes	string	
Manufacturer	string	Computer's manufacturer
Model	string	Computer's model
Serial	string	Computer's serial number
MBManufacturer	string	Motherboard's manufacturer
MBModel	string	Motherboard's model
MBSerial	string	Motherboard's serial
SmBIOSVersion	string	Supported version of the SMBIOS standard
DComEnabled	number	0/1 DCOM is disabled/enabled
RegisteredOwner	string	Name of the registered user
RegisteredOrganization	string	Name of the registered company
LastUser	string	Last logged on user (link to users\account_name)
SystemRoot	string	OS directory (commonly c:\winnt c:\windows)
ProgramFilesDir	string	Commonly c:\program files\
CommonFilesDir	string	Commonly c:\program files\Common Files
BootTime	number	Time interval (in days) since the last boot of the machine
IdleTime	number	Idle Time (in days) since the last boot. % Used processor time = 100-IdleTime/BootTime*100
ScanTime	time	Scan time
IEVersion	number	Internet Explorer version
IESPNumber	number	Internet Explorer service pack
LanguageId	number	Operating system language. See appendix 2 for the meaning of this number.
CanonicalName	string	Canonical name of the computer in the Active Directory
Container	string	Container of the computer in the Active Directory
ComputerState	number	1/0 need a reboot yes/no
ChassisType	number	Computer case see appendix 3.

5.3.2.3 Appendix 1

Symbolic constant	Value	Meaning
SV_TYPE_WORKSTATION	0x00000001	All LAN Manager workstations.
SV_TYPE_SERVER	0x00000002	All LAN Manager servers.
SV_TYPE_SQLSERVER	0x00000004	Any server running with Microsoft SQL Server.
SV_TYPE_DOMAIN_CTRL	0x00000008	Primary domain controller.
SV_TYPE_DOMAIN_BAKCTRL	0x00000010	Backup domain controller.
SV_TYPE_TIMESOURCE	0x00000020	Server running the Timesource service.
SV_TYPE_AFP	0x00000040	Apple File Protocol servers.
SV_TYPE_NOVELL	0x00000080	Novell servers.
SV_TYPE_DOMAIN_MEMBER	0x00000100	LAN Manager 2.x Domain

		Member.
SV_TYPE_LOCAL_LIST_ONLY	0x40000000	Servers maintained by the browser.
SV_TYPE_PRINT	0x00000200	Server sharing print queue.
SV_TYPE_DIALIN	0x00000400	Server running dial-in service.
SV_TYPE_XENIX_SERVER	0x00000800	Xenix server.
SV_TYPE_MFPN	0x00004000	Microsoft File and Print for Netware.
SV_TYPE_NT	0x00001000	Windows NT (either Workstation or Server).
SV_TYPE_WFW	0x00002000	Server running Windows for Workgroups.
SV_TYPE_SERVER_NT	0x00008000	Windows NT non-DC server.
SV_TYPE_POTENTIAL_BROWSER	0x00010000	Server that can run the Browser service.
SV_TYPE_BACKUP_BROWSER	0x00020000	Server running a Browser service as backup.
SV_TYPE_MASTER_BROWSER	0x00040000	Server running the master Browser service.
SV_TYPE_DOMAIN_MASTER	0x00080000	Server running the domain master Browser.
SV_TYPE_DOMAIN_ENUM	0x80000000	Primary Domain.
SV_TYPE_WINDOWS	0x00400000	Windows 95 or later.
SV_TYPE_ALL	0xFFFFFFF	All servers.

5.3.2.4 Appendix 2

Symbolic constant	Value	Meaning
LANG_NEUTRAL	0x00	Neutral
LANG_ARABIC	0x01	Arabic
LANG_BULGARIAN	0x02	Bulgarian
LANG_CATALAN	0x03	Catalan
LANG_CHINESE	0x04	Chinese
LANG_CZECH	0x05	Czech
LANG_DANISH	0x06	Danish
LANG_GERMAN	0x07	German
LANG_GREEK	0x08	Greek
LANG_ENGLISH	0x09	English
LANG_SPANISH	0x0a	Spanish
LANG_FINNISH	0x0b	Finnish
LANG_FRENCH	0x0c	French
LANG_HEBREW	0x0d	Hebrew
LANG_HUNGARIAN	0x0e	Hungarian
LANG_ICELANDIC	0x0f	Icelandic
LANG_ITALIAN	0x10	Italian

LANG_JAPANESE	0x11	Japanese
LANG_KOREAN	0x12	Korean
LANG_DUTCH	0x13	Dutch
LANG_NORWEGIAN	0x14	Norwegian
LANG_POLISH	0x15	Polish
LANG_PORTUGUESE	0x16	Portuguese
LANG_ROMANIAN	0x18	Romanian
LANG_RUSSIAN	0x19	Russian
LANG_CROATIAN	0x1a	Croatian
LANG_SERBIAN	0x1a	Serbian
LANG_SLOVAK	0x1b	Slovak
LANG_ALBANIAN	0x1c	Albanian
LANG_SWEDISH	0x1d	Swedish
LANG_THAI	0x1e	Thai
LANG_TURKISH	0x1f	Turkish
LANG_URDU	0x20	Urdu
LANG_INDONESIAN	0x21	Indonesian
LANG_UKRAINIAN	0x22	Ukrainian
LANG_BELARUSIAN	0x23	Belarusian
LANG_SLOVENIAN	0x24	Slovenian
LANG_ESTONIAN	0x25	Estonian
LANG_LATVIAN	0x26	Latvian
LANG_LITHUANIAN	0x27	Lithuanian
LANG_FARSI	0x29	Farsi
LANG_VIETNAMESE	0x2a	Vietnamese
LANG_ARMENIAN	0x2b	Armenian
LANG_AZERI	0x2c	Azeri
LANG_BASQUE	0x2d	Basque
LANG_MACEDONIAN	0x2f	FYRO Macedonian
LANG_AFRIKAANS	0x36	Afrikaans
LANG_GEORGIAN	0x37	Georgian
LANG_FAEROESE	0x38	Faeroese
LANG_HINDI	0x39	Hindi
LANG_MALAY	0x3e	Malay
LANG_KAZAK	0x3f	Kazak
LANG_KYRGYZ	0x40	Kyrgyz
LANG_SWAHILI	0x41	Swahili
LANG_UZBEK	0x43	Uzbek
LANG_TATAR	0x44	Tatar
LANG_BENGALI	0x45	Not supported
LANG_PUNJABI	0x46	Punjabi
LANG_GUJARATI	0x47	Gujarati
LANG_ORIYA	0x48	Not supported
LANG_TAMIL	0x49	Tamil
LANG_TELUGU	0x4a	Telugu

LANG_KANNADA	0x4b	Kannada
LANG_MALAYALAM	0x4c	Not supported
LANG_ASSAMESE	0x4d	Not supported
LANG_MARATHI	0x4e	Marathi
LANG_SANSKRIT	0x4f	Sanskrit
LANG_MONGOLIAN	0x50	Mongolian
LANG_GALICIAN	0x56	Galician
LANG_KONKANI	0x57	Konkani
LANG_MANIPURI	0x58	Not supported
LANG_SINDHI	0x59	Not supported
LANG_SYRIAC	0x5a	Syriac
LANG_KASHMIRI	0x60	Not supported
LANG_NEPALI	0x61	Not supported
LANG_DIVEHI	0x65	Divehi
LANG_INVARIANT	0x7f	

5.3.2.5 Appendix 3 Chassis type

Number	Case
1	Other
2	Unknown
3	Desktop
4	Low Profile Desktop
5	Pizza Box
6	Mini Tower
7	Tower
8	Portable
9	LapTop
10	Notebook
11	Hand Held
12	Docking Station
13	All in One
14	Sub Notebook
15	Space-saving
16	Lunch Box
17	Main Server Chassis
18	Expansion Chassis
19	SubChassis
20	Bus Expansion Chassis
21	Peripheral Chassis
22	RAID Chassis
23	Rack Mount Chassis
24	Multi-system chassis.

5.3.2.6 Example

As an example, to know all the Windows NT workstations without the service pack 5 installed, use the following SQL query:

```
SELECT * FROM servers WHERE (type & 0x00001000 <> 0) AND (sp <> 'Service
Pack 4')
```

5.3.3 snapshots

5.3.3.1 Description

This table lists all the network images available in the database. Each image is identified by the "id_snapshot" field and this field is present in every WinReporter table.

