

Table of Contents

Part I Welcome	4
Part II Requirements / Installation	4
Part III Command Line Applications	5
1 ADSList	5
Usage	5
2 CheckDB	6
Usage	6
Event Log Logging	8
3 CheckTCP	9
Usage	9
4 CheckURL	10
Usage	10
Event Log Logging	11
5 DirectoryMonitor	12
Usage	12
6 DirectorySize	13
Usage	13
7 FileReplace	13
Usage	14
8 FPing	14
Usage	14
9 GetHTTP	15
Usage	15
10 IPMon	16
Usage	17
11 IsAdmin	18
Usage	19
12 Logoff Delay	19
Usage	19
13 NTPClient	20
Usage	20
14 PageSNPP	20
Usage	20
15 ServiceSecure	21
Usage	21
Hints	22
Screenshots	23
16 SHA Checksum Generator	24
Usage	24
17 Sleep	24

Usage	25
18 SuperDelete	25
Usage	25
19 TaskSecure	26
Usage	26
20 Uptime	26
Usage	27
21 WakeOnLAN	27
Usage	27
Part IV Graphical User Interface Applications	28
1 Hardlink Shell Extension	28
Hardlinks	28
Usage	28
Browsing for a hard link.....	28
Drag & Drop.....	30
2 NetSend	32
Usage	33
Tray Icon	34
3 Password Assistant	34
Usage	35
Hints	36
Command Line Version	36
4 ShutdownTimer	37
Usage	38
Conditional Countdown Options.....	40
Tray Icon	41
5 Event Message Browser	41
Usage	42
Part V Applications running as a Service	42
1 ServiceScheduler	42
Installation	43
Configuration	43
Security	44
Part VI Credits	44
1 WinPcap	44
Part VII Questions or Problems?	48
Part VIII Suggestions?	48
Part IX Other Software from NETIKUS.NET	48

Index

0

1 Welcome



Thank you for using NTToolkit, we hope that the NTToolkit will help you with your daily administration / networking tasks!

The NTToolkit is a set of small and useful utilities designed to help network administrators with their daily administrative tasks. The NTToolkit is freeware and constantly under development, and most of the tools found are spin-offs from [EventSentry](#), our event log, server and network monitoring suite.

If you have any questions regarding NTToolkit then please contact us through our support forums at forums.netikus.net.

Your **NETIKUS.NET** team.

2 Requirements / Installation

Requirements

All NTToolkit applications require one of the following Operating Systems:

- Windows NT
- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista
- Windows Server 2008



Windows Vista Notes: Most of the executables require administrative access (e.g. uptime.exe), as such you will have to launch the command-line prompt with a user that has administrative permissions (right-click the icon and select "Run As Administrator").

The **Hard link Shell Extension** needs **Windows 2000** or **Windows XP** and only works on NTFS file systems.

The NTToolkit will **not run** on Windows 95, 98 or ME.

Installation

To install the software, simply run the installer and select the components to be installed.

To update an existing installation, simply run the latest installer which should update the existing installation automatically. If the update fails, simply uninstall the existing version (if still possible) and reinstall the latest version.

3 Command Line Applications

3.1 ADSList

ADSList analyzes one or more directories and lists any alternate data streams (aka as "hidden streams") that are associated with a file. When an alternate data stream is found, the name of the stream is displayed along with the regular file the stream is associated with. The output will also show a summary that lists:

- the number of files analyzed
- the number of files that have an alternate data stream associated with them
- the number of alternate data streams that have been found
- the elapsed time

The main purpose of `adslst.exe` is to give a System Administrator a command-line utility that can be run/scheduled on a regular basis to reveal any hidden streams on a server or workstation.



ADSList only works on **NTFS** volumes, since alternate data streams are only supported on the NTFS file system.

Return Code (%ERRORLEVEL%)

ADSList returns 0 when no alternate data streams have been found, and returns 1 if at least one alternate data stream has been found.

Files

`adslst.exe`

3.1.1 Usage

Command Line Parameters

```
adslst <DIRECTORY> /s /q
```

DIRECTORY	The directory to analyze, uses the current directory if none is specified
/s	Include sub directories
/q	Quiet output, omit headers, omit error messages and only prints text when alternate data streams are found



You can schedule **adslst.exe** using the [EventSentry Application Scheduler](#), which can analyze the return code and output of the utility and **only log an event to the event log** when one or more alternate data streams have been found.

Examples

Example 1: Look for alternate data streams in the **%SYSTEMROOT%** directory, including sub directories

```
adslst %SYSTEMROOT% /s
```

Example 2: Look for the alternate data streams in the `C:\Windows\System32`, including sub directories, and use the quiet output

```
adslst C:\Windows\System32 /s /q
```

Sample Output

```
C:\>adslst C:\ /s
```

ADSLList v1.0 by NETIKUS.NET ltd [compiled on Jul 27 2008]
(support@netikus.net)

List alternate data streams on NTFS volumes.

```
0001:  C:\\Documents and Settings\\Administrator\\Favorites\\Download details
Feature Pack for SQL Server 2005 Nov 2005.url
       favicon
0002:  C:\\Documents and Settings\\Administrator\\Local Settings\\Temporary
Internet Files\\Content.IE5\\68B6GYDG\\LSSetup_en_US[1].exe
       Zone.Identifier
0003:  C:\\Documents and Settings\\Administrator\\Local Settings\\Temporary
Internet Files\\Content.IE5\\CUQF6SXR\\launch[1].lsf
       Zone.Identifier
0004:  C:\\images\\temp\\logo_v2_white.png
       ?Q30lsldxJoudresxAaaqpcawXc
       {4c8cc155-6c1e-11d1-8e41-00c04fb9386d}
0005:  C:\\images\\logo_v2_white.jpg
       ?Q30lsldxJoudresxAaaqpcawXc
       {4c8cc155-6c1e-11d1-8e41-00c04fb9386d}
```

Summary:

```
=====
Time elapsed:                5 second(s)
Files Processed:            66680
Files with alternate data streams:  5
Alternate Data Streams found:      7
```

3.2 CheckDB

CheckDB verifies a database connection through ODBC to ensure that a connection to a database can be established. You can optionally also run a single SQL statement after a successful connection has been established. A connection can be specified either through a DSN (Data Source Name) or a connection string. The output from CheckDB can either be displayed in the command line or logged to the event log.

With CheckDB, you can verify that:

- a database server is available
- the database specified in the DSN / connection string is online
- the specified user has permission to log into the database server and database
- the optionally specified SQL statement executed successfully



As with all ODBC-based utilities, you will need to ensure that the necessary ODBC drivers are installed on the machine from which you run this utility.

Return Code (%ERRORLEVEL%)

CheckDB returns 0 when no errors have been encountered, and returns 1 if an error (e.g. database is unavailable, SQL query cannot execute) was encountered. Use event logging (/le) for detailed troubleshooting information.

Files

checkdb.exe

3.2.1 Usage

Command Line Parameters

```
checkdb <DSN|ConnectionString> /u <USER> /p <PASS> /q <SQLQUERY> /lc /le
```

DSN or Connection String	DSN or connection string to connect to
/u <USERNAME>	Username to connect as (DSN only)
/p <PASSWORD>	Password for USERNAME (DSN only)
/q <SQLQUERY>	SQL query to execute upon successful connection
/lc	Log all output to console
/le	Log all output to event log



When using a connection string, both username and password need to be specified inside the connection string, the **/u** and **/p** options cannot be used.

Examples

Example 1: Check whether the database defined in DSN **EventSentry** is available and log output to the console

```
checkdb EventSentry /u eventsentry_web /p !$^&3jdk3 /lc
```

Example 2: Check whether the database defined in the connection string is available and log output to the event log

```
checkdb "driver={SQL Server};server=mssqlserver;Network=DBMSSOCN;database=EventSentry;uid=eventsentry_svc;pwd=1234" /le
```

Example 3: Check whether the database defined in DSN **EventSentry** is available, verify that the table **ESEventlogLog** exists and log output to the console and event log

```
checkdb EventSentry /u eventsentry_web /p !$^&3jdk3 /q "select top 1 * from ESEventlogLog" /lc /le
```

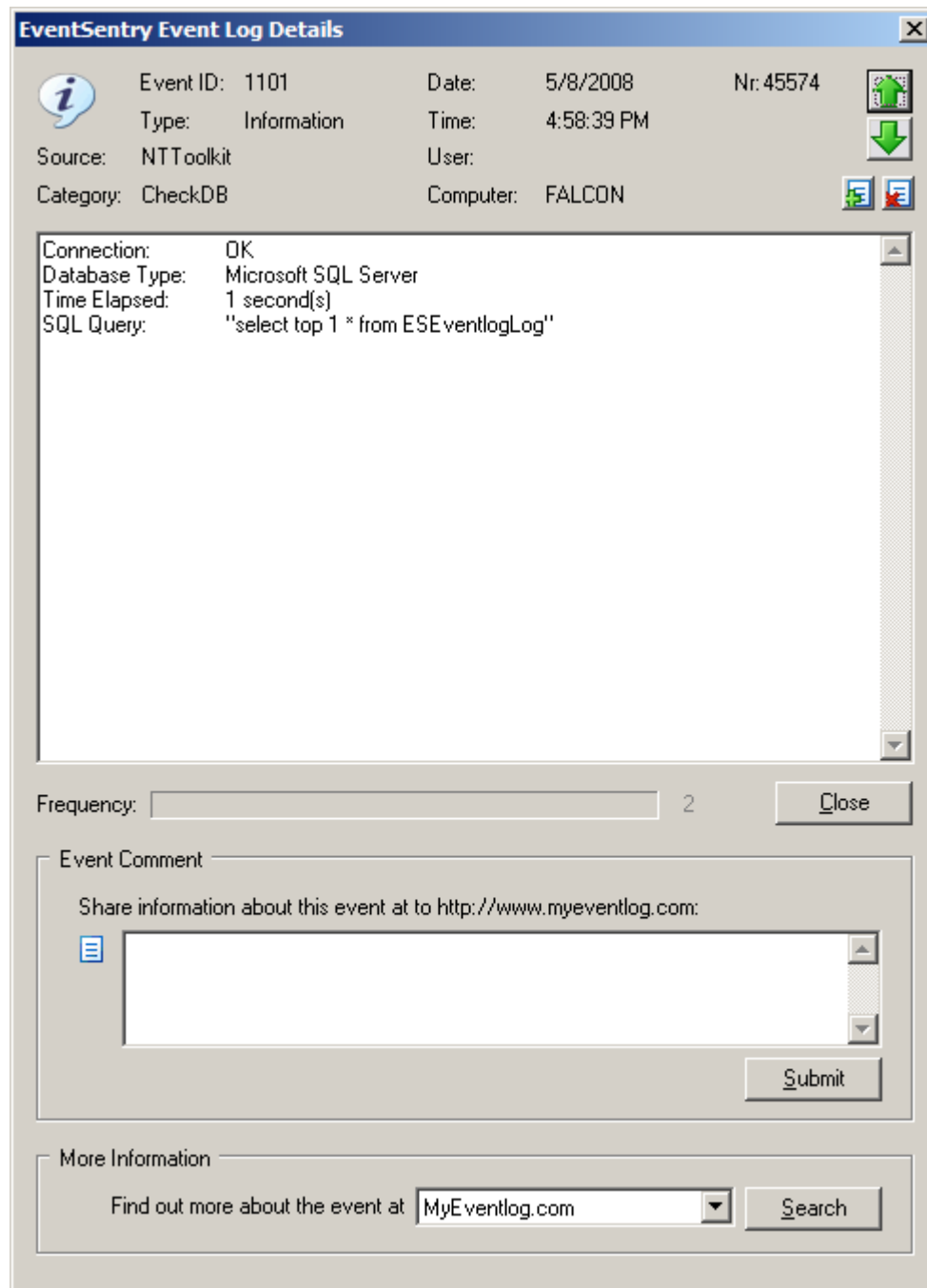
Sample Output

```
C:\>checkdb SQLSERVER /u eventsentry_web /p password /q "select top 1 * from ESEventlogLog" /lc /le
```

```
-----
CheckDB v1.0 by NETIKUS.NET ltd [ compiled on May 8 2008 ]
                                (support@netikus.net)
-----
```

Verify a database connection through ODBC, optionally execute SQL statement.

```
Connect      : OK
DB Type     : Microsoft SQL Server
Time        : 1 second(s)
SQL Query:  select top 1 * from ESEventlogLog -> OK
```



Example event from the event log

3.2.2 Event Log Logging

When specifying the /le option, CheckDB will log all actions to the event log with the event source **NTToolkit** and the event category **CheckDB**. All successful checks will be logged as **informational** events, whereas all errors will be logged as **error** events.

