

Table of Contents

Part I Welcome	4
Part II Requirements / Installation	4
Part III Database Tools	5
1 PostgreSQL Vacuum Utility	5
Usage	5
Part IV File System Tools	6
1 adslint	6
Usage	7
2 checksum	8
Usage	8
3 datahog	9
Usage	9
4 directorymonitor	10
Usage	10
5 directorysize	11
Usage	11
6 filereplace	11
Usage	12
7 purgetemp	12
Usage	12
8 superdelete	13
Usage	13
Part V Monitoring Tools	14
1 checkdb	14
Usage	14
Event Log Logging	16
2 checkurl	17
Usage	18
Event Log Logging	19
3 checktcp	20
Usage	20
4 listsuspended	21
Usage	21
5 perfquery	22
Usage	22
Part VI Network Tools	23
1 fping	23

Usage	24
2 gethttp	25
Usage	25
3 ipmon	27
Usage	29
4 IPMon+	30
Usage	31
Screenshots	32
5 MXQuery	34
Usage	34
6 ntpclient	35
Usage	35
7 pagesnpp	36
Usage	36
8 snmpinfo	36
Usage	37
9 wakeonlan	37
Usage	38

Part VII Security Tools 39

1 Password Assistant	39
Usage	40
Hints	42
2 servicesecure	42
Usage	42
Hints	43
Screenshots	44
3 tasksecure	45
Usage	45
4 Compliance Validator	46

Part VIII Windows Tools 48

1 Event Message Browser	48
Usage	48
2 isadmin	50
Usage	50
3 LogEvent	51
Usage	51
4 Logoff Delay	51
Usage	52
5 ProcessDmp	52
Usage	53
6 servicescheduler	53
Installation	53
Configuration	54
Security	55

7	sleep	56
	Usage	56
8	ShutdownTimer	56
	Usage	57
	Conditional Countdown Options.....	58
	Tray Icon	59
9	uptime	60
	Usage	60
10	EventSentray (Tray App)	60
11	SeriMon	62
	Usage	62
Part IX Credits		63
1	WinPcap	63
Part X Questions or Problems?		67
Part XI Suggestions?		67
Part XII Other Software from NETIKUS.NET		68
Index		0

1 Welcome

EVENTSENTRY EventSentry SysAdmin Tools v3.0

Thank you for using EventSentry SysAdmin Tools, we hope that the EventSentry SysAdmin Tools will improve and assist you with your server & network administration tasks!

The EventSentry SysAdmin Tools is a set of command-line and graphical utilities designed to help network administrators with various administrative tasks. The EventSentry SysAdmin Tools is freeware and constantly under development, and most of the tools found are spin-offs from [EventSentry](#), our Hybrid SIEM solution which monitors log, system health, inventory, network devices, NetFlow and Active Directory.

If you have any questions regarding EventSentry SysAdmin Tools then please contact us through our [support forums](#).

Your **NETIKUS.NET** team.

2 Requirements / Installation

Requirements

All EventSentry SysAdmin Tools applications require one of the following **64-bit** Windows Operating Systems (referred to as "Windows" through this document):

- Windows Server 2003 x64
- Windows XP x64
- Windows Vista x64
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows 7 x64
- Windows 8 or 8.1
- Windows Server 2012 (R2)
- Windows 10
- Windows Server 2016
- Windows Server 2019

Unix

Version 2.0 of the NTToolkit (legacy name) includes Unix versions for some of the included utilities, however the most recent version of the EventSentry SysAdmin Tools only support the above listed Windows-based platforms. The following Unix-based platforms are supported in v2.0:

- Linux
- FreeBSD 8.x
- OS X 10.5 & 10.6

The above platforms will be simply referred to as Linux, FreeBSD and OS X through this document.



Windows 2008 and later: Some of the executables require administrative access, 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").

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 Database Tools

3.1 PostgreSQL Vacuum Utility

Compresses files used by the specified table - using the built-in compression feature of Windows (NTFS) - prior to performing a full vacuum on the table, thus freeing up as much disk space as possible prior to the vacuum operation.

The compressed files will be automatically removed by the PostgreSQL database server after the full vacuum is complete and the table was re-created.

```

Connect      : OK
DB Type     : PostgreSQL
DB Version:  14.9
DB Dir      : D:/ESDB

Total Database Files Size: 8 GB

Compressing file(s) now ...

Compressed D:\ESDB\base\16384\204900 [1 GB][Progress: 12%]
Compressed D:\ESDB\base\16384\204900.1 [1 GB][Progress: 24%]
Compressed D:\ESDB\base\16384\204900.2 [1 GB][Progress: 37%]
Compressed D:\ESDB\base\16384\204900.3 [1 GB][Progress: 49%]
Compressed D:\ESDB\base\16384\204900.4 [1 GB][Progress: 61%]
Compressed D:\ESDB\base\16384\204900.5 [1 GB][Progress: 74%]
Compressed D:\ESDB\base\16384\204900.6 [1 GB][Progress: 86%]
Compressed D:\ESDB\base\16384\204900.7 [1 GB][Progress: 98%]
Compressed D:\ESDB\base\16384\204900.8 [95 MB][Progress: 100%]

Starting FULL VACUUM on table eventsentry.essyslogmain in 5 seconds .....

FULL VACUUM completed in 17 minutes and 21 seconds
Total disk space freed: 3 GB