5.3.3.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
shot_time	time	Time when the scan of the snapshot began.

5.3.3.3 Example

For example, to view all the snapshots available in the database ordered by time, use the following SQL query:

```
SELECT * FROM snapshots ORDER BY shot_time
```

5.3.4 WRptDbVersion

WinReporter database structure version.

Data field	Data value	Description
VersionNumber	number	Database integer version number
Product version	string	WinReporter display version

5.3.5 ScanErrors

The scanner insert in this table all errors and warnings occuring during a scan. An error means that the computer was not scanned. A warning means that information will be missing for the computer.

Field name	Data type	Description
id_snapshot	number	snapshot auto-number.
server_name	string	Name or network address of the related computer
EventLevel	number	0/1 for warning/error
EventCode	number	scan error number see appendix

5.3.5.1

5.3.5.2 Appendix Errors & Warning codes

Code	Synbolic name	Level	Description
0	SCAN_ERROR_NAME_RESOLUTION	Error	Unable to to resolve the name
1	SCAN_ERROR_PING	Error	Unable to ping
2	SCAN_ERROR_NETPATH_NOTFOUND	Error	Network path not found

3	SCAN_ERROR_REMOTEREG	Error	Unable to access the registry
4	SCAN_ERROR_ACCESS_DENIED	Error	Access denied
5	SCAN_ERROR_CONNECT	Error	Unable to connect
6	SCAN_ERROR_COMPUTER_REC	Error	Unable to insert the computer in the database
7	SCAN_ERROR_LICENSE_SERVERS	Error	Not enough server licenses
8	SCAN_ERROR_LICENSE_WKSTAS	Error	Not enough workstation licenses
9	SCAN_ERROR_OTHER	Error	Unspecified error
10	SCAN_ERROR_EXCEPTION	Error	Unexpected error
100	SCAN_WARNING_SMBIOS_INITDENIED	Warning	Advanced scan (Initialization denied)
101	SCAN_WARNING_SMBIOS_RPCUNAVAILABLE	Warning	Advanced scan (RPC server unavailable)
102	SCAN_WARNING_SMBIOS_NODATA	Warning	Advanced scan (No SMBIOS data)
103	SCAN_WARNING_SMBIOS_OTHER	Warning	Advanced scan error
104	SCAN_WARNING_NOADMINSHARES	Warning	No administrative shares
105	SCAN_WARNING_DBINSERTION	Warning	Database insertion error
106	SCAN_WARNING_OTHER	Warning	Unspecified warning
107	SCAN_WARNING_ERRORSHARES	Warning	Unable to scan shares
108	SCAN_WARNING_ERRORSERVICES	Warning	Unable to scan services
109	SCAN_WARNING_EXCEPTION	Warning	Unexpected warning
1000	SCAN_DOMAIN_ERROR_OU	Domain Error	Unable to retrieve computers from the Global Catalog
1001	SCAN_DOMAIN_ERROR_LIST	Domain Error	Unable to find a domain controler
1002	SCAN_DOMAIN_ERROR_CONTROLLER	Domain Error	Unable to retrieve computers from the domain controller

5.3.6 Hardware

5.3.6.1 partitions

5.3.6.1.1 Description

This table lists all the partitions of the server and specifies their free disk space, total disk space...

5.3.6.1.2 Fields

Field name	Data type	Description
id_snapshot	number	snapshot auto-number.

server_name	string	Netbios name of the server without the 2 backslashes.
partition	string	Name of the partition
disksize	number	Total disk space on the partition (in Kb)
id_disk	number	Physical disk number (link to PhysicalDisks table)
FileSystem	string	NTFS or FAT
FileSystemFlags	number	See appendix 1 for the meaning
VolumeName	string	Label of the partition
VolumeSerial	string	Serial number of the partition
spacefree	number	Total free disk space on the partition (in Kb)

5.3.6.1.3 Appendix 1 File system flags

Symbolic constant	Value	Meaning
FS_CASE_IS_PRESERVED	0x00000002	The file system preserves the case of file names when it places a name on disk.
FS_CASE_SENSITIVE	0x00000001	The file system supports case-sensitive file names.
FS_UNICODE_STORED_ON_DISK	0x00000004	The file system supports Unicode in file names as they appear on disk.
FS_PERSISTENT_ACLS	0x00000008	The file system preserves and enforces ACLs. For example, NTFS preserves and enforces ACLs, and FAT does not.
FS_FILE_COMPRESSION	0x00000010	The file system supports file-based compression.
FS_VOL_IS_COMPRESSED	0x00008000	The specified volume is a compressed volume; for example, a DoubleSpace volume.
FILE_NAMED_STREAMS	0x00040000	The file system supports named streams.
FILE_READ_ONLY_VOLUME		**Windows XP:** The specified volume is read-only.
FILE_SUPPORTS_ENCRYPTION	0x00020000	The file system supports the Encrypted File System (EFS).
FILE_SUPPORTS_OBJECT_IDS	0x00010000	The file system supports object identifiers.
FILE_SUPPORTS_REPARSE_POINTS	0x00000080	The file system supports reparse points.
FILE_SUPPORTS_SPARSE_FILES	0x00000040	The file system supports sparse files.
FILE_VOLUME_QUOTAS	0x00000020	The file system supports disk quotas.

5.3.6.2 PhysicalDisks

Hard disks, floppy disks, CD-ROM/DVD-ROM and tapes (despite the table name).

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.

server_name	string	Netbios name of the server without the two preceding backslash characters.
DeviceName	string	Name of the device (devices table field DeviceName)
id_disk	number	Order number of the disk link with partition id_disk field
DiskType	number	See appendix 1
DiskSize	number	Currently not scanned
DiskLetter	string	Logical drive or included partitions
id_DiskControler	string	Link to the disk controller with the field PnpInstanceID in table devices
PortNumber	number	Usually the cable number
BusNumber	number	
Position	number	Usually the SCSI Identifier or 0/1 for IDE Master/Slave

5.3.6.2.1 Appendix 1 Disk types

Value	Meaning
0	Hard Disk
1	Floppy disk
2	CD-ROM
3	Tape

5.3.6.3 VideoAdapters

5.3.6.3.1 Description

This table lists video adapters from all Windows NT/2000 computers. Some fields are not not available for Windows 9x computers.

5.3.6.3.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
DeviceDescription	string	Commonly used name of the video adapter
BiosString	string	String to identify the BIOS (manufacturer, version and so on)
ChipType	string	Type of video processor
AdapterString	string	String to identify the adapter
DacType	string	Type of DAC
VideoMemory	number	Size of video memory in kB
xResolution	number	Horizontal resolution
yResolution	number	Vertical resolution
RefreshRate	number	Vertical refresh rate in Hz **(1)**
BitsPerPixel	number	Number of bits used by one pixel **(2)**

(1) With some adapters (in particular the standard vga device) the RefreshRate is equal to 1. This means 60 Hz.
(2) correspondence between bits per pixel and number of colors.

Bits	Colors

4	16
8	256
16	65536
24	16 millions
32	16 millions

5.3.6.4 Devices

Devices available in the device manager of Windows computers. Currently not available for Windows 9x computers.

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
DeviceType	string	device type in clear
id_DeviceType	string	GUID of the device type
DeviceName	string	Device name
DeviceLocation	string	Device location
Manufacturer	string	Manufacturer
ActiveService	string	Driver service. Link with table services field internal_name
PnpInstanceID	string	PnP Id of the device

5.3.6.5 ServersSubnets

List subnets to which each server belongs.

Data field	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
subnet	string	Subnet IP address and mask (e.g. 10.1.0.0/255.255.0.0)

5.3.6.6 netcards

5.3.6.6.1 Description

This table lists the network adapter cards installed on all Windows Systems (includes Windows 9x).