CheckDB logs the following events to the event log:

Event ID	Event Message
1100	Connection: OK

```

1101      Database Type: %1
          Time Elapsed: %2
          Connection:   OK
          Database Type: %1
          Time Elapsed: %2
1102      SQL Query:   "%3"
          Connection:   ERROR
          Reason:       %1
1103      Connection:   OK
          Database Type: %1
          Time Elapsed: %2
          SQL Query:   "%3" -> ERROR
          Failure Reason: %4

```

3.3 CheckTCP

CheckTCP is an command line application that can determine whether a TCP port on a host is open. Additionally you can receive initial data sent from the remote host through an open TCP connection, such as when connecting to most SMTP hosts.

CheckTCP can be used to quickly determine whether a certain TCP port is open and optionally display any data sent by the remote host over the established connection. CheckTCP is not intended to be used as a portscanner and does not have good performance for such use.

CheckTCP returns an **%ERRORLEVEL%** of 0 when the port is open and an **%ERRORLEVEL% > 0** when the port is not open. This is useful when using checktcp.exe in scripts.

Files

checktcp.exe

3.3.1 Usage

Command Line Parameters

```
checktcp hostname | ipaddress port /show /timeout:timeout
```

hostname / ipaddress	Hostname or IP address to connect to
port	TCP port on host to connect to, only one port can be specified at one time
/show	Displays any data sent by the remote host through the TCP connection. This works with some protocols, such as SMTP or SSH
/timeout:timeout	Override the default timeout of 3 seconds when specifying the /showheader switch.

Examples

Example 1: Check whether port **25** on host **smtp.aol.com** is open

```
checktcp smtp.aol.com 25
```

Example 2: Check whether port 25 on host mail.hotmail.com is open and display data

```
checktcp mail.hotmail.com 25 /show
```

Sample Output

```
c : \>checktcp mail.hotmail.com 25 /show
```

```
-----
CheckTCP V1.0 by NETIKUS.NET [ compiled on May 9 2004 ]
```

(support@netikus.net)

Command-line utility to check whether a TCP port is open.

```
Status:  mail.hotmail.com:25  is  open
Data:    220  mc9-f37.hotmail.com  Microsoft  ESMTP  MAIL  Service,  Version:
5.0.2195.6824  ready at  Sun, 9 May 2004 19:11:01 -0700
```

3.4 CheckURL

CheckURL verifies availability of a web page and can also check for content inside the page and/or verify the checksum of that page. CheckURL can also log its actions to the event log and supports web-based authentication for password-protected web pages.

With CheckURL you can:

- verify that a web page exists and is accessible
- check if a particular text exists or does not exist in a web page
- verify that credentials for a web page work
- log all output to the event log or console
- automatically create checksums to be notified when the content of a web page changes

Checksum Monitoring

With checksum monitoring, CheckURL downloads the specified page and creates a SHA checksum which it stores in the registry (HKLM\Software\netikus.net\NTToolkit\CheckURL). Upon a subsequent check, CheckURL compares the current checksum with the previously stored checksum and notifies you when it has changed. You can optionally log results to the event log with the **/evt** switch (use CHECKSUM_CHANGE and CHECKSUM_EQUAL).

Content Monitoring

With content monitoring, CheckURL looks for a specific string in a page and notifies you whether the string has been found or not. You can optionally log results to the event log with the **/evt** switch (use TXT_FOUND and TXT_NOTFOUND).

Return Code (%ERRORLEVEL%)

CheckURL returns 0 when no errors have been encountered, and returns 1 if an error (e.g. unable to establish connection with web site) was encountered. Use event logging (/le) for detailed troubleshooting information.

Files

checkurl.exe

3.4.1 Usage

Command Line Parameters

```
checkurl /u <USER> /p <PASS> /checksum /checksums_clear /t <TEXT> /cs /lc
/le /evt <OPTIONS>
```

```
/u MyUser           Authenticate as user MyUser to web page
/p "my pass"       Use specified password for /u option
```

```
/checksum          Create or compare checksum of page
/checksums_clear   Delete all cached checksums from the registry
```

```
/t "text to look for"  Search for specified text on page
/cs                Make text search case sensitive (case insensitive by default)
```

/lc Log all output to console
 /le Log all output to event log
 /evt "options" Rules for event log logging

Examples

Example 1: Log an error to the event log when the page http://www.eventsentry.com/support_knownproblems.php changes.
 checkurl /checksum /lc /le /evt
 "CHECKSUM_CHANGE=Error,CHECKSUM_EQUAL=Ignore"
http://www.eventsentry.com/support_knownproblems.php

Example 2: Log a warning to the event log when the string "About Google" is not found in URL <http://www.google.com> and log results to the event log
 checkurl /t "About Google" /le /evt
 "TXT_FOUND=Information,TXT_NOTFOUND=Warning" <http://www.google.com/>

3.4.2 Event Log Logging

When specifying the /le option, CheckURL will log all actions to the event log with the event source **NTToolkit** and the event category **CheckURL**. Depending on the options specified in the /evt parameter, CheckURL will either log an informational, warning or error event to the event log.

Event Log Rules (/evt)

The event log rules allow you to specify with which severity certain checks will be logged to the event log. For example, you can log an ERROR to the event log if a particular text is not found in an URL, or a WARNING when the checksum of a page has changed.

You can create the event log rules with the following pattern pair: ACTION=SEVERITY, ACTION=SEVERITY,...

Actions

The following actions are available:

- CHECKSUM_CHANGE A checksum change has been detected
- CHECKSUM_EQUAL A checksum has not changed
- TXT_FOUND The specified text has been found in the page
- TXT_NOTFOUND The specified text has not been found in the page

Severities

Events can be logged with the following severities:

- Error Logs event as an error
- Warning Logs event as a warning
- Information Logs event as a warning
- Ignore Does not log an event to the event log

Some examples for rules are:

- TXT_FOUND=Ignore,TXT_NOTFOUND=Warning
- CHECKSUM_CHANGE=Error,CHECKSUM_EQUAL=Information

Events

CheckURL logs the following events to the event log:

Event ID	Event Message
1000	Unable to connect to "%1" due to error "%2" (%3).
1001	The checksum of URL "%1" was initialized to "%2".
1002	The checksum of URL "%1" changed to "%2".
1003	The checksum of URL "%1" did not change.

3.5 DirectoryMonitor

The Directory Monitor utility monitors a directory (and optionally sub directories) and displays all file changes in real-time. Dirmon will show you when

- Files are added
- Files are deleted
- Files are modified

Dirmon also lets you specify include **or** exclude filters, so that you can skip files that you are not interested in or only show files that you are interested in.

Files

dirmon.exe

3.5.1 Usage

Command Line Parameters

```
dirmon /d [path] /s (/i filename,filename,..) | (/e filename,filename,..)
```

```
/d path          Path to the directory to monitor
/s              Include subdirectories
/i *.exe,*.sys  When specified, only lists files that match items in the comma-separated list
/e *software.log When specified, ignores files that match items in the comma-separated list
```



Both the **/i** and **/e** parameters support wildcards (* and ?), but you can only use one at a time. You can specify multiple file names with a comma. You **cannot use both /i and /e at the same time.**

Examples

Example 1: Monitor the C:\Windows directory, including subdirectories, but ignore files with the **.log** extension and files that end in **ntuser.dat**

```
dirmon /d C:\Windows /s /e *.log,*ntuser.dat
```

```
-----
Directory Monitor v1.0 by NETIKUS.NET ltd [ compiled on Oct 19 2007 ]
                                     (support@netikus.net)
-----
```

Monitors directories for write changes in real-time.

```
10/19/2007 13:37:26: ~MODIFIED      :
WINDOWS\system32\wbem\Repository\Fs\OBJECTS.MAP
10/19/2007 13:37:26: ~MODIFIED      :
WINDOWS\system32\wbem\Repository\Fs\MAPPING2.MAP
10/19/2007 13:37:26: ~MODIFIED      :
WINDOWS\system32\wbem\Repository\Fs\MAPPING.VER
10/19/2007 13:37:26: ~MODIFIED      : Documents and Settings\All
Users\Application Data\Skype\Plugins\_sstore8.dat
10/19/2007 13:37:26: ~MODIFIED      : Documents and Settings\All
```

Users\Application Data\Skype\Plugins_sstore8.dat

7 filtered file transactions not shown.

3.6 DirectorySize

The Directory Size utility calculates the current size of a directory, including subdirectories, and displays it on the screen. The output shows the number of files and directories searched and the total size in physical (actual size taken up on the disk) and logical (actual file size) bytes.

Dirsize will process the current directory if no command-line arguments were passed.

Files

dirsize.exe

3.6.1 Usage

Command Line Parameters

dirsize [path]

/d path Path to the directory to calculate

Examples

Example 1: Display the size of the C:\Fujitsu directory

dirsize C:\Fujitsu

```
-----
DirSize v1.0 by NETIKUS.NET ltd [ compiled on May 14 2007 ]
                               (support@netikus.net)
-----
Command-line utility to calculate the size of a directory.
```

Summary (took 0 seconds):

```
=====
Directories/Files searched: 9/51
Logical Directory Size : 4,430,372 bytes
Physical Directory Size : 4,538,368 bytes
```

3.7 FileReplace

FileReplace is a command line utility that parses a directory (including subdirectories) and replaces multiple occurrences of one template file.

Example

You have file **C:\WebSite\Default\index.html** and would like to replace all other **index.html** files in the directory **D:\WWW** (including subdirectories) with **C:\WebSite\Default\index.html**. File Replace will do that for you by typing in one command.

Files

filereplace.exe

3.7.1 Usage

Command Line Parameters

filereplace <directory> <source file> [/test]

Source File	The original file the other files will be replaced with
Directory	The directory to parse and look for duplicates of this file
/test	Do not actually replace the files, only show which files would be replaced

Example

Example 1: Replace all files named **default.php** in the folder **E:\Data** (including subfolders) with **D:\Templates\default.php**

```
filereplace d:\data d:\templates\default.php
```

3.8 FPing

FPing (Fast Ping) is an command line application that sends ICMP echo-type packets pings remote hosts to determine whether they are up and running. FPing is intended to be a replacement for the ping.exe utility that ships with Windows. FPing will ping remote hosts much faster the built-in ping utility, but offers only the most commonly used features.

FPing returns an **%ERRORLEVEL%** of 0 when the remote host was reachable and an **%ERRORLEVEL% > 0** when the remote host did not respond to the ICMP echo requests.

To determine whether a particular TCP port is open use **CheckTCP**.

Files

fping.exe

3.8.1 Usage

Command Line Parameters

fping *hostname* /count:*packets* /size:*packetsize* /delay:*delay* /loop

hostname / ipaddress	Hostname or IP address to ping
/count: <i>packets</i>	Sets the number of ICMP packets to send, default are 4.
/size: <i>packetsize</i>	Sets the payload size of the ICMP packets in bytes, default are 32.
/delay: <i>delay</i>	Determines how long (in ms) to wait between each ICMP packet, default are 150ms.
/loop	Pings host indefinitely, abort with CTRL-C

Examples

Example 1: Ping host www.netikus.net

```
fping www.netikus.net
```

Example 2: Ping host www.eventsentry.com with 8 packets and 64 bytes in size

```
fping www.eventsentry.com /count:8 /size:64
```

Sample Output

```
c:\>fping www.eventsentry.com /count:2 /size:128 /delay:300
Binging www.eventsentry.com@216.92.10.83
128 bytes from 216.92.10.83: seq = 0 time: 32 ms TTL = 49
128 bytes from 216.92.10.83: seq = 1 time: 32 ms TTL = 49
Roundtrip Summary:
Average: 32 ms, Minimum: 32 ms, Maximum: 32 ms, Rate: 100%
```

3.9 GetHTTP

GetHTTP is an command line application that allows you to retrieve files through the **HTTP** protocol. Please note that SSL is not supported.