```

3.1.1 Usage

Command Line Parameters

dbpgsql vacuum /u <USER> /p <PASS> /t <TABLE> /c /I <DSN|ConnectionString>

Argument	Description	Required	Default Value
----------	-------------	----------	---------------

/s <HOSTNAME IP>	Hostname or IP address to connect to	NO	172.0.0.1
/b <PORT>	TCP Port PostgreSQL server is listening on	NO	5432
/d <DATABASE>	Database where TABLE is located	YES	
/t <TABLE>	SQL table (including schema) to perform full vacuum on	YES	
/u <USERNAME>	Username to connect as	NO	postgres
/p <PASSWORD>	Password for USERNAME	YES	



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: Perform a full vacuum on the **eventsentry.eseventlogmain** table in the **EventSentry** database

```
dbpgsql vacuum / u post gres / p !$^&3j dk3 / d Event Sent ry / t
event sent ry. esevent logmai n
```

4 File System Tools

4.1 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 adslist.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.

Interface

Command-line

Files

adslist.exe

Supported Platforms

Windows

4.1.1 Usage

Command Line Parameters

adsl i st /s /q <DI RECTORY>

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
/p <filter>	Exclude paths that match <filter>, wildcards are supported



You can schedule **adsl i st.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
adsl i st %SYSTEMROOT% /s

Example 2: Look for the alternate data streams in the C:\Windows\System32, including sub directories, and use the quiet output
adsl i st C:\W ndows\Syst em32 /s /q

Example 3: Look for the alternate data streams on the entire C drive but exclude any path that contains **SYSVOL_DFSR\domain\DfsrPrivate\Staging**
adsl i st C:\W ndows\Syst em32 /s /p *SYSVOL_DFSR\ domai n\ Df sr Pri vat e\ St agi ng*

Sample Output

C:\>**adsl i st** C:\ /s

```
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
       ?Q30lsl dxJoudresxAaaqpcawXc
       {4c8cc155-6c1e-11d1-8e41-00c04f b9386d}
0005: C:\\Images\logo_v2_white.jpg
       ?Q30lsl dxJoudresxAaaqpcawXc
       {4c8cc155-6c1e-11d1-8e41-00c04f b9386d}
```

Summary:

=====

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

4.2 checksum

The **Checksum Generator** generates a one-way checksum of a file with a configurable algorithm (SHA256 by default) 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 (Integrity) Monitoring" feature which can automatically generate SHA 256 checksums.

To display and create a checksum of a file, simply supply the file name as the first argument. Please keep in mind that generating checksums of large files can take a significant amount of (CPU) time depending on the system where it's running.

This utility can also calculate the entropy (randomness) of a file and verify its digital signature.

A comparison checksum can be passed as a parameter to checksum.exe. If the actual file checksum does not match the comparison checksum, checksum.exe will set the return code (%ERRORLEVEL%) to 1, when it matches to 0.

Interface

Command-line

Files

checksum.exe

Supported Platforms

Windows

4.2.1 Usage

Command Line Parameters

```
checksum /s /a: ENTROPY| CRC32| MD5| SHA1| SHA256| SHA384| SHA512 <filename>
```

/a algorithm to use, can be one of the following (case sensitive): ENTROPY, CRC32, MD5, SHA1, SHA256, SHA384 or SHA512. Default is SHA256.

Note: Entropy is neither a cryptographic algorithm nor will it produce a checksum

/c comparison checksum, affects %ERRORLEVEL% (match=0, no match=1)

/e calculate the "Shannon" entropy of the specified file

/s Verify the digital signature of the file and display its digital signature information (if available)

/b Brief output, only displays checksum

/t Display/guess file type regardless of extension

filename path to the filename to generate the checksum from



The file entropy is only calculated for files with a file size of less than 512Mb .

Examples

Example 1: Create a SHA 512 checksum of file C:\Windows\notepad.exe


```
checksum /a:SHA512 c:\windows\notepad.exe
```

Example 2: Create a SHA 512 checksum and calculate the entropy of file C:\Windows\notepad.exe

```
checksum /e /a:SHA512 c:\windows\notepad.exe
```

4.3 datahog

DataHog is a command-line utility which analyzes all files and directories in a given path, usually a logical drive, to find the

- Largest sub directories, based on the file size
- Largest sub directories, based on the number of files
- Largest files (logical and/or physical size)

Note that datahog doesn't just find the largest top-level directories of the given path, it will use a unique algorithm to traverse the entire directory structure to find sub directories which are larger (or contain more files) than the other directories in the path.