5.3.6.6.2 Fields

Field name	Data type	Description
id_snapshot	number	snapshot auto-number
server_name	string	Netbios name of the server without the 2 backslashes.
manufacturer	string	Manufacturer of the card.
title	string	String describing logically the network adapter.
driver	string	Internal name of the driver.
usedhcp	boolean	True if the IP address of this server is allocated by DHCP.

ips	string	List of the IP addresses associated with this server.
MacAddress	string	MAC address of the network adapter
gateways	string	List of the gateways used by this workstation.
wins1	string	Primary WINS server address.
wins2	string	Secondary WINS server address.
PnpInstanceID	string	Link to the devices table field *PnpInstanceID*
NetConnection	string	Name of the network connection for this adapter
dns1	string	IP address of the first DNS server
dns2	string	IP address of the second DNS server
dns_suffix	string	DNS suffix
DhcpServer	string	IP address of the DHCP server
LeaseTerminatesTime	datetime	Expiration date of the DHCP lease
LeaseObtainedTime	datetime	Start date of the DHCP lease

5.3.6.6.3 Example

As an example, to list all the servers with a Token Ring network adapter made by Olicom, use the following SQL query:

```
SELECT DISTINCT server_name
FROM netcards
WHERE
UPPER(manufacturer) = 'OLICOM' AND
title LIKE '%Token%'
```

5.3.6.7 NetComponents

Network services and protocols.

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
ComponentType	number	See appendix 1
ComponentName	number	Name of the network component

5.3.6.7.1 Appendix 1 Network component types

Value	Meaning
0	Protocol
1	Client service
2	Server service

5.3.6.8 processors

5.3.6.8.1 Description

This table lists all the processors of a computer. There is one entry per processor. The processor frequency is not available on Windows 9x computers.

5.3.6.8.2 Fields

Field name	Data type	Description

id_snapshot	number	snapshot auto-number
server_name	string	Netbios name of the server without the backslashes.
mhz	number	Processor's frequency.
vendor	string	Name of the processor's manufacturer
model	string	Intelligible name of the processor (if available)
version	string	Cpu Id (family, model and stepping)
Serial	string	serial number of the processor (rarely available)
ExternalClock	number	Bus speed in MHz
L1Cache	number	size (KB) of the L1 cache if available
L2Cache	number	size (KB) of the L2 cache if available
L3Cache	number	size (KB) of the L3 cache if available
model2	string	for debugging purpose only
model3	string	more precise model

5.3.6.8.3 Example

To list all the servers with a 250 MHz frequency, use the following SQL query:

```
SELECT server_name
FROM processors
WHERE mhz = 250
```

5.3.6.9 MemSlots

Memory slots

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
InstalledSize	number	Size of the installed memory module (in MB)
MaxSize	number	Maximum size for the memory module (in MB)
MemoryType	number	Type of memory (see Appendix 1)
Speed	number	Speed in MHz
SlotName	string	Slot name on the motherboard

5.3.6.9.1 Appendix 1 Memory type

Value	Meaning
1	Other
2	Unknown
3	DRAM
4	EDRAM
5	VRAM
6	SRAM
7	RAM
8	ROM
9	FLASH
10	EEPROM
11	FEPROM
12	EPROM

13	CDRAM
14	3DRAM
15	SDRAM
16	SGRAM
17	RDRAM
18	DDR

5.3.6.10 printers

5.3.6.10.1 Description

This table describes all shared printers and their properties.

5.3.6.10.2 Fields

Field name	Data type	Description
id_snapshot	number	network snapshot auto-number
id_printer	number	Identifier of the printer record (link aces/object_id.
id_share	number	Identifier of the share record sharing this printer.
name	string	Name of the printer.
port	string	Physical port of the printer.
state	number	Describes the current status of the printer (see Appendix 1).
ppm	number	Number of pages printable per minute.
location	string	Physical location of the printer.
nbjobs	number	Number of jobs.
account_name	string	Full account name of the printer's owner.
driver	string	device driver of the printer (link to devices/devicename)
PrintProcessor	string	Print processor
DataType	string	Commonly RAW or EMF
SpoolDirectory	string	Spooler directory for the print queue
HorizontalDPI	number	Horizontal resolution in DPI
Vertical DPI	number	Vertical resolution in DPI
MaxDPI	number	Maximum resolution in dot per inch
Attributes	number	
Orientation	number	1 = Portrait/ 0 = Landscape
PaperSize	number	See appendix 2 for the meaning of the number
PaperLength	number	Paper length in mm
PaperWidth	number	Paper width in mm
Color	number	1 = Yes / 0 = No
Zoom	number	Zoom in %
DoubleSided	number	Double sided 1 = Yes / 0 = No
PaperSource	number	Number of the paper source

5.3.6.10.3 Appendix 1

Name	Value	Meaning
PRINTER_STATUS_BUSY	0x00000200	The printer is busy.

PRINTER_STATUS_DOOR_OPEN	0x00400000	The printer cover is open.
PRINTER_STATUS_ERROR	0x00000002	The printer is in an error state.
PRINTER_STATUS_INITIALIZING	0x00008000	The printer is initializing.
PRINTER_STATUS_IO_ACTIVE	0x00000100	The printer is in an active input/output state
PRINTER_STATUS_MANUAL_FEED	0x00000020	The printer is in a manual feed state.
PRINTER_STATUS_NO_TONER	0x00040000	The printer is out of toner.
PRINTER_STATUS_NOT_AVAILABLE	0x00001000	The printer is not available for printing.
PRINTER_STATUS_OFFLINE	0x00000080	The printer is offline.
PRINTER_STATUS_OUT_OF_MEMORY	0x00200000	The printer has run out of memory.
PRINTER_STATUS_OUTPUT_BIN_FULL	0x00000800	The printer's output bin is full.
PRINTER_STATUS_PAGE_PUNT	0x00080000	The printer cannot print the current page.
PRINTER_STATUS_PAPER_JAM	0x00000008	Paper jam
PRINTER_STATUS_PAPER_OUT	0x00000010	The printer is out of paper.
PRINTER_STATUS_PAPER_PROBLEM	0x00000040	The printer has a paper problem.
PRINTER_STATUS_PAUSED	0x00000001	The printer is paused.
PRINTER_STATUS_PENDING_DELETION	0x00000004	The printer is deleting a job.
PRINTER_STATUS_POWER_SAVE	0x01000000	
PRINTER_STATUS_PRINTING	0x00000400	The printer is printing.
PRINTER_STATUS_PROCESSING	0x00004000	The printer is processing a job.
PRINTER_STATUS_SERVER_UNKNOWN	0x00800000	
PRINTER_STATUS_TONER_LOW	0x00020000	The printer's toner is low.
PRINTER_STATUS_USER_INTERVENTION	0x00100000	The printer requires user's intervention.
PRINTER_STATUS_WAITING	0x00002000	The printer is waiting.
PRINTER_STATUS_WARMING_UP	0x00010000	The printer is warming up.

5.3.6.10.4 Appendix 2

Constant Name	Value	Meaning
	1	Letter 8 1/2 x 11 in
	2	Letter Small 8 1/2 x 11 in
	3	Tabloid 11 x 17 in
	4	Ledger 17 x 11 in
	5	Legal 8 1/2 x 14 in
	6	Statement 5 1/2 x 8 1/2 in
	7	Executive 7 1/4 x 10 1/2 in
	8	A3 297 x 420 mm
	9	A4 210 x 297 mm
	10	A4 Small 210 x 297 mm
	11	A5 148 x 210 mm
	12	B4 (JIS) 250 x 354
	13	B5 (JIS) 182 x 257 mm

5.3.6.10.5 Example

To view all printers shared by the server MYSERVER, use the following SQL Query:

```
SELECT printers.name, printers.location FROM printers, shares WHERE
shares.id_share = printers.id_share AND shares.server_name = 'MYSERVER'
```

5.3.7 Windows

5.3.7.1 aces

5.3.7.1.1 Description

This table contains the ACEs (access control entries) of the total scanned objects (files and printers).