Files

gethttp.exe

3.9.1 Usage

Command Line Parameters

```
gethttp [-f filename] [-u UserAgent] [http://]www.somehost.com/file.htm
```

-f filename Instead of writing to a file with the name found in the URL use *filename*
-u UserAgent Override the default user agent used by GetHTTP. This is useful for sites that use cloaking.
URL The URL pointing to the file to download. The starting **http://** is optional and can be left out



Please note that existing local files will be overwritten without a prompt.

Examples

Example 1: Download the file http://www.netikus.net/downloads/rpm_update.pl.gz

```
gethttp www.netikus.net/downloads/rpm_update.pl.gz
```

Example 2: Download the file <http://www.netikus.net/downloads/getconfig.sh> and save it locally as `getconfig`

```
gethttp -f getconfig http://www.netikus.net/downloads/getconfig.sh
```

Example 3: Download the document

http://www.experts-exchange.com/Programming/System/Windows__Programming/MFC/Q_22133017.html and save it locally as `answer.html`

```
gethttp -u "Googlebot" -f answer.html
http://www.experts-exchange.com/Programming/System/Windows__Programming/MFC/Q_22133017.html
```

Sample Output

```
c:\>gethttp www.netikus.net/downloads/getconfig.sh
```

```
-----
GetHTTP V1.1 by NETIKUS.NET [ compiled on Oct 23 2002 ]
                                     (nttoolkit@netikus.net)
-----
```

```
Command-line utility to retrieve files over HTTP
```

```
Saved file "getconfig.sh" in current directory
Received 9.53 kb in 0.310 seconds (30.76 kb/sec)
```

3.10 IPMon

IPMon is a command-line utility that utilizes the [WinPcap network driver](#) to monitor IP traffic to the local host for troubleshooting and monitoring purposes. Unlike full blown network sniffers, IPMon only shows the IP addresses and ports (for TCP/UDP) affected, and groups output so that repetitive traffic is not being displayed. For example, any IP address that communicates with the local host where IPMon runs is only displayed once.

Using IPMon, a system or network administrator can quickly see which TCP/UDP/ICMP communication is taking place from the local host, without having to parse through thousands of lines network captures. IPMon currently supports the following IP protocols:

- UDP
- TCP
- ICMP

and has the following filtering / output capabilities:

- Filter based on TCP port number
- Filter based on UDP port number
- Filter protocols (UDP, TCP, ICMP)
- Show any IP address only once, even when communication is flowing to/from multiple ports
- Show any IP address / remote port combination only once
- Resolve IP addresses to host names

Simply running IPMon without arguments will, in most cases, reveal interesting information about the IP traffic to the local host.



In this version IPMon only shows incoming traffic sent from remote hosts **to** the local machine. Outgoing traffic, as well as traffic sent to interfaces other than a local one, are not shown.

IPMon outputs captured traffic to the command line as follows:

```
[Timestamp] [IP Protocol] [Remote IP Address] [Source Port->Destination
Port] [Resolved Host Name]
```

- Timestamp: Current time as Hour:Minute:Seconds
- IP Protocol: The IP protocol used, either UDP, TCP or ICMP
- Remote IP Address: The IP address of the remote host sending a packet to the local host
- Source Port: The UDP/TCP source port (from the remote host)
- Destination Port: The UDP/TCP destination port (on the local machine)
- Resolved Host Name: The FQDN of the remote host, when run with **/resolve** option. Only available when the IP address can be resolved through DNS.

```

Capturing traffic on interface:
Intel(R) 82566DC-2 Gigabit Network Connection [192.168.1.100]

[TCP] [192.168.6. ] [1433->54636]
[TCP] [192.168.6. ] [3306->55360]
[TCP] [192.168.6. ] [445->50906]
[TCP] [66.150.96.118] [80->55349]
[TCP] [ ] [22->49376]
[TCP] [75.57.94.167] [40353->49385]
[TCP] [209.85.163.125] [5222->49388]
[TCP] [66.39.30.10] [80->55362]
[TCP] [209.85.133.127] [80->55368]
[TCP] [192.168. ] [5222->51079]
[TCP] [216.92.199.161] [80->55369]
[TCP] [74.125.93.99] [80->55376]
[UDP] [192.168. ] [137->137]

Summary:
=====
Total Packets analyzed: 1071
Total Bytes analyzed: 672561

```

Figure 1: All TCP and UDP communication

```

[UDP] [12.201.76.73] [46019->61354] [12-201-76-73.client.mchsi.com]
[UDP] [208.120.104.175] [54972->61354] [user-387gq5f.cable.mindspring.com]
[UDP] [82.6.171.187] [46515->61354] [spci-harg1-0-0-cust954.seac.broadband.ntl.com]
[UDP] [89.78.224.7] [27457->61354] [chello089078224007.chello.pl]
[UDP] [82.240.165.244] [52094->61354] [nan92-6-82-240-165-244.fbx.proxad.net]
[UDP] [193.144.51.45] [61703->61354] [gorry.dc.fi.udc.es]
[UDP] [68.116.180.65] [43761->61354] [68-116-180-65.dhcp.oxfr.ma.charter.com]
[UDP] [81.66.170.78] [45490->61354] [81-66-170-78.rev.numericable.fr]
[UDP] [69.64.63.138] [13235->61354] [balder089.startdedicated.com]
[UDP] [18.139.7.176] [17715->61354] [warehouse-six-eighty-seven.mit.edu]
[UDP] [82.137.49.47] [25255->61354] [82-137-49-47.rdsnet.ro]
[UDP] [85.91.136.183] [21158->61354] [85-91-136-183.spectrumnet.bg]
[UDP] [88.213.192.142] [19014->61354] [ppptp-192-142.dobrich.net]
[UDP] [121.92.153.78] [55492->61354] [ntkngw376078.kngw.nt.ftth.ppp.infoweb.ne.jp]
[UDP] [190.142.89.96] [20446->61354]
[UDP] [193.219.33.50] [45100->61354] [merkurijus.pit.ktu.lt]
[UDP] [76.208.48.214] [60854->61354] [adsl-76-208-48-214.dsl.sbnadin.sbcglobal.net]
[UDP] [68.77.2.26] [55669->61354] [adsl-68-77-2-26.dsl.emhril.ameritech.net]
[UDP] [98.192.118.72] [36583->61354] [c-98-192-118-72.hsd1.ga.comcast.net]
[UDP] [80.221.26.75] [43717->61354] [hoasnet-fe1add00-75.dhcp.inet.fi]
[UDP] [93.152.133.29] [28079->61354] [2072597225.ddns.onlinedirect.bg]
[UDP] [83.29.30.213] [42407->61354] [boo213.neoplus.adsl.tpnet.pl]
[UDP] [220.135.230.107] [46807->61354] [220-135-230-107.hinet-ip.hinet.net]
[UDP] [173.20.64.221] [63327->61354] [173-20-64-221.client.mchsi.com]
[UDP] [190.160.131.236] [58871->61354]
[UDP] [59.85.240.139] [40399->61354] [139.net059085240.t-com.ne.jp]
[TCPP] [216.92.199.161] [80->56628] [inetikus.net]

```

Figure 2: IPMon quickly shows questionable traffic via UDP (in this case Skype is the "culprit")

3.10.1 Usage

Command Line Parameters

```

ipmon  [/i INTERFACE]  [/udp]  [/tcp]  [/icmp]  [/dport PORT]  [/sport PORT]
[/list]  [/group-port]  [/resolve]

```

/i INTERFACE The interface ipmon should be capturing packets on. If not interface is specified and only one interface with a valid IP address exists on the system, then that interface will automatically be used. If multiple active interfaces exist, a list of interfaces will be presented for a selection.

/udp Capture UDP traffic (activated by default)

/tcp	Capture TCP traffic (activated by default)
/icmp	Capture ICMP traffic (not activated by default)
/dport PORT	Only include UDP/TCP packets that are sent to local port PORT
/sport PORT	Only include UDP/TCP packets that are sent from remote port PORT
/list	List all available interfaces
/group-port	By default, IPMon shows each remote IP address that sent a packet to the local machine only once, even when packets have been sent from different remote ports. Activating this option will result in more output since the same IP address will be shown multiple times if communication between different ports is taking place.
/resolve	Resolves the remote IP address to a host name. Please note that using this option when capturing large amounts of packets may incur a delay with real time monitoring.

Examples

Example 1: Display all UDP + TCP communication from the default interface.

```
ipmon
```

Example 2: Display all UDP, TCP and ICMP communication from the default interface and resolve all host name where possible

```
ipmon /udp /tcp /icmp /resolve
```

Example 3: Display all UDP, TCP and ICMP communication from the default interface and resolve all host name where possible

```
ipmon /udp /tcp /icmp /resolve
```

Example 4: Display all TCP communication from interface
 \Device\NPF_{E84D78AB-18AC-4705-A7CA-221EC0CDAE12}

```
ipmon /i \Device\NPF_{E84D78AB-18AC-4705-A7CA-221EC0CDAE12} /TCP
```

3.11 IsAdmin

IsAdmin detects whether a user is a member of the local **Administrators** group, either through direct membership in the Administrators group or through indirect membership through another group.

IsAdmin by default evaluates the currently logged on user (in whose context IsAdmin runs) but you can also specify a different username through the command line.

Workstation / Member Server vs. Domain Controller

If IsAdmin is executed on a workstation or member server then it will check the local **Administrators** group, but you can also force IsAdmin to check the **Administrators** group of the domain instead. When executed on a domain controller, IsAdmin has to check the domain's **Administrator** group.

Return Code (%ERRORLEVEL%)

IsAdmin returns 0 if the specified user is an Administrator or 1 if the user is not an administrator or an error occurred.

Files

isadmin.exe

3.11.1 Usage**Command Line Parameters****isadmin** <USERNAME> /forcedomain

<USERNAME>	Checks if USERNAME has administrative rights. If no username is passed then the currently logged on user is used. Always specify the username without the domain prefix.
/forcedomain	Always check the domain's Administrator group, even on non-domain controllers (optional).

Examples

Example 1: Check if user "john.doe" is a local Administrator
isadmin john.doe

Example 2: Checks if the currently logged on user is a member of the domain's administrator group
isadmin /forcedomain

3.12 Logoff Delay

Logoff Delay lets you log off a user in a specified amount of time. This can be useful if you want to restrict the logon time of users.

In order to rely on **Logoff Delay** you will need to make sure however that users have no ability to kill running processes since **Logoff Delay** runs as a user process and can therefore be killed.

Files

logofdel.exe

3.12.1 Usage**Command Line Parameters****logofdel** <timeout> [logfile] [/force] [/hide]

timeout	Seconds after which the user will be logged off
logfile	Full path to a log file where Logoff Delay will write information to
/force	Force a logoff, no questions will be asked and unsaved data will be lost
/hide	Detach from the console and become "invisible". The process can still be seen and controlled through task manager

Examples

Example 1: Logoff a user after 5 minutes and hide the application

```
logofdel 300 /hide
```

Example 2: Logoff a user after 10 minutes, write information to the logfile c:\logoff_delay.txt, hide and force a logoff

```
logoffdel 600 c:\logoff_delay.txt /force /hide
```

3.13 NTPClient

NTPClient returns the current time as reported by a NTP server and calculates the local clock offset based on RFC 1315 and RFC 2030. NTPClient supports the NTP (Network Time Protocol) up to version 3.

NTPClient can optionally adjust the local time to match the time reported by the NTP server. Network latency is taken into consideration when calculating the clock offset, with a precision down to milliseconds.

Files

ntpclient.exe

3.13.1 Usage

Command Line Parameters

```
ntpclient /set <NTP Server>
```

/set	Set the local time to the time retrieved from the NTP server
NTP Server	host name or IP address of the NTP server

Examples

Example 1: Retrieve the current time from host time-a.nist.gov

```
ntpclient time-a.nist.gov
```

Example 2: Set the local time to the time reported by host mydc.mydomain.local

```
ntpclient /set mydc.mydomain.local
```

3.14 PageSNPP

PageSNPP (SNPP stands for *Simple Network Paging Protocol*) is a command line application that sends short messages to pages using the SNPP protocol. You can only use PageSNPP if your paging provider supports SNPP.