5.3.7.1.2 Fields

Field name	Data type	Description
id_snapshot	number	auto-numbering of network snapshots.
object_id	number	Identifier of a file (see "realfiles") or a printer (see "printers") or a share (see "shares").
type	number	Type of access (can be: ACCESS_ALLOWED_ACE_TYPE = 1 or ACCESS_DENIED_ACE_TYPE = 0).
rightmask	number	Bit mask describing the type of access : allowed or denied (see Appendix).
account_name	string	Full account name corresponding to the ACE. This can be linked to a group or a user.
Rights	string	rwxd **r**ead **w**rite e**x**ecute **d**elete access rights

5.3.7.1.3 Appendix

Bits	Meaning
0 through 15	Specific rights. Contains the access mask specific to the object type associated with the mask.
16 through 23	Standard rights. Contains the object's standard access rights and can be a combination of the following pre-defined flags:

Bit	Flag	Meaning
16	DELETE	Delete access
17	READ_CONTROL	Read access to the owner, group, and discretionary access-control list (ACL) of the security descriptor
18	WRITE_DAC	Write access to the discretionary access-control list (ACL)
19	WRITE_OWNER	Write access to owner
20	SYNCHRONIZE	**Windows NT:** Synchronize access

Bits	Meaning
24	Access system security (ACCESS_SYSTEM_SECURITY). This flag is not a typical access type. It is used to indicate access to an ACL system. This type of access requires the calling process to have a specific privilege.
25	Maximum allowed (MAXIMUM_ALLOWED)
26 through 27	Reserved
28	Generic all (GENERIC_ALL)
29	Generic execute (GENERIC_EXECUTE)
30	Generic write (GENERIC_WRITE)
31	Generic read (GENERIC_READ)

5.3.7.1.4 Example

As an example, to list all the accounts which have a "denied access" to the printer "HP Color LaserJet 5" on the server MYSERVER, use the following SQL query:

```
SELECT DISTINCT
users.shortname , users.fullname
FROM
printers , users , aces , shares
WHERE
aces.object_id = printers.id_share AND
users.account_name = aces.account_name AND
shares.id_share = printers.id_share AND
shares.server_name = 'MYSERVER' AND
printers.name = 'HP Color LaserJet 5' AND
aces.type = 1
ORDER BY
users.shortname
```

5.3.7.2 acc_ownership

5.3.7.2.1 Description

This table is used to identify:
User accounts included in global groups
Global groups included in local groups
User accounts included in local groups

5.3.7.2.2 Fields

Field name	Data type	Description
id_snapshot	number	auto-numbering of network snapshots.
account_name	string	Name of the account owned by the user or by the global group.
owned_group_name	string	Name of the global group owned by the local group identified by the account_name.
owned_user_name	string	Name of user owned by the group (local or global) identified by account_name.

5.3.7.2.3 Example

As an example, in order to list all the users and global groups in the local 'Administrators' group of the 'COPERNET' domain , use the following SQL query:

```
SELECT owned_group_name, owned_user_name
FROM acc_ownership
WHERE account_name = 'COPERNET\Administrators'
```

5.3.7.3 users

5.3.7.3.1 Description

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
domain_name	string	Domain name (or computer name) of the user account.
user_sid	string	SID of the user.
shortname	string	Internal name of the account.
fullname	string	Full name of the account.

passwd_age	number	Number of seconds elapsed since the last password change.
privilege	number	Indicates the privilege of this user (0 for guest, 1 for normal user, or 2 for an administrator).
homedir	string	Path of the user home directory.
comments	string	Comment about the user.
script	string	Path of the user's logon script.
usr_comment	string	String containing a user comment.
workstations	string	String that contains the names of workstations from which the user can log on. As many as eight workstations can be specified; the names must be separated by commas (,).
last_logon	time	Time of the last user's logon.
last_logoff	time	Time of the last user's logoff.
expire_date	time	Time when the account will expire (if not specified, the account will never expire).
logonserver	string	String that contains the name of the server to which logon requests are sent. Server names should be preceded by two backslashes (\\). A servername of an asterisk (*) indicates that the logon request can be handled by any logon server.
num_logons	string	Number of successful logons known.
num_bad_logons	string	Number of bad logons known.
country_code	number	Country code for the user's language of choice.
code_page	number	Code page for the user's language of choice.
flags	number	Bit mask specifying more boolean properties about the account (see Appendix).
rid	number	Specifies the relative ID (RID) of the user. The RID is determined by the SAM when the user is created. It uniquely defines this user account to SAM within the domain.
profile	string	Specifies a path to the user's profile.
home_dir_drive	string	Specifies the drive letter assigned to the user's home directory for logon purposes.
expired	boolean	Indicates if the user's password has expired.
account_name	string	Windows NT complete user name (composed of domain_name, a backslash character and the shortname). This is the field that should be linked with other security relative tables where a security account field is present (like acc_ownership).

5.3.7.3.2 Appendix

Symbolic constant	Value	Meaning
UF_SCRIPT	0x00001	The logon script executed. This value must be set for Windows NT.
UF_ACCOUNTDISABLE	0x00002	The user's account is

		disabled.
UF_PASSWD_NOTREQD	0x00020	No password is required.
UF_PASSWD_CANT_CHANGE	0x00040	The user cannot change the password.
UF_LOCKOUT	0x00010	The account is currently locked out.
UF_DONT_EXPIRE_PASSWD	0x10000	Represents the password, which should never expire on the account.

5.3.7.3.3 Example

To list all the disabled user accounts, use the following SQL query:

```
SELECT shortname , fullname
FROM users
WHERE flags & 0x00002 <> 0
ORDER BY shortname
```

5.3.7.4 groups

5.3.7.4.1 Description

This table describes the list of groups in the SAM database of a server (or a PDC). To view groups and user relationships, use the acc_ownership table.

5.3.7.4.2 Fields

Field name	Data type	Description
id_snapshot	number	snapshots auto-numbering
server_name	string	name of the server that owns the group (**if the group belongs to a domain, the server_name is the domain name**).
group_sid	string	group's security identifier (SID)
group_name	string	Decorative name of the group.
description	string	Short text describing the group.
account_name	string	Windows NT full account name that should be used in security relative tables like acc_ownership.
global	boolean	True if the group is global or false if the group is local.

5.3.7.4.3 Example

To retrieve all the global groups of the domain 'MYDOMAIN', use the following SQL request:

```
SELECT name , description
FROM groups
WHERE server_name = 'MYDOMAIN' AND global = 1
ORDER BY name
```

5.3.7.5 jobs

5.3.7.5.1 Description

This table lists all the scheduled jobs (accessible via the "at" command) of NT servers.

5.3.7.5.2 Fields

Field name	Data type	Description
id_snapshot	number	snapshots auto-numbering
server_name	string	Netbios name of the server (without the two backslashes).
command	string	String describing the command to be executed at the specified time.
jobid	number	Identifier used by the scheduler service.
hour_run	string	Specifies the command executing time (HH:MM format).
flags	number	Bit mask describing the properties of the scheduler job (see Appendix 1).
days_of_month	string	String listing the days of the month the command should be executed.
days_of_week	string	String listing the days of the week the command should be executed.

5.3.7.5.3 Appendix 1

Following are the values used for the flags field bit mask:

Symbolic constant	Value	Meaning
JOB_RUN_PERIODICALLY	0x00000001	This flag bit is equal to the original value of this flag bit when a job was submitted.
JOB_RUNS_TODAY	0x00000004	This flag bit is set if JobId is larger than the current time of day of the computer from which this job is queued .
JOB_EXEC_ERROR	0x00000002	This flag bit is set whenever the Schedule service failed to execute successfully this job the last time this job was supposed to run.

5.3.7.5.4 Example

To list the jobs running each Monday, the following SQL query may be used:

```
SELECT * FROM jobs WHERE days_of_week LIKE '%Monday%'
```

5.3.7.6 AdServers

Settings and roles of active directory domain controllers.

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
domain_name	string	Domain of the domain controller
GlobalCatalog	number	Is global catolog 1 = Yes/ 0 = No
InfrastructureMaster	number	Is Infrastructure master 1 = Yes/ 0 = No
PdcEmulator	number	Is PDC emulator 1 = Yes/ 0 = No
RidMaster	number	Is RID master 1 = Yes/ 0 = No
SchemaMaster	number	Is Schema master 1 = Yes/ 0 = No
DomainNamingMaster	number	Is domain naming master 1 = Yes/ 0 = No
NtdsDirectory	string	Path to the *ntds* folder

NtdsLogDirectory	string	Path to the *ntds* log folder
SysVolDirectory	string	Path to the *sysvol* folder

5.3.7.7 IISServers

Microsoft IIS enabled services

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the IIS server without the two preceding backslash characters.
WebServer	number	The web service is running/not running 1/0
FtpServer	number	The ftp service is running/not running 1/0
SmtpServer	number	The SMTP service is running/not running 1/0
NntpServer	number	The NNTP service is running/not running 1/0
IISAdmin	number	The admin service is running/not running 1/0
IISWebAdmin	number	The web admin service is running/not running 1/0

5.3.7.8 DnsServers

Microsoft DNS servers' configuration.
The hereafter table lists links between fields and settings in the DNS administration console.
Please read the Microsoft DNS help for more information.

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
DatabaseDirectory	string	Folder were all zone file are stored. If empty means %Systemroot%\System32\Dns
Forwarders	string	See Forwarders tab of the DNS administration console (server properties)
ForwardingTimeout	number	See Forwarders tab of the DNS administration console (server properties)
LogLevel	number	Bit mask (see Appendix 1)
ListenAddresses		Interfaces tab of the DNS administration console (server properties)
NoRecursion	number	1/0 "Enable recursion" in the Advanced tab of the DNS administration console (server properties)
BindSecondaries	number	1/0 Bind Secondaries in the Advanced tab of the DNS administration console (server properties)
StrictFileParsing	number	1/0 "Failed on load if bad data" in the Advanced tab of the DNS administration console (server properties)
RoundRobin	number	1/0 "Enable Round robin" in the Advanced tab of the DNS administration console (server properties)
LocalNetPriority	number	1/0 "Enable netmask ordering" in the Advanced tab of the DNS administration console (server properties)
SecureResponses	number	1/0 "Secure cache against polution" in the Advanced tab of the DNS administration console (server properties)
ScavengingInterval	number	(hours) "Enable automatic scavenging of stale record"

		in the Advanced tab of the DNS administration console (server properties)
NameCheckFlag	number	1/0 "Fail load on bad data file" in the Advanced tab of the DNS administration console (server properties)
BootMethod	number	"Load zone data on startup". See appendix 2.

5.3.7.8.1 Appendix 1 Log level

Value	Meaning
0x0	None. The DNS Service does not create Dns.log.
0x1	Queries
0x10	Notifications
0x20	Updates
0xFE	Non-query transactions
0x100	Questions
0x200	Answers
0x1000	Send packets
0x2000	Receive packets
0x4000	UDP packets
0x8000	TCP packets
0xFFFF	All packets
0x10000	Active Directory write transaction
0x20000	Active Directory update transaction
0x1000000	Full packets
0x80000000	Write-through transactions

5.3.7.8.2 Appendix 2 Boot method

Value	Description
0	Unknown
1	Load from file
2	Load from registry
3	Load from registry and active directory

5.3.7.9 DnsZones

DNS zone from Microsoft DNS servers. Please see the Microsoft DNS help if you need more information.

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the DNS server without the two preceding backslash characters.
zone_name	string	Name of the zone
DatabaseFile	string	Files were all name definition are stored (in DatabaseDirectory)
MasterServers	string	Master server for this zone (only for not Active Directory integrated zones)

AllowUpdate	number	1/0 Allows Dynamic Updates
NotifyLevel	number	Notify button in the "Zone transfers" tab (See appendix 1)
NotifyServers	string	Notify servers if NotifyLevel = 2
SecureSecondaries	number	Allows Zone Transfer (see appendix 2)
SecondaryServers	string	List of secondary servers on which the zone can be transferred if SecureSecondaries = 2
Aging	number	0/1 scavenging is disable/enabled. Aging button in general tab "Scavenge stale resource records".
ScavengeServers	string	
RefreshInterval	number	Aging button in general tab
NoRefreshInterval	number	Aging button in general tab
DsIntegrated	number	1 The zone is integrated in the active directory/ 0 is not integrated
Type	number	1/2 Primary zone/Secondary zone

5.3.7.9.1 Appendix 1 Notify Level

Value	Description
0	No Notification
1	Notify only authoritative servers for this zone
2	Notify only servers specified in "Notify Servers"

5.3.7.9.2 Appendix 2 Allows Zone Transfer

Value	Description
0	To any servers
1	Only to authoritative servers for this zone
2	Only on servers listed in Secondary servers
3	

5.3.7.10 shares

5.3.7.10.1 Description

This table describes shares of your Windows Servers.

5.3.7.10.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
unc	string	UNC path of this share.
server_name	string	Name of the server sharing the resource.
share_name	string	Name of the share
comments	string	Comments of the share.
max_uses	number	Maximal number of users allowed to accessing the resource at the same time (if it equals -1, it means that there is no limit).
current_uses	number	Current number of users connected to the resource.
path	string	Local path of the resource.

permissions	number	Bit mask specifying the global permissions (resource level) of the share (see Appendix 1).
type	number	Specifies the type of the share (see Appendix 2).
id_share	number	Internal ID of the share used to link to tables "printers" or "realfolders" (id_share field)

5.3.7.10.3 Appendix 1

Following are the values used to encode the permissions bit mask:

Symbolic constant	Value	Meaning
ACCESS_READ	0x01	Permission to read data from a resource and, by default, to execute the resource.
ACCESS_WRITE	0x02	Permission to write data to the resource.
ACCESS_CREATE	0x04	Permission to create an instance of the resource (such as a file); data can be written to the resource as the resource is created.
ACCESS_EXEC	0x08	Permission to execute the resource.
ACCESS_DELETE	0x10	Permission to delete the resource.
ACCESS_ATRIB	0x20	Permission to modify the resource's attributes (such as the date and time when a file was last modified).
ACCESS_PERM	0x40	Permission to modify the permissions (read, write, create, execute, and delete) assigned to a resource for a user or application.
ACCESS_ALL	0x7F	Permission to read, write, create, execute, and delete resources, and to modify their attributes and permissions.

5.3.7.10.4 Appendix 2

Following are the possible values for the "type" data field:

Symbolic constant	Value	Meaning
STYPE_DISKTREE	0x01	Permission to read data from a resource and, by default, to execute the resource.
STYPE_PRINTQ	0x02	Permission to write data to the resource.
STYPE_DEVICE	0x04	Permission to create an instance of the resource (such as a file); data can be written to the resource as the resource is created.
STYPE_IPC	0x08	Permission to execute the resource.

5.3.7.10.5 Example

For example, to retrieve all the disk shares on server MYSERVER, use the following SQL query:

```
SELECT unc , comments
FROM shares
WHERE type = 0
```

5.3.7.11 services

5.3.7.11.1 Description

This table describes all the Windows NT services installed on a server. This table is filled only on Windows NT computers.

5.3.7.11.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
internal_name	string	Internal name of the service (used with the NET START and NET STOP syntax).
display_name	string	Display string for the service (shown on the Services applet of the control panel).
account_name	string	Windows NT complete user name of the service owner. You can link it to the account_name field of the users table.
state	number	Specifies the current state of the service (see Appendix 1).
type	number	Identifies the type of the service (see Appendix 2).
startmode	number	Identifies the service starting (see Appendix 3)
description	string	Description displayed in the service console
ImagePath	string	Path to the service executable
ServiceGroup	string	The service belong to this group

5.3.7.11.3 Appendix 1

Following are the constants used to identify the service state:
SERVICE_STOPPED = 0x1
SERVICE_START_PENDING = 0x2
SERVICE_STOP_PENDING = 0x3
SERVICE_RUNNING = 0x4
SERVICE_CONTINUE_PENDING = 0x5
SERVICE_PAUSE_PENDING = 0x6
SERVICE_PAUSED = 0x7

5.3.7.11.4 Appendix 2

Symbolic constant	Value	Meaning
SERVICE_WIN32_OWN_PROCESS	0x00000010	A service type flag that indicates a Win32 service that runs in its own process.
SERVICE_WIN32_SHARE_PROCESS	0x00000020	A service type flag that indicates a Win32 service that shares a process with other services.
SERVICE_KERNEL_DRIVER	0x00000001	A service type flag that indicates a device driver.
SERVICE_FILE_SYSTEM_DRIVER	0x00000002	A service type flag that indicates a file system driver.
SERVICE_INTERACTIVE_PROCESS	0x00000100	A flag that indicates a Win32 service process that can interact with the desktop.

5.3.7.11.5 Appendix 3

Symbolic constant	Value	Meaning
SERVICE_BOOT_START	0x00000001	Specifies a device driver started by the system loader. This value is valid only if the service type is SERVICE_KERNEL_DRIVER or SERVICE_FILE_SYSTEM_DRIVER.
SERVICE_SYSTEM_START	0x00000002	Specifies a device driver started by the IoInitSystem function. This value is valid only if the service type is SERVICE_KERNEL_DRIVER or SERVICE_FILE_SYSTEM_DRIVER.
SERVICE_AUTO_START	0x00000003	Specifies a device driver or Win32 service started by the service control manager automatically during system startup.
SERVICE_DEMAND_START	0x00000004	Specifies a device driver or Win32 service started by the service control manager when a process calls the StartService function.
SERVICE_DISABLED	0x00000005	Specifies a device driver or Win32 service that can no longer be started.