PageSNPP itself has a message limit of 1500 characters, but check with your paging provider to see what their maximum supported message length for your plan and device are (usually less than 500).

For a list of SNPP servers check the web site <http://www.notepage.net/snpp.htm>.

PageSNPP returns an **%ERRORLEVEL%** of 0 when the message was sent successfully, and an **%ERRORLEVEL% > 0** when the message could not be sent.

Files

pagesnpp.exe

3.14.1 Usage

Command Line Parameters

```
pagesnpp <snpp server> <snpp port> <pager id> "message"
```

SNPP server	The SNPP server to use, check with your provider
SNPP port	The TCP port to us when talking to the SNPP server
Pager ID	The ID of the pager
message	The actual message to send to the pager

Examples

Example: Send the message "It is time to download & install EventSentry" to the pager ID 443234 via snpp.skytel.com:

```
pagesnpp snpp.skytel.com 7777 443234 "It is time to download & install
EventSentry"
```

3.15 ServiceSecure

ServiceSecure allows you to reset service passwords by specifying the **username** and **password** rather than having to specify the service names themselves or changing the password manually.

Password changes of user accounts that are being used for services no longer have to be feared. Just run **ServiceSecure** and tell it what username has changed to what password, the rest is done automatically. **ServiceSecure** even restarts services after the password has been changed (optional).

With **ServiceSecure** you can literally change the password of service accounts in seconds on a number of machines (when used in a batch file).

Files

srvsec.exe

3.15.1 Usage

Command Line Parameters

```
srvsec [\servername] [username] [password] [/restart]
```

<without options> enumerates all services, grouped by service account username

\\servername Perform all actions on computer "**servername**"

username List only services running under the specified **username**

password Set the password to **password**. Only valid in conjunction with **username**.

/changepwd Changes the password in the SAM database (or Active Directory, depending on network configuration)

/restart Restart the service(s) after the password has been changed. Only valid in conjunction with the *username* and *password* options.

Examples

Example 1: Enumerate all services on host \\server1

```
srvsec \\server1
```

Example 2: Show all services on host \\fileserver that are using the **DOMAIN\Administrator** account

```
srvsec \\fileserver DOMAIN\Administrator
```

Example 3: Change the service password of all services that are using the **DOMAIN\SrvAcc** username to "**yUye\$#34ww:**"

```
srvsec DOMAIN\SrvAcc yUye$#34ww:
```

Example 4: Change the service password of all services running on \\dbserver1 that are using the .\User1 username to "**blaUip432**" and restart the modified services

```
srvsec \\dbserver1 .\User1 blaUip432 /restart
```

Example 5: Change the service password of all services running on \\dbserver1 that are using the **wupdup** username to "**blaUip432**" and restart the modified services

```
srvsec \\dbserver1 wupdup blaUip432 /changepwd /restart
```

3.15.2 Hints

Specifying Usernames

ServiceSecure distinguishes between builtin, local and domain accounts. To see how **ServiceSecure** specifies user accounts simply run it once without command line parameters (or with only the \\server parameter).

Builtin, Local and Non-Domain accounts should be prefixed with a ".", like ".\Administrator".

Domain accounts should be prefixed with the domain name, like "DOMAIN\User1".

Service Dependencies

When specifying the **/restart** option the modified services will also be restarted. Note that services that depend on the modified services, even though unaffected, will also be restarted.

Example: You are modifying the service **MSSQLServer** which runs under the account "**DOMAIN1\SQLUser**". The service **SQLServerAgent**, which depends on **MSSQLServer**, runs under the **LocalSystem** account. However in order to stop and restart the **MSSQLServer** service the **SQLServerAgent** service will also have to be restarted. This is done automatically when the **/restart** switch is specified.

3.15.3 Screenshots



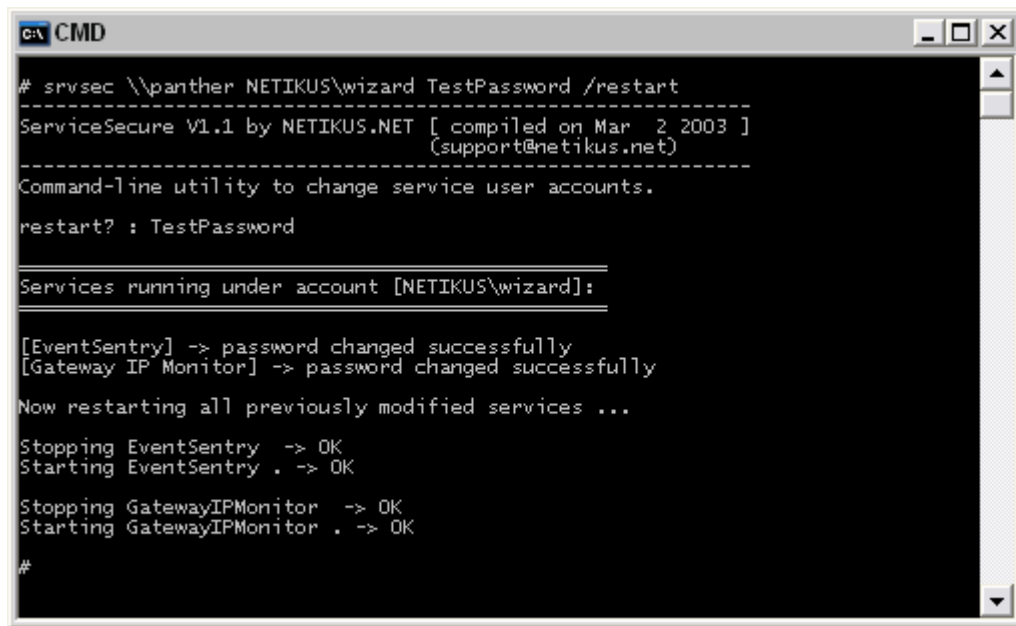
```
c:\ CMD
# srvsec
-----
ServiceSecure V1.1 by NETIKUS.NET [ compiled on Mar  2 2003 ]
                               (support@netikus.net)
-----
Command-line utility to change service user accounts.

-----
Services running under account [nt authority\local service]:
-----

[Alert]
[Application Layer Gateway Service]
[Remote Registry]
[Smart Card]
[Smart Card Helper]
[SSDP Discovery Service]
[TCP/IP NetBIOS Helper]
[Uninterruptible Power Supply]
[Universal Plug and Play Device Host]
[WebClient]

-----
Services running under account [localsystem]:
-----

[Application Management]
[Automatic Updates]
[AVG6 Service]
[Background Intelligent Transfer Service]
[BrSp]Service]
[ClipBook]
[COM+ Event System]
[COM+ System Application]
[Computer Browser]
[Cryptographic Services]
[DHCP Client]
[Diskkeeper]
[Distributed Link Tracking Client]
[Error Reporting Service]
[Event Log]
[EventSentry]
[Eventwatch NT]
[Fast User Switching Compatibility]
[Fax]
[Gateway IP Monitor]
[Help and Support]
[Human Interface Device Access]
[IBM PM Service]
[IMAPI CD-Burning COM Service]
[Indexing Service]
[Infrared Monitor]
[Internet Connection Firewall] (ICF) / Internet Connection Sharing (ICS)
[IPSEC Services]
[Logical Disk Manager]
[Logical Disk Manager Administrative Service]
[Messenger]
[Monitor Control Service]
[MS Software Shadow Copy Provider]
[Net Logon]
[NetMeeting Remote Desktop Sharing]
[Network Connections]
[Network DDE]
[Network DDE DSDM]
[Network Location Awareness (NLA)]
[NT LM Security Support Provider]
[Plug and Play]
[Portable Media Serial Number]
[Print Spooler]
```



```
C:\> CMD

# srvsec \\panther NETIKUS\wizard TestPassword /restart
-----
ServiceSecure V1.1 by NETIKUS.NET [ compiled on Mar  2 2003 ]
                                (support@netikus.net)
-----
Command-line utility to change service user accounts.

restart? : TestPassword

=====
Services running under account [NETIKUS\wizard]:
=====

[EventSentry] -> password changed successfully
[Gateway IP Monitor] -> password changed successfully

Now restarting all previously modified services ...

Stopping EventSentry -> OK
Starting EventSentry . -> OK

Stopping GatewayIPMonitor -> OK
Starting GatewayIPMonitor . -> OK

#
```

3.16 SHA Checksum Generator

The **SHA Checksum Generator** generates the SHA-256 checksum of a file and displays it on the screen. This is useful to ensure the integrity of a file and make sure that it has not been modified.

This utility is also included in EventSentry as an Add-On to the "File Monitoring" feature which can automatically generate SHA checksums.

To display and create a SHA checksum of a file, simply supply the file name as the first argument. Please keep in mind that generating the SHA checksum of large files (e.g. > 100Mb) can take a significant amount of time and CPU time.

Files

shachecksum.exe

3.16.1 Usage

Command Line Parameters

```
shachecksum    [filename]
```

Filename path to the filename to generate the checksum from

Examples

Example 1: Create the checksum of the C:\Windows\notepad.exe file

```
shachecksum    c:\windows\notepad.exe
```

3.17 Sleep

Sleep is an command line application that sleeps for X milliseconds and is most useful for use in batch files.

Sleep returns an **%ERRORLEVEL%** of 0 when the sleep received a valid argument and paused processing for > 0 milliseconds.

Files

sleep.exe

3.17.1 Usage

Command Line Parameters

sleep milliseconds

milliseconds Milliseconds to wait

Examples

Example 1: Sleep for 1 second

```
sleep 1000
```

Example 2: Sleep for 2.5 seconds

```
sleep 2500
```

3.18 SuperDelete

SuperDelete is a command line utility that parses a directory (including subdirectories) and deletes multiple occurrences of one file.

Example

Delete all **thumbs.db** files on the C drive of your computer.

Files

superdel.exe

3.18.1 Usage

Command Line Parameters

superdel <directory> <file to delete> [/test]

File to delete

The filename to delete

Directory

The directory to parse and delete occurrences of this file

/test

Do not actually replace the files, only show which files would be replaced

Example

Example 1: Delete all files named **thumbs.db** the folder "**C:\Documents and Settings**" (including subfolders).

```
superdel "c:\documents and settings" thumbs.db
```

3.19 TaskSecure

TaskSecure allows you to reset scheduled tasks passwords by specifying the **username** and **password** rather than having to manually open and reset each scheduled task on your network after a password change.

Password changes of user accounts that are being used for scheduled tasks no longer have to be feared. Just run **TaskSecure** and tell it what username has changed to what password, the rest is done automatically.

With **TaskSecure** you can literally change the password of scheduled tasks in seconds on a number of machines (when used in a batch file). **TaskSecure** works on both the local host and remote machines.

Files

tasksec.exe

3.19.1 Usage

Command Line Parameters

```
tasksec [\servername] [username] [password] [/restart]
```

<without options>	enumerates all scheduled tasks, grouped by account username
\\servername	Perform all actions on computer " servername "
username	List only scheduled tasks running under the specified username
password	Set the password to password . Only valid in conjunction with username .

Examples

Example 1: Enumerate all scheduled tasks on host **\\server1**

```
tasksec \\server1
```

Example 2: Show all scheduled tasks on host \\fileserver that are using the **DOMAIN\Administrator** account

```
tasksec \\fileserver DOMAIN\Administrator
```

Example 3: Change the account password of all scheduled tasks that are using the **DOMAIN\SrvAcc** username to "**yUye\$#34ww:**"

```
tasksec DOMAIN\SrvAcc yUye$#34ww:
```

3.20 Uptime

Uptime shows you the current uptime of the local host. Uptime can either update the current uptime every second and display it on the screen, or it can return the uptime one time and return. You can also have uptime return the uptime in seconds.

Files

uptime.exe

3.20.1 Usage

Command Line Parameters

uptime [/onetime] [/secs]

/onetime displays the current uptime one time and returns
/secs displays the uptime in seconds, instead of a formatted date and time

Examples

Example 1: Display the current uptime on the screen and automatically refresh it automatically every second

```
uptime
```

Example 2: Display the current uptime, in seconds, one time on the screen

```
uptime /onetime /secs
```

3.21 WakeOnLAN

The WakeOnLAN (WOL) utility sends a "magic" package to a network card, based on the MAC address. If the network card supports the "Wake On Lan" feature (and the feature is enabled in the BIOS of the computer), then the computer will power on automatically after receiving the packet.