5.3.7.11.6 Example

To view all the services started at boot time on the server \\MYSERVER , use the following SQL query:

```
SELECT * FROM services WHERE server_name = 'MYSERVER' AND startmode =
0x00000001
```

5.3.7.12 hotfixes

5.3.7.12.1 Description

This table describes the list of hotfixes installed on the computer. A hotfix is a corrective patch for the Windows NT System. Hotfixes included in Windows NT Service Packs are not listed in this table.

5.3.7.12.2 Fields

Field name	Data type	Description
id_snapshot	number	Network snapshots auto-numbering
server_name	string	Netbios name of the server (without the two back slashs)
hotfix_name	string	Name of the hotfix.
comments	string	Comments about the hotfix.
description	string	Description of the hotfix.
installed_by	string	Account used to install the hotfix (usually not retrieved).
installed_on2	datetime	Where the hotfix has been installed (usually not retrieved).
backup_dir	string	Backup directory for the hotfix (usually not retrieved).
installed	boolean	Indicates if the hotfix is currently installed.
valid	boolean	Indicates if the hotfix is currently valid.

5.3.7.12.3 Example

The administrator of a local network has several problems with Exchange 5.5 and IIS 4.0 as described in the Microsoft Knowledge base in the Q147222 article. The problem is corrected with the Q147222 hotfix or with the Service Pack 4.
The following query can be used to list the Windows NT servers where the problem has been fixed:

```
SELECT DISTINCT hotfixes.server_name FROM hotfixes, servers WHERE
hotfixes.server_name = servers.server_name AND ((servers.sp='Service Pack
4') OR (hotfixes.hotfix_name='Q147222'))
```

5.3.7.13 SwapFiles

Swap files configuration.

Data field	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
Path	string	Path to the swap file (pagefile.sys).
Partition	string	Partition on which is located the swap file.
MinSize	number	Minimum allowed size (in MB) for the swap file.
MaxSize	number	Maximum allowed size (in MB) for the swap file.
CurrentSize	number	Current size of the swap file (in MB).
Usage	number	Current usage of the swap file (in %).
UsagePeak	number	Peak usage of the swap file (in %).

5.3.7.14 AccountPolicy

Acount logon policy for each scanned computer and domain (Configured in the "Security console" or in the "User manager for domains").

Data field	Data type	Data description
id_snapshot	number	Identifier of the network snapshot.
domain_name	string	Domain name (or computer name) of the policy.
PasswordMinAge	real	Minimum password age in days before a user can change it
PasswordMaxAge	real	Maximum password age in days
PasswordMinLength	integer	Minimum length of the password in characters
PasswordHistoryLength	integer	Number of password changes needed before a user can use the same password again
PasswordComplexity	integer	Currently not scanned
ForceLogoff	integer	Number of second after what the user is logged of after the expiration of logon hours. -1 means that the user will never be logged of.

5.3.7.15 ScheduledTasks

All tasks scheduled with the standard Windows scheduler are listed in this table.

Data field	Data type	Data description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.

TaskName	string	Name of the job file
NextRunTime	date	Next run time. A null value means never.
LastRunTime	date	Last run time. A null value means never.
StartCode	number	Error code if the task did not start. If the value is 0 the task successfully started.
ExitCode	number	Exit code of the started process. If the value is not 0 a problem occured during the execution.
Command	string	Executable file to start.
Arguments	string	Arguments for the executable.
WorkingFolder	real	Working folder for the executable
MaxRunTime	real	Max run time in days.
Flags	number	Task flags. See Appendix 1
Status	number	Task status. See Appendix 2
RunAs	string	Execution account for the process
Schedule	string	Description of the schedule

5.3.7.15.1 Appendix 1 Task flags

Symbolic name	Bit value	Description
TASK_FLAG_INTERACTIVE	0x1	
TASK_FLAG_DELETE_WHEN_DONE	0x2	The work item will be deleted when there are no more scheduled run times.
TASK_FLAG_DISABLED	0x4	The work item is disabled. This is useful to temporarily prevent a work item from running at the scheduled time(s).
TASK_FLAG_START_ONLY_IF_IDLE	0x10	The work item begins only if the computer is not in use at the scheduled start time. Windows 95 only.
TASK_FLAG_KILL_ON_IDLE_END	0x20	The work item terminates if the computer makes an idle to non-idle transition while the work item is running.
TASK_FLAG_DONT_START_IF_ON_BATTERIES	0x40	The work item does not start if its target computer is running on battery power. Windows 95 only.
TASK_FLAG_KILL_IF_GOING_ON_BATTERIES	0x80	The work item ends, and the associated application quits if the work item's target computer switches to battery power. Windows 95 only.

TASK_FLAG_RUN_ONLY_IF_DOCKED	0x100	
TASK_FLAG_HIDDEN	0x200	The work item is hidden. When the work item begins execution, it runs in a hidden window.
TASK_FLAG_RUN_IF_CONNECTED_TO_INTERNET	0x400	The work item runs only if there is currently a valid Internet connection.
TASK_FLAG_RESTART_ON_IDLE_RESUME	0x800	The work item starts again if the computer makes a non-idle to idle transition before all the work item's task_triggers elapse.
TASK_FLAG_SYSTEM_REQUIRED	0x1000	
TASK_FLAG_RUN_ONLY_IF_LOGGED_ON	0x2000	

5.3.7.15.2 Appendix 2 Tasks status

Symbolic name	Value	Description
SCHED_S_TASK_NOT_SCHEDULED	0x00041305	The work item is ready to run at its next scheduled time.
SCHED_S_TASK_RUNNING	0x00041301	The work item is currently running.
SCHED_S_TASK_READY	0x00041300	One or more of the properties that are needed to run this work item on a schedule have not been set.

5.3.7.16 RegValues

To fill this table you need to start the scan with the advanced wizard (Windows NT step) and specify the registry values you want to scan. To do this, copy for each value, the path and the name from regedit and merge them as follows: %pathname%\%ValueName%.

Data field	Data type	Data description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
RegPath	string	Registry path of the key/value
ValueData	string	Data in the key/value
ValueType	number	Type of the value (see Appendix)

5.3.7.16.1 Appendix registry value types

Number	Symbolic name	Description
0	REG_NONE	No value type
1	REG_SZ	Unicode nul terminated string
2	REG_EXPAND_SZ	Unicode nul terminated string (with environment variable references)
3	REG_BINARY	Free form binary
4	REG_DWORD	32-bit number
4	REG_DWORD_LITTLE_ENDIAN	32-bit number (same as REG_DWORD)

5	REG_DWORD_BIG_ENDIAN	32-bit number
6	REG_LINK	Symbolic Link (unicode)
7	REG_MULTI_SZ	Multiple Unicode strings
8	REG_RESOURCE_LIST	Resource list in the resource map
9	REG_FULL_RESOURCE_DESCRIPTOR	Resource list in the hardware description
10	REG_RESOURCE_REQUIREMENTS_LIST	
11	REG_QWORD	64-bit number
11	REG_QWORD_LITTLE_ENDIAN	64-bit number (same as REG_QWORD)

5.3.8 Software

5.3.8.1 versions

5.3.8.1.1 Description

This table describes signature and version information of files. It is linked to a file entry through the realfiles table.

5.3.8.1.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
id_realfile	number	Identifier of the file to link the record with the realfile entry.
file_ver	string	Version of the file.
product_ver	string	Version of the product.
OS	string	Name of the operating system the file is designed for.
type	string	Main type of the file.
subtype	string	Subtype of the file (depending on the main type).
comments	string	Comments of the file.
company	string	Company that designed the file.
file_desc	string	Textual description of the file.
product_name	string	Name of the product the file is part of.
internal_name	string	Internal name of the file.
copyright	string	Copyright of the product/file.
trademarks	string	Trademarks of the product/file.

5.3.8.1.3 Example

For example, to view the name of the company which designed the file USER32.DLL, use the following SQL query:

```
SELECT versions.company
FROM versions, realfiles
WHERE
versions.id_realfile = realfiles.id_realfile AND
realfiles.pathname = 'C:\WINNT\System32\USER32.DLL'
```

5.3.8.2 software

5.3.8.2.1 Description

This table lists all applications installed on each computer. This can be very useful if you want to be sure that you own enough licenses of your programs.

5.3.8.2.2 Fields

Field name	Data type	Description
id_snapshot	number	Identifier of the network snapshot.
server_name	string	Netbios name of the server without the two preceding backslash characters.
product	string	Name of the software (as shown in the Add/Remove programs control panel applet).
uninstaller	string	Path of the program removing the software from the computer.
InternalName	string	Key in the registry
InstallSource	string	Location of the setup file (Windows installer setup only)
DisplayVersion	string	Textual version number
Publisher	string	Publisher
InstallDate	time	Installation date (Windows installer setup only)
LastModificationDate	time	Installation date (if not upgraded) or last upgrade date.
Version	number	Version number (Windows installer setup only)
VersionMajor	number	Major version number (Windows installer setup only)
VersionMinor	number	Minor version number (Windows installer setup only)
EstimatedSize	number	Size of the application (in KB) (Windows installer setup only)

5.3.8.2.3 Example

To know how many licenses of WinZip are needed in the domain 'MYDOMAIN', use the following SQL query:

```
SELECT COUNT(*)
FROM software, server_name
WHERE
software.server_name = servers.server_name AND
software.product = 'WinZip' AND
servers.server_name = 'MYDOMAIN'
```

5.3.8.3 realfolders

This table describes all folders available on your Windows computers (or a subset). See the software scan configuration for more information about scanning folders and files. Shared folders are scanned if shares are selected in the Windows scan configuration.

Field name	Data type	Description
id_snapshot	number	snapshot auto-number
server_name	string	Netbios name of the server without the 2 backslashes.
id_realfolder	number	Identifier of this folder. The field is used to link tables such as aces\object_id
id_share	number	Link to the share if the folder is shared (shares table).
pathname	string	Full path of the folder.

foldername	string	Name of the folder
attribs	number	Bit mask specifying the folder's attributes (see Appendix in table realfiles).
time_created	time	Time when the folder was created.
account_name	string	Owner of the file. The field can be linked with an entry of the groups table or the user table.
realsize	number	Size of the folder including al subdirectories and files (Bytes)
compressedsize	number	Currently not scanned
NbFiles	number	Number of files in the folder (scan files needed)
NbFolders	number	Number of subfolders in the folder (scan files needed)

5.3.8.4 realfiles

5.3.8.4.1 Description

This table describes all files available on your Windows computers (or a subset if you define file masks or folder restrictions). See the software scan configuration for more information about scanning files.

5.3.8.4.2 Fields

Field name	Data type	Description
id_snapshot	number	snapshot auto-number
server_name	string	Netbios name of the server without the 2 backslashes.
id_realfile	number	Identifier of this file. The field is used to link tables such as versions.
pathname	string	Full path of the file.
attribs	number	Bit mask specifying the file's attributes (see Appendix).
realsize	number	Real size of the file.
compressedsize	number	Compressed size of the file.
time_created	time	Time when the file was created.
time_modified	time	Last modified time.
time_accessed	time	Last accessing time.
account_name	string	Owner of the file. The field can be linked with an entry of the groups table.

5.3.8.4.3 Appendix

Symbolic constant	Value	Meaning
FILE_ATTRIBUTE_ARCHIVE	0x00000020	The file or directory is an archived file or directory. Applications use this attribute to mark files for backup or removal.
FILE_ATTRIBUTE_COMPRESSED	0x00000800	The file or directory is compressed. For a file, this means that the file is compressed. For a directory, this means that compression is the default for newly created files and subdirectories.
FILE_ATTRIBUTE_DIRECTORY	0x00000010	The handle identifies a directory.

FILE_ATTRIBUTE_ENCRYPTED	0x00000040	The file or directory is encrypted. For a file, this means that data in the file is encrypted. For a directory, this means that encryption is the default for newly created files and subdirectories.
FILE_ATTRIBUTE_HIDDEN	0x00000002	The file or directory is hidden. It is not included in an ordinary directory listing.
FILE_ATTRIBUTE_NORMAL	0x00000080	The file or directory has no other attributes set. This attribute is valid only if used alone.
FILE_ATTRIBUTE_OFFLINE	0x00001000	The file data is not immediately available. Indicates that the file data has been physically moved to offline storage.
FILE_ATTRIBUTE_READONLY	0x00000001	The file or directory is read-only. Applications can read the file but cannot write to it or delete it. If this is a directory, applications cannot delete it.
FILE_ATTRIBUTE_REPARSE_POINT	0x00000400	The file has an associated reparse point.
FILE_ATTRIBUTE_SPARSE_FILE	0x00000200	The file is a sparse file.
FILE_ATTRIBUTE_SYSTEM	0x00000004	The file or directory is part of the operating system or is used exclusively by the operating system.
FILE_ATTRIBUTE_TEMPORARY	0x00000100	The file is being used for temporary storage. File systems attempt to keep all of the data in memory for a quicker access, rather than flushing it back to mass storage. A temporary file should be deleted by the application as soon as it is no longer needed.

5.3.8.4.4 Example

To retrieve all the compressed files shared on server MYSERVER, use the following SQL query:

```
SELECT pathname
FROM realfiles
WHERE attribs & 0x800 <> 0
```

5.3.9 Event log

5.3.9.1 ET_Events

WinReporter insert in this table all scanned events. This table is compliant with EvenTrigger 2.0. If more than 20 parameters are available for an event you will find them in ET_Params.

Data field	Data type	Description
id_snapshot	number	snapshot auto-number
Ref	number	Insertion order of the event in the table (index)
Computer	string	Name of the computer where the event was generated

LogName	string	Name of the event log
EventId	number	Identifier of the event
Source	string	Source of the event
Category	string	Category of the event (Source specific)
Type	number	Type of the event (Error, Warning, Information, Success Audit, Failure Audit)
EventTime	date	Time generation of the event
Message	string	The event message
User	string	User account associated with the event
RecordNumber	number	Order of the event in the eventlog (since the last clear)
ParamCount	number	Number of dynamic parameters for the event
Param1	string	First dynamic parameter
...		
ParamN	string	N^{th} dynamic parameter
...		
Param20	string	20^{th} dynamic parameter

5.3.9.2 ET_Params

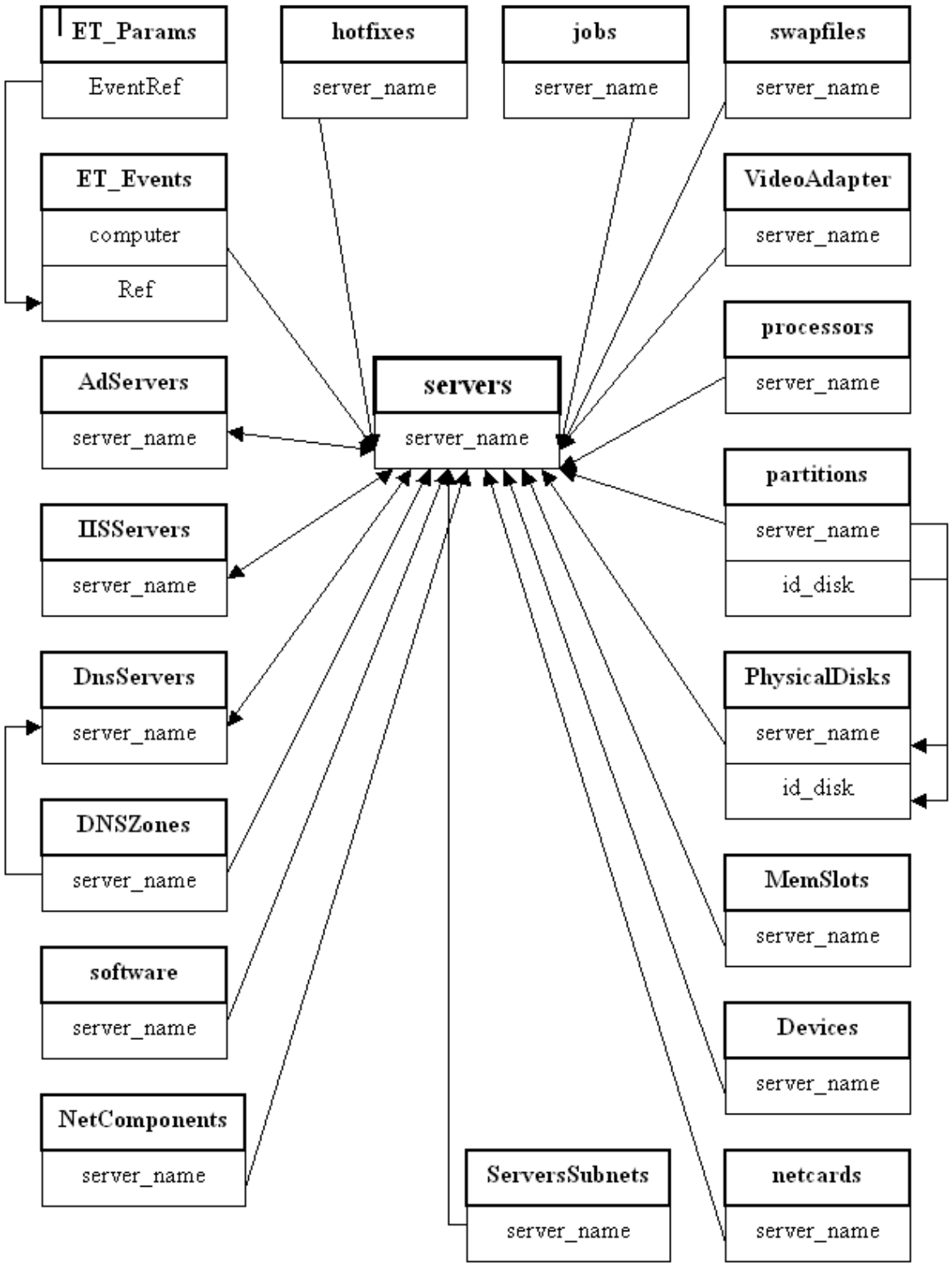
If you have more than 20 parameters in an event you will find all additional parameters in this table. In most cases events don't have so many parameters so this table will be mostly empty.