You can also send the magic packet to a router, if the router supports direct broadcasts.

Files

wakeonlan.exe

3.21.1 Usage

Command Line Parameters

wakeonlan MAC-Address ([/i] ip-address)

MAC Address The MAC address of the NIC that is to be woken up
/i ip-address Optional: The IP address of a router or computer that is to receive the packet. Instead of sending the magic packet to the local broadcast address (255.255.255.255), you can also send it to a router which can then forward the packet to the local subnet.

The router must be configured to allow direct broadcasts for this to work.

Examples

Example 1: Wake up the computer with MAC address 00-19-A9-06-F0-23

```
wakeonlan 00-19-A9-06-F0-23
```

Example 2: Wake up the computer with MAC address 00-19-A9-06-F0-23 but send the packet through router with IP address 192.168.3.1

```
wakeonlan 00-19-A9-06-F0-23 /i 192.168.3.1
```

4 Graphical User Interface Applications

4.1 Hardlink Shell Extension

Hardlink Shell Extension is an extension to the Windows shell. It allows you to create hardlinks from within the explorer shell by right-clicking any file.

Files

hlshext.dll

4.1.1 Hardlinks

Background about Hardlinks

Hardlinks (up to now used mainly on Unix like systems) are pointers (similar to shortcuts) to another file. They can have the same name as the file they point to (if they are not in the same directory) and, since they are essentially just a pointer, have the **exact same** file attributes.

Requirements

Hardlinks can only be created on the same logical drive where the original file relies.

Modifying a hardlink

If you modify the hardlink of a file you automatically modify the original file - and vice versa.

Deleting a hardlink

If you delete a hardlink then the original files remains since you are just deleting the pointer. If you delete the original file then the hardlink remains and "**becomes**" the original file. All hardlinks (including the file itself) will need to be deleted for the file to actually be deleted from the filesystem.

4.1.2 Usage

You can create a hard link to a file in two ways, by **browsing for a hard link** or by **drag & drop**. Both methods are outlined in the next chapters.

With browsing you can choose a new name for the hard link, when you drag & drop (with the right mouse button pushed) the filename remains the same. This is useful if you want to create a hard link in a different directory.

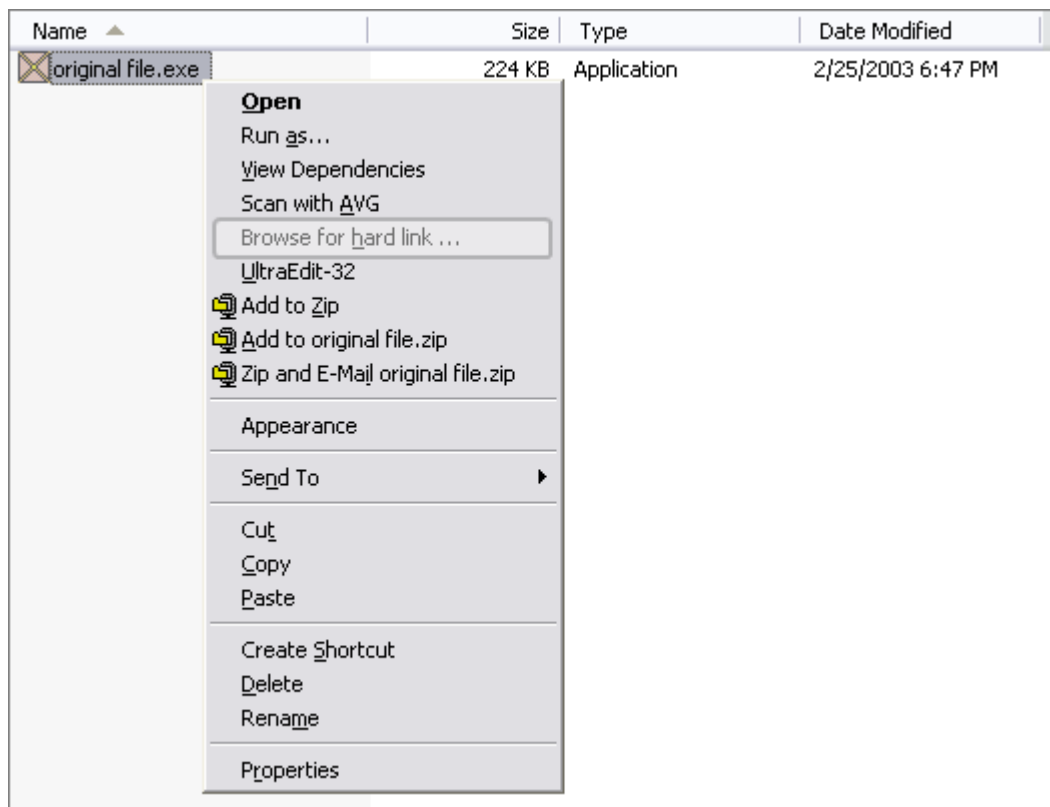
>> [Browsing for a Hard link](#)

>> [Drag & Drop](#)

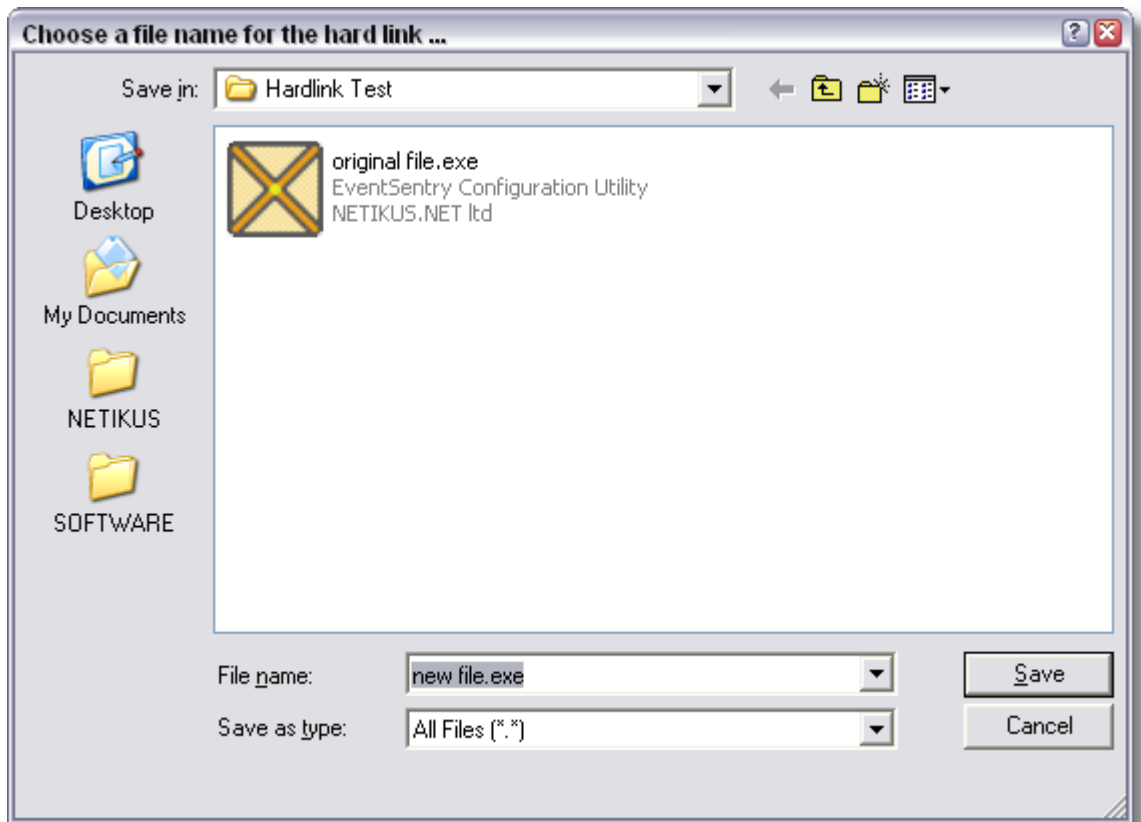
4.1.2.1 Browsing for a hard link

You can create a hard link to any file by right-clicking it. To browse for a hard link:

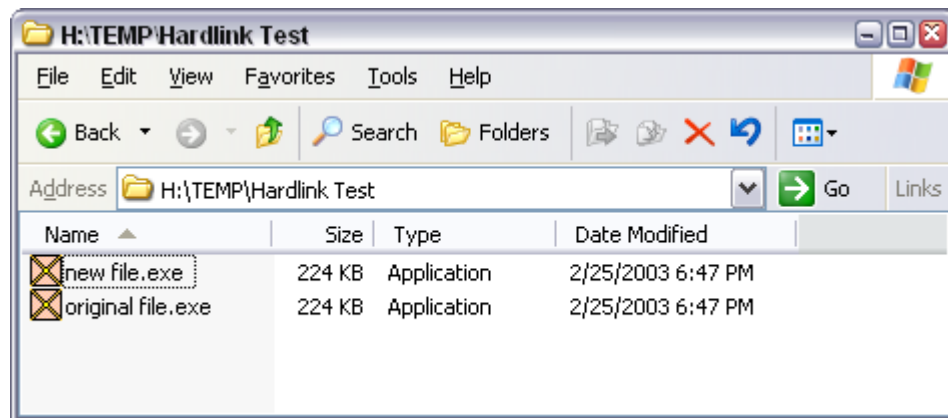
- Right-click any file
- Choose **Browse for hard link** in the context menu (shown below)



- Select the filename for the hardlink ("new file.exe" in the example below)



... and the new file name should appear a few seconds after you click "SAVE".

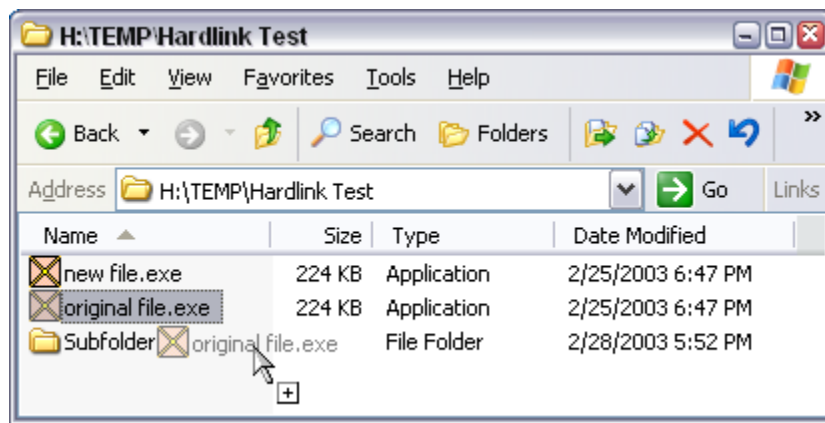


- Note how the hard link **new file.exe** has the same attributes (file size, date, ...) as the original file **original file.exe**.