Data field	Data type	Description
id_snapshot	number	snapshot auto-number
EventRef	number	Index number of the event in the *ET_Events* table (*ref* field)
ParameterValue	string	Value of the parameter
ParameterOrder	number	Order of the parameter in the dynamic parameters list

5.4 Relationships

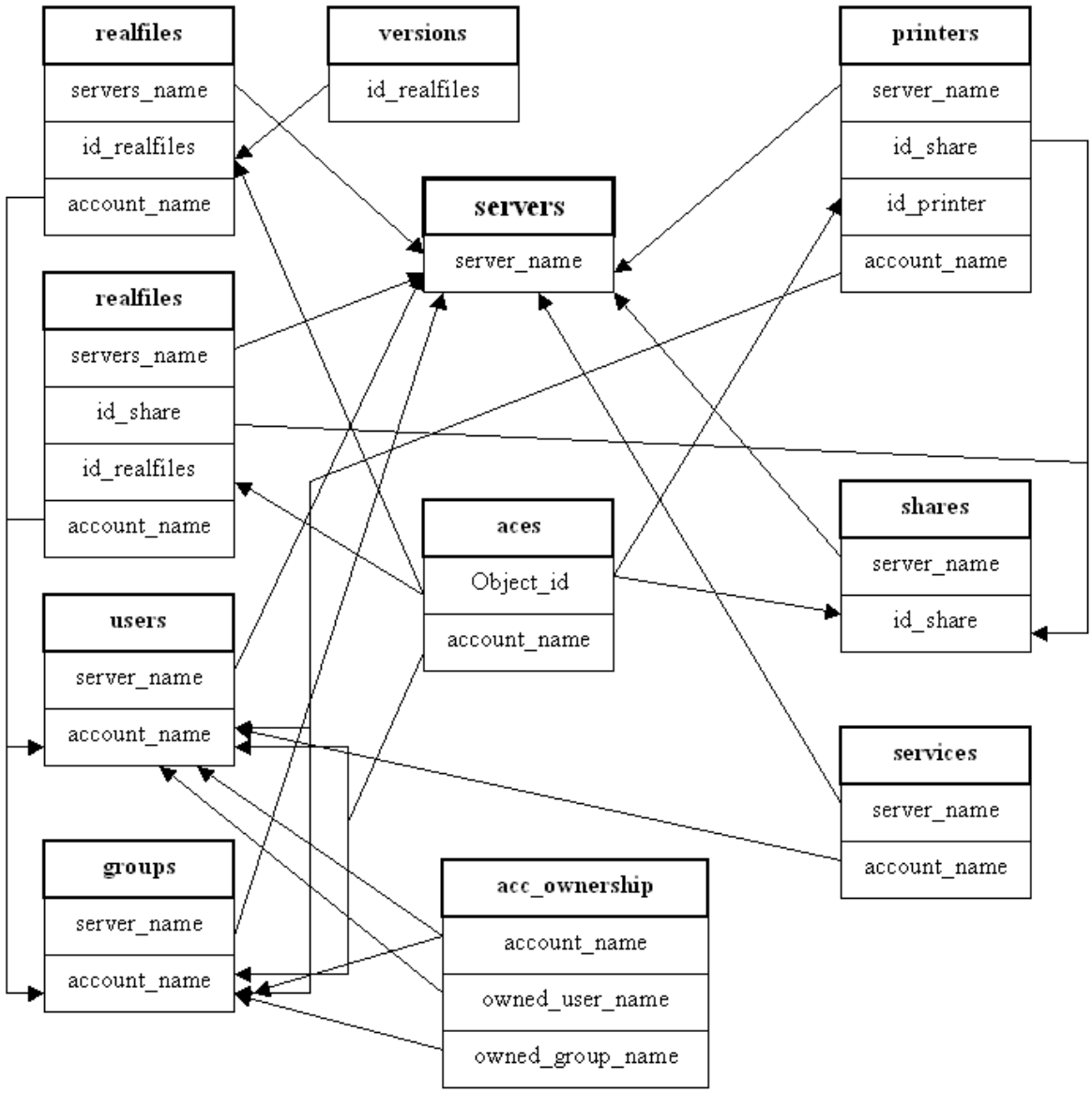
5.4.1 Relationships I

To help you to design query here are relationships between most tables of the WinReporter database.



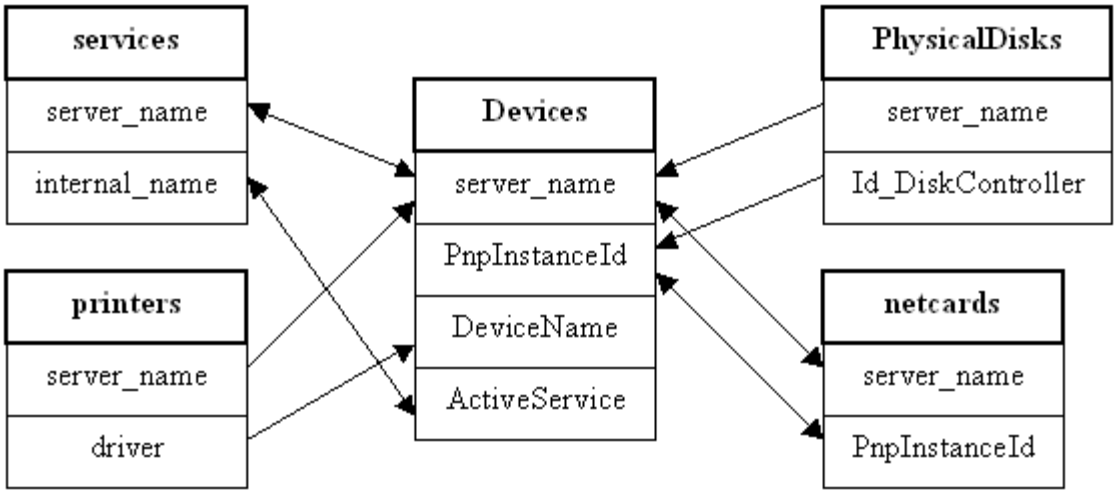
5.4.2 Relationships II

Relations ship between WinReporter tables around objects and security.



5.4.3 Relationships III

Relationships between WinReporter tables around devices.


services
server_name
internal_name
printers
server_name
driver
Devices
server_name
PnpInstanceId
DeviceName
ActiveService
PhysicalDisks
server_name
Id_DiskController
netcards
server_name
PnpInstanceId

6 Index

8