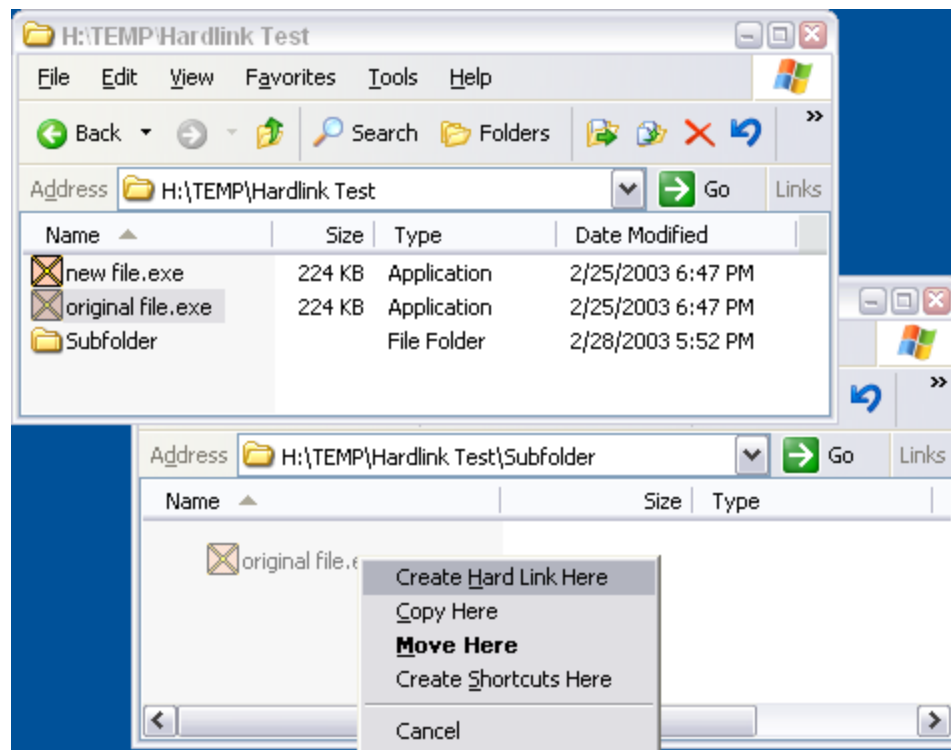
4.1.2.2 Drag & Drop

You can also create a hard link from the explorer by dragging and dropping a file. This can be useful to create multiple occurrences of one file, while only having to maintain one file.

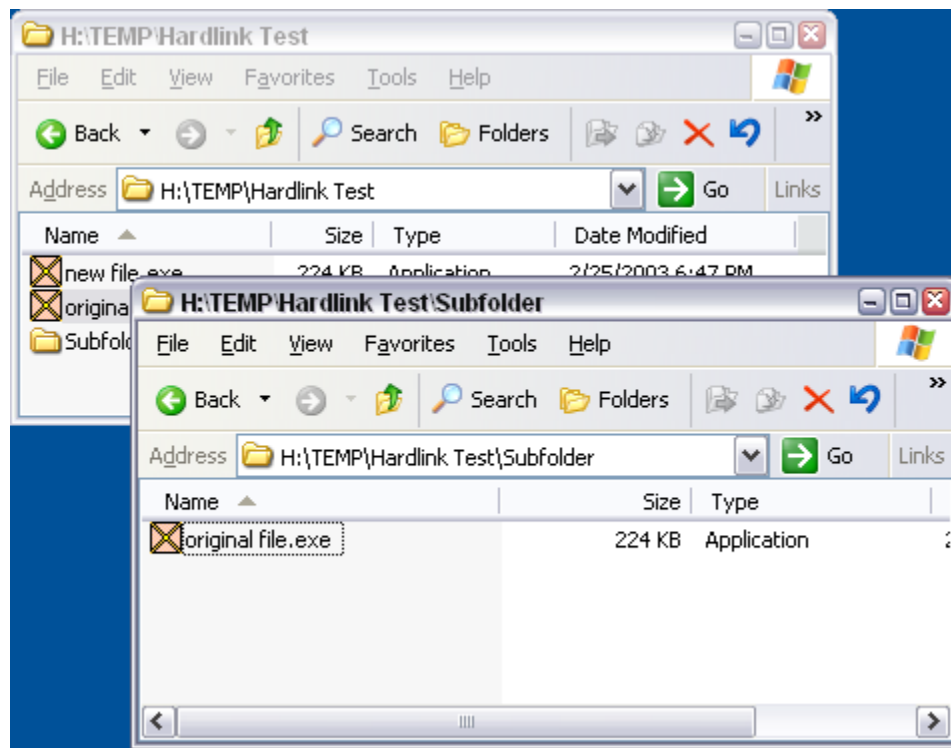
- Right-click any file, keep the right mouse button pressed and move the mouse. You should see a duplicate icon similar to the one shown below:



- You can now release the right mouse button either on a subfolder of the current folder or in a completely new folder:



When you created the hard link you will have an identical file in a different folder:



Remember that hard links can only be created on the same volume / drive letter, **H:** in the example shown above.

4.2 NetSend

NetSend is an application with a graphical user interface that allows you to send a text message to a remote Windows NT, Windows 2000 or Windows XP computer that is running the **Messenger** service (activated by default)

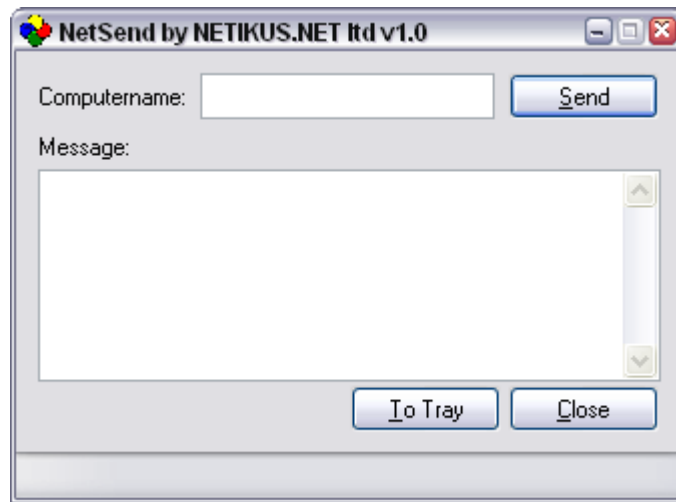
Traditionally you have to send network messages with the command line:

```
net send remote_computer message
```

NetSend minimizes to the system tray and is re-activated simply by double-clicking the icon.

Files

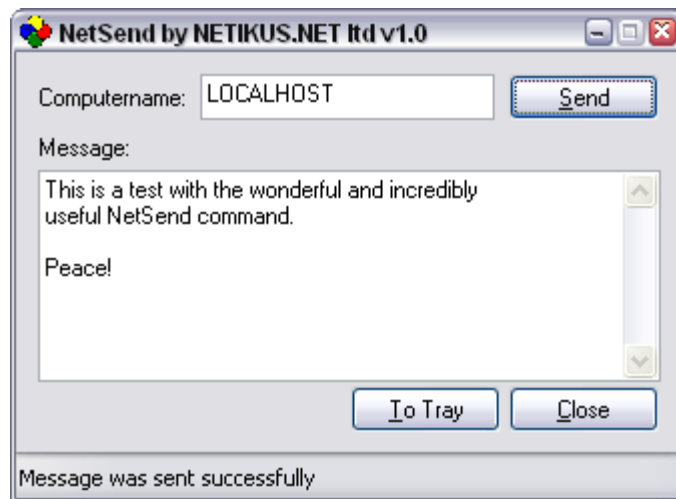
netsend.exe



Sample Screenshot

4.2.1 Usage

To send a message with NetSend launch the application and type the NetBIOS computer name into the **Computername** field and the actual message into the **Message** field.

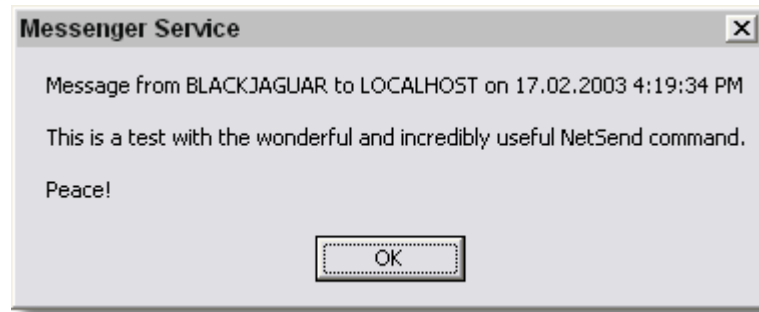


*If your computer is part of a Windows NT or Windows 2000 domain then you can also type in a **username** or **domain name**.*

To see if the message was sent successfully or not look at the status bar of the application

Message was sent successfully

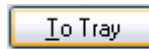
which indicates the success or failure of the operation. A sent message will look like this on the target computer:



4.2.2 Tray Icon

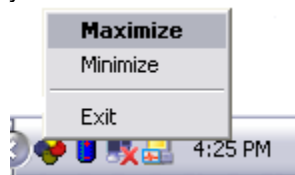
To minimize NetSend to the System Tray you can:

- Simply minimize NetSend
- Click on the **To Tray** button



- Enter ALT+T on the keyboard
- Right-Click the system tray icon and choose "Minimize" (see below)

NetSend will then sit in the systems tray:



To reactivate it:

- double-click the icon
- right-click the icon and choose "Maximize"

Clicking **Exit** will close NetSend.

4.3 Password Assistant

Password Assistant is a GUI application that lets you update passwords of user accounts on multiple Windows NT, Windows 2000 or Windows XP machines. A good example is updating the Administrator password on all of your networks workstations.

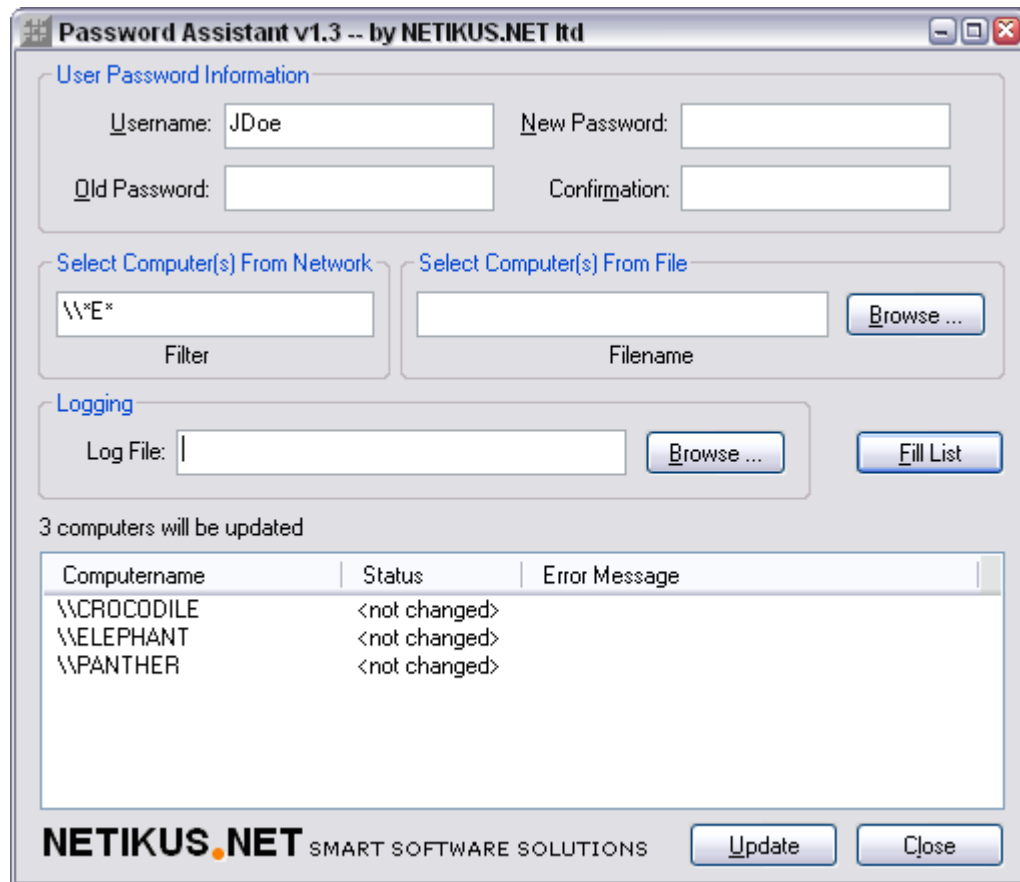
You can obtain computer names to update from the network neighbourhood (with a filter option) or from a text file. The update process can also be logged to a text file.



[AutoAdministrator](http://www.netikus.net) has the same functionality than Password Assistant, plus many more features such as manipulating remote registries, rebooting servers, controlling services and more. For more information on [AutoAdministrator](http://www.netikus.net) please visit our web site <http://www.netikus.net>.

Files

PasswordAssistant.exe

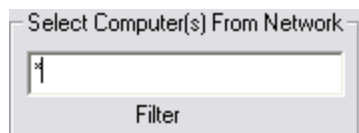


4.3.1 Usage

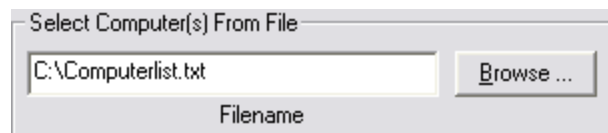
To update a password on multiple machines launch the application and specify the username whose password you would like to update, the current password, and the new password.



Then you need specify which computers to update. Either choose a **file** that contains one computername per row or enter a **wildcard** into the "Filter" field:



Specifying a filter



Getting computers from a text file

To log the password update process to a text log file, specify it here:



To fill the computer list now press the **Fill List** button and you should see a screen similar to the one shown below:

Computername	Status	Error Message
\\CROCODILE	<not changed>	
\\ELEPHANT	<not changed>	
\\WAKAL	<not changed>	
\\PANTHER	<not changed>	

To perform the update now press the **Change Now** button. If the update was successful then you will see an **OK** in the **Status** column:

Computername	Status	Error Message
\\CROCODILE	OK	
\\ELEPHANT	OK	
\\PANTHER	OK	

If the update is not successful then you will see **ERROR** in the **Status** column with the respective error message in the **Error Message** column:

Computername	Status	Error Message
\\CROCODILE	ERROR	The specified network password is not correct.
\\ELEPHANT	ERROR	The specified network password is not correct.
\\PANTHER	ERROR	The specified network password is not correct.

In the previous example above the password update was not successful because the current password for the user was incorrect.

4.3.2 Hints

Filter

You can use the "*" and "?" wildcard characters in the filter field. The asterisk stands for any character occurring zero or more times while the question mark stands for any character occurring one time only. The wildcard characters work just like they do in the Windows command line.

Note that computernames start with a \\, make sure you take this into consideration when typing your filter.

Updating Samba

It is possible to update user passwords on servers running Samba as well. This is not a feature of Password Assistant, instead Samba supports the standard Windows NT method of remotely changing a user password.

We had mixed results trying to change passwords on a Samba server, while it usually worked it sometimes would not.

4.3.3 Command Line Version

Password Assistant also has a command line version, the file is called **pwdupd.exe**. Please run **pwdupd.exe** without any parameters to see the syntax or take a look at the screenshot below.

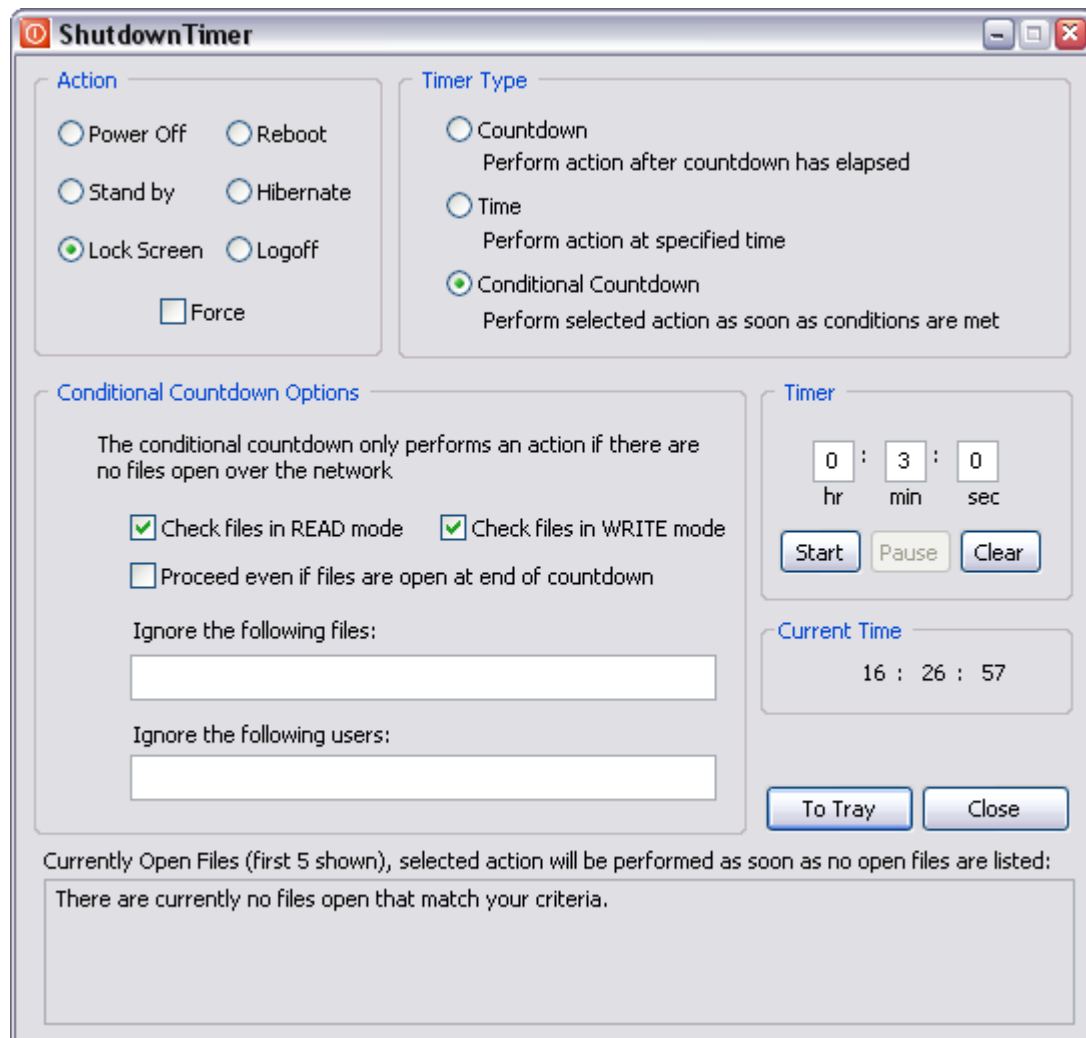
```
C:\ CMD
# pwdupd.exe
-----
PasswordAssistant V1.0 by NETIKUS.NET [ compiled on Mar  4 2003 ]
                        (support@netikus.net)
-----
Command-line utility to update passwords on multiple machines in batch mode.
Command-line syntax:
pwdupd <Username> <Old Pwd> <New Pwd> (/f or /n) (<filename> or <filter>)
Command-line options:
Username  The username whose password you want to change
Old Pwd   The current password of the user "username"
New Pwd   The new password of the user "username"
/f or /n  /f: take the computernames from a text-file (one entry per line)
          /n: take the computernames from the network neighborhood
filename  Full path to the file with the computernames
filter    A filter has to be specified, allowed filters are:
          *           All computers
          \\PC*       All computers starting with \\PC
          *NYC        All computers ending with NYC
          *server*    All computers containing "server"
          \\server12  Exact match
          FILTERS ARE NOT CASE SENSITIVE
Examples:
1. Change the password of the Administrator account on all computers where the
   computername starts with \\BOSPC from HoliGoli1 to xRfw8&dc!x :
pwdupd.exe Administrator HoliGoli1 xRfw8&dc!x /n \\BOSPC*
2. Change the password of the Support account on all computers where the
   computername contains SRV from 82765235 to JDduynb-s3 :
pwdupd.exe Support 82765235 JDduynb-s3 /n *SRV*
3. Change the password of the Administrator account on all computers that are
   listed in the file c:\computers.txt from unjnfuf to UjGrC54D :
pwdupd.exe Administrator unjnfuf UjGrC54D /f c:\computers.txt
Important note:
Password Assistant logs output to the console and also writes a logfile with the
name pwdupd.log to the directory where pwdupd was started from.
Password Assistant will display a list of matching computers and prompt you to
proceed if you choose the \n option.
#
```

4.4 ShutdownTimer

ShutdownTimer allows you to perform certain system actions either at a certain time or in a specified amount of time. The new conditional feature allows you to make the selected action based on whether certain files open over the network. See [Usage](#) for more information.

Examples

- Shut down your computer in 1 hour
- Logoff the current user in 10 minutes
- Hibernate the computer at 23:30:00
- Reboot a server at 4AM in the morning
- Reboot a server when no users have files open for WRITE access



Files

ShutdownTimer.exe

4.4.1 Usage

Selecting an Action

You can choose one of the following actions in the **What?** section:

- shut down (power off)
- reboot
- stand by (only Windows 2000+ and if supported)
- hibernate (only Windows 2000+ and if supported)
- logoff
- lock screen (only Windows 2000+)

Forcing applications to close: Check the **Force** checkbox to force applications to close when you perform a **Power Off**, **Reboot** or **Logoff** action. **Warning: Selecting this option might result in the loss of data if open applications contain unsaved data.**

Choosing the Timer Type

You can either perform the select action by using a countdown, by specifying the exact time or by selecting a conditional countdown.

Countdown:

Performs the selected action after the countdown has expired.

Time:

Performs the selected action at the specified time.

Conditional Countdown:

Performs the selected action **as soon as** no remote users have files open over the network on this machine (server). The selected action will be performed **immediately** if there are no files open at the time you click the START button. The specified timer (e.g. 3 hours) is basically the maximum period of time you are willing to wait for. While the countdown is running, ShutdownTimer will continuously enumerate all open files and only proceed with the selected action if there are no open files. ShutdownTimer will not do anything if the countdown has elapsed and there are still files open, **UNLESS** you check the "Proceed even if files are open at end of countdown" option.

For more information see [Conditional Countdown Options](#).

Starting the countdown

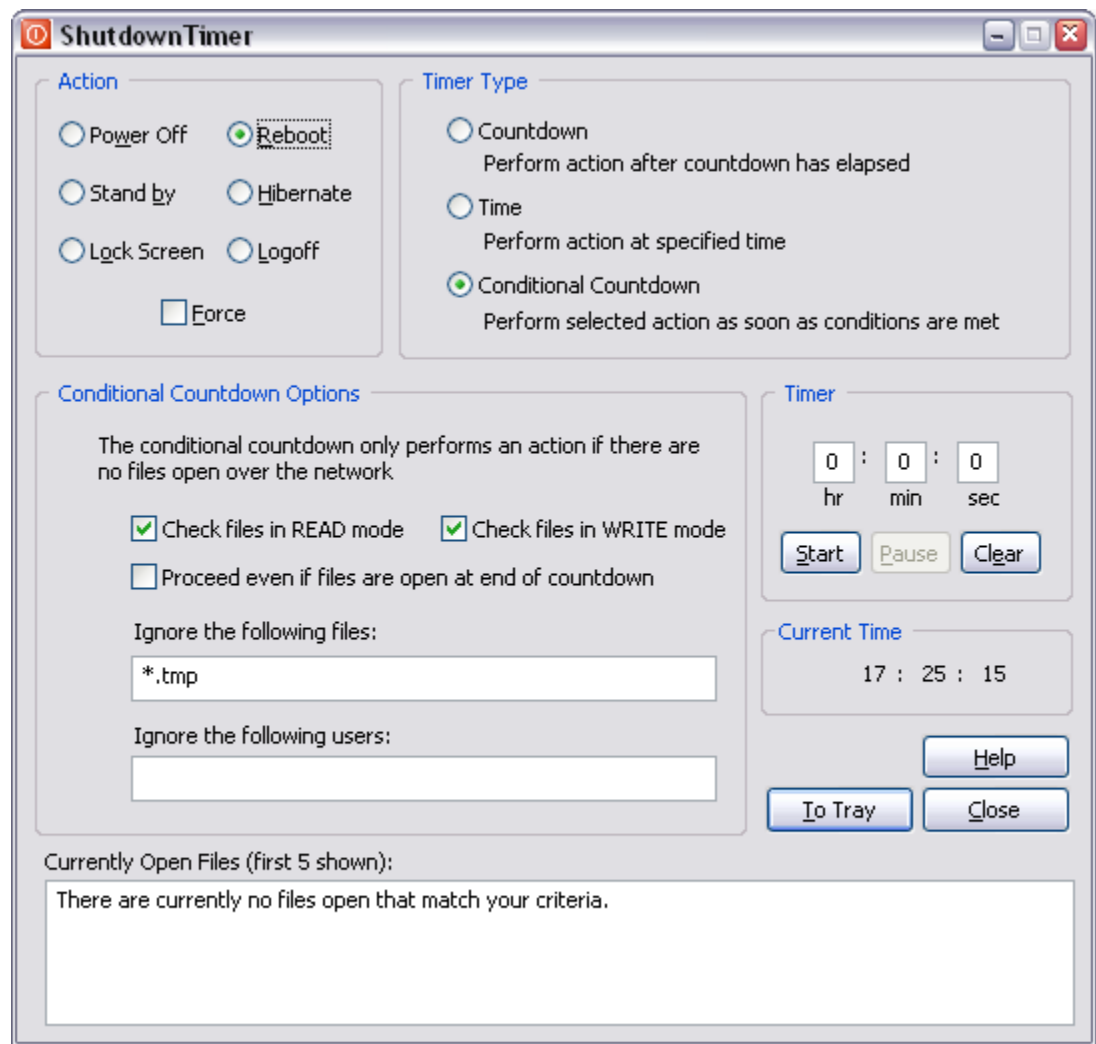
To start the countdown, enter the desired time interval / time in the **Timer** section and click on **Start**. You can pause the the countdown anytime by clicking the **Pause** button either in the dialog or in the context menu of the tray icon. To pause and clear the entered time press the **Clear** button.

Command Line Parameters

To start **ShutdownTimer** minimized (as a tray icon) execute

```
shutdowntimer.exe /hide
```

with the **/hide** command line parameter.



4.4.1.1 Conditional Countdown Options

The conditional countdown feature is useful when you need to restart a server, but need to wait until (almost) nobody has network files (office documents, databases, etc.) open on the server. Rather than checking the open files periodically, you can have ShutdownTimer do the work for you.

For example, to perform a conditional reboot when all files are closed over the network follow these steps:

1. Select the appropriate action, **Reboot** in this case. You may want to check **Force** as well.
2. Set the timer to the maximum amount you want ShutdownTimer to wait, for example **8 hours**.
3. Select the **Conditional Countdown** option, watch the "Currently Open Files" list.
4. Check either the READ, WRITE or both check boxes.
5. Exclude any files and/or users that can be ignored - ShutdownTimer will still proceed even those are open. For example, specify ***.tmp**.
6. Set the timeout period, for example 6 hours.
7. Click **Start**.

With the above settings, the server will be rebooted **as soon as** no files are open over the network, files ending in **.tmp** will not count. This means that a reboot might be triggered as early as one second,

or as late as 5 hours, 59 minutes and 59 seconds later. To reboot the server even when files are open at the end of the countdown, check the "**Proceed even if files are open at end of countdown**" checkbox.

Conditional Countdown Options

The following options are only available when selecting "Conditional Countdown" as the timer type. These options allow you to specify which open files ShutdownTimer should take into consideration during the countdown.

Check files in READ mode

Enumerate files that open for READ access. You will have to check either READ and/or WRITE access.

Check files in WRITE mode

Enumerate files that are open for WRITE access. You will have to check either READ and/or WRITE access.

Proceed even if files are open at the end of countdown

If there are still files open when the countdown has expired, then proceed with the selected action anyway.

Ignore the following files

You can ignore certain files by listing the file names or parts of the file names (use wildcards) here. For example, you can ignore all temporary and text files by specifying *.tmp, *.txt.

Ignore the following users

You can ignore files from one or more users by listing the user names, separated by comma. You can use wildcards with the usernames as well, e.g. *johndoe*.

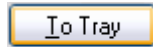
Currently Open Files

This field shows you the first five open files on your server and is updated every second. If you specified files and/or users to be ignored, then those files/users will not show up in this field.

4.4.2 Tray Icon

To minimize ShutdownTimer to the System Tray you can:

- Simply minimize ShutdownTimer
- Click on the **To Tray** button



- Enter ALT+T on the keyboard
- Right-Click the system tray icon and choose "Minimize"

To reactivate it:

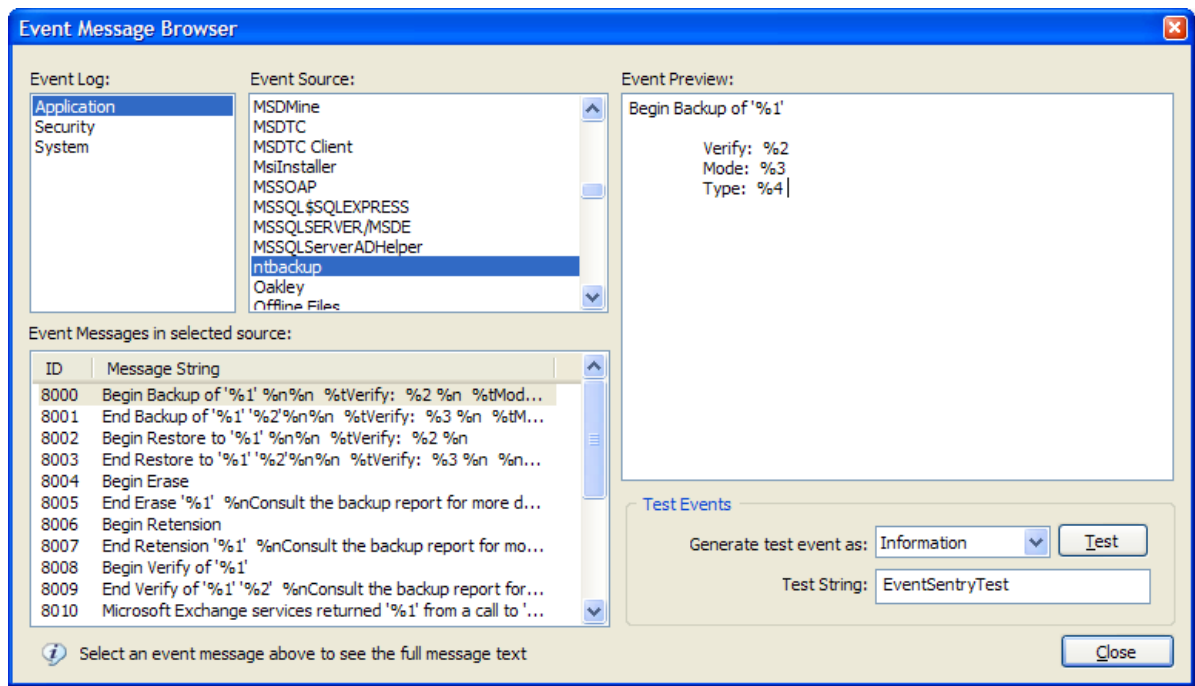
- double-click the icon
- right-click the icon and choose "Maximize"

Clicking **Exit** will close ShutdownTimer.

4.5 Event Message Browser

The Event Message Browser lets you review all the installed **Message DLLs** used by various system services and applications that log events to the event log. Additionally, you can also generate events to test any event log monitoring solutions (e.g. [EventSentry](#)) you have in place.

Please see the [Online EventSentry Documentation](#) for more information.



4.5.1 Usage

The main dialog is context sensitive, and you can start browsing by selecting an event log from the top left. Once you have selected an event log, select one of the associated event sources to see a list of all registered event messages. Click an event to see a full preview of it, you may also generate a test event if the event appears in the event preview.

Please see the [Online EventSentry Documentation](#) for more information.

5 Applications running as a Service

5.1 ServiceScheduler

ServiceScheduler is a scheduler service which controls (stops, starts, ...) services at specified times. It is independent from the Windows built-in scheduler service.

Example

For example, you can stop the SQL Server service every weekday at 2am in the morning, and start it again at 5am in the morning.

Files

servicescheduler.exe	service file, will be copied to %systemroot%\system32
servicescheduler.ini	configuration file, needs to be present in %systemroot%

Logging

ServiceScheduler logs its activity to the log file %systemroot%\servicescheduler.log. This behaviour cannot currently be disabled.

5.1.1 Installation

The ServiceScheduler service and files are automatically installed with the setup routine. To install the service manually, without the installer, follow these steps:

1. Copy the files **servicescheduler.exe** and **servicescheduler.ini** to the machine where you want to install the service. The configuration file **servicescheduler.ini** may be created from scratch.
2. Run `servicescheduler.exe /install` to create the service and have the file **servicescheduler.exe** copied to the `%SYSTEMROOT%\system32` directory.
3. Configure the service configuration file **servicescheduler.ini** (see next chapter on syntax)
4. Run `servicescheduler.exe /start` to start the service

5.1.2 Configuration

The ServiceScheduler service is configured with the configuration file **servicescheduler.ini** which has to be created in the `%SYSTEMROOT%` directory (usually `c:\winnt` or `c:\windows`).

Lines starting with a hash `#` or an exclamation mark `!` will be treated as comments and not interpreted. The syntax for the actual instructions is as follows:

```
[Service Name],[Service Action],[Time],[Mon.Tue.Wed...Sun]
```

Service Name The name of the service. This is **not** the display name of the service, but the real name of the service

Service Action The action you want to be taken. Actions include:

- start
- stop
- pause
- continue

Time The time at which the action should be performed. Note that the European time format is required, for example:

```
02:50  
11:35  
15:30  
21:00
```

Weekdays The weekdays on which the action should be performed. You may specify between one and seven weekdays. Weekdays include:

- Mon
- Tue
- Wed
- Thu
- Fri
- Sat
- Sun

Multiple weekdays have to be separated by a dot (`.`). Please see below for

configuration examples.



Important: You will need to stop and restart the ServiceScheduler service whenever you make changes to the configuration file **servicescheduler.ini**.

Configuration Examples

Example 1: Stop the EventSentry service weekdays at 10pm, and start the service again at 10:15pm

```
EventSentry,stop,22:00,Mon.Tue.Wed.Thu.Fri
EventSentry,start,22:15,Mon.Tue.Wed.Thu.Fri
```

Example 2: Stop the MS SQL Server service daily at 3am and restart it again at 5am

```
MSSQLServer,stop,03:00,Mon.Tue.Wed.Thu.Fri.Sat.Sun
MSSQLServer,start,05:00,Mon.Tue.Wed.Thu.Fri.Sat.Sun
```



If you only know the service **display name** but not the **service name**, then open **regedit.exe** and navigate to **HKLM\System\CurrentControlSet\Services** to determine the service name.

5.1.3 Security

When running ServiceScheduler in secure environments you can take the following steps to make ServiceScheduler more secure:

- Assign an account **other** than the SYSTEM account to the service. Make sure this account has the privileges to control the desired services.
- Make sure only authorized users can access the configuration file **%systemroot%\servicescheduler.ini**.

6 Credits

6.1 WinPcap

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
 Copyright (c) 2005 - 2008 CACE Technologies, Davis (California).
 All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.

This product includes software developed by Yen Yen Lim and North Dakota State University.

Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University"
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.
THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution. The name of Juniper Networks may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright 1989 by Carnegie Mellon.

Permission to use, copy, modify, and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Carnegie Mellon not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting

documentation that copying and distribution is by permission of Carnegie Mellon and Stanford University. Carnegie Mellon makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

7 Questions or Problems?

Questions

If you still have questions after reading this manual then please post a question in our support forums:

forums.netikus.net

and include the following information:

- The Operating System (incl. Service Pack Version) on which NTToolkit is running
- The version of NTToolkit
- Your question

Problems

If you are experiencing problems with NTToolkit then please visit our support forums:

forums.netikus.net

and include the following information:

- The Operating System (incl. Service Pack Version) on which NTToolkit is running
- The version of NTToolkit
- An exact description of the problem. Include information such as:
 - Does this problem occur on one or more installations?
 - Did it happen once or does it happen repeatedly?
- - What can we do to reproduce the problem?

8 Suggestions?

Nobody is perfect and neither is NTToolkit. We have implemented many features from customer suggestions in the past!

If you are missing a feature and would like to see it in a future release then please write to:

support@netikus.net

and include all or some of the following information:

- A description of the feature
- Why and how this feature would benefit you
- An example

After looking through your request we will get back to you and let you know if and when we will add your feature to NTToolkit.

9 Other Software from NETIKUS.NET

If you like our NTToolkit then you might want to check out our other software:

	Description	License
EventSentry	Event log, system and network monitoring software with many features	Commercial
EventSentry Light	Free version of EventSentry with limited functionality	Freeware
AutoAdministrator	Software to automate common tasks of Administrators	Commercial
Gateway IP Monitor	Monitor the IP address of your default gateway when using NAT	Freeware