Interface

Command-line

Files

datahog.exe

Supported Platforms

Windows (64-bit version available)

4.3.1 Usage

Command Line Parameters

```
datahog /fp /f /dc /d /l <max # of results> <path>
```

/fp	Find the largest files based on the physical file size
/f	Find the largest files (logical file size)
/dc	Find the largest sub directories (based on # of files contained)
/d	Find the largest sub directories (by size)
/l <max # of results>	Maximum number of results, 15 by default

Examples

Example 1: Find the largest 20 largest sub directories on the C drive

```
datahog /d /l 20 C:\
```

Example 2: Find the 10 largest files in the C:\Program Files directory

```
datahog /f /l 10 "C:\Program Files"
```

Example 3: Find the 10 sub directories which contain the largest number of files in the D:\ drive

```
datahog /dc /l 10 D:\
```

4.4 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.

Interface

Command-line

Files

dirmon.exe

Supported Platforms

Windows

4.4.1 Usage

Command Line Parameters

```
dirmon /d [path] /s (/i fileA.txt,fileB.txt,...) | (/e
fileA.txt,fileB.txt,...) <path>
```

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

```
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\_store8.dat
10/19/2007 13:37:26: ~MODIFIED      : Documents and Settings\All
Users\Application Data\Skype\Plugins\_store8.dat
```

7 filtered file transactions not shown.

4.5 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.

Interface

Command-line

Files

dirsize.exe

Supported Platforms

Windows

4.5.1 Usage

Command Line Parameters

`dirsize [path]`

Examples

Example 1: Display the size of the C:\Windows\System32 directory

`dirsize C:\Windows\System32`

Summary (took 0 seconds):

=====

Directories/Files searched: 954/9942

Logical directory size : 2,418,698,780 bytes

Physical directory size : 2,390,917,120 bytes

Average logical file size : 243,280 bytes

4.6 filereplace

FileReplace 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.

Interface

Command-line

Files

filereplace.exe

Supported Platforms

Windows

4.6.1 Usage**Command Line Parameters****filer replace** /t <directory> <file>

file	The original file the other files will be replaced with
directory	The directory to parse and look for files with the same file name as <file>
/t	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 sub folders) with **D:\Templates\default.php**

```
filer replace d:\data d:\templates\default.php
```

4.7 purgetemp

PurgeTemp traverses the default %TEMP% directory (or a manually specified directory) and deletes files which have not been modified for a specified amount of days (120 by default).

Purgetemp is designed to be called from login scripts to automatically keep users' temp folders small.

When called without arguments simply shows the configured temp directory, the number of files in the directory and their cumulative size:

```
Directory analyzed:  C: / Users / JOHNNY~1. PEA / AppData / Local / Temp
Total file size:    1.48 Gbytes
Total number of files: 1626
```

Interface

Command-line

Files

```
purgetemp.exe
QtCore4.dll
```

Supported Platforms

Windows

4.7.1 Usage**Command Line Parameters**

```
purgetemp /a <PATTERN> /d /r /s /l /t <days> /p <path>
```

/a <PATTERN>	Pattern which must be present in the %TEMP% environment variable
/d	Delete files, by default only lists statistics
/r	Delete files with read-only attribute set

/s	Delete files with system attribute set
/l	Delete hidden files
/t <days>	Delete files not modified in <days> days, 120 by default
/p <path>	Examine <path> path instead of %TEMP% directory

Examples

Example 1: Delete all files from the temp directory which have not been modified in 180 days:

```
pur get emp / d / t 180
```

Example 2: Delete all files from the C:\Temp directory which have not been modified in 2 months:

```
pur get emp / d / t 60 / p C:\Temp
```

4.8 superdelete

SuperDelete parses a directory (including subdirectories) and deletes multiple occurrences of one file.

Interface

Command-line

Files

superdel.exe

Supported Platforms

Windows

4.8.1 Usage

Command Line Parameters

```
super del /v /r /t <directory> <file to delete>
```

/v /verbose	Verbose - show which files would be deleted (requires /t)
/r /ro	Removes READ-ONLY attribute if set on file(s)
/t	Doesn't delete file(s) but instead shows each file which would be deleted

File to delete	The filename to delete
Directory	The directory to parse and delete occurrences of this file

Example

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

```
super del "c:\documents and settings" thumbs.db
```

5 Monitoring Tools

5.1 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.

CheckDB 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. Non-Windows platforms also need the respective ODBC framework (see "Prerequisites" below) installed.

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.

Interface

Command-line

Files

checkdb(.exe)

Prerequisites

OS X: iODBC

Linux / FreeBSD: unixODBC

Supported Platforms

Windows (64-bit version available)

Linux

FreeBSD

OS X

5.1.1 Usage

Command Line Parameters

checkdb /u <USER> /p <PASS> /q <SQLQUERY> /c /l <DSN|ConnectionString>

DSN or Connection String

/u <USERNAME>

/p <PASSWORD>

/q <SQLQUERY>

DSN or connection string to connect to

Username to connect as (**DSN only**)

Password for USERNAME (**DSN only**)

SQL query to execute upon successful connection

/c Log all output to console
/l 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 /u event sentry_web /p !$^&3j dk3 /c Event Sentry
```

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

```
checkdb /l "driver={SQL  
Server};server=mssqlserver;Network=DBMSSOCN;database=Event Sentry;uid=event s  
entry_svc;pwd=1234"
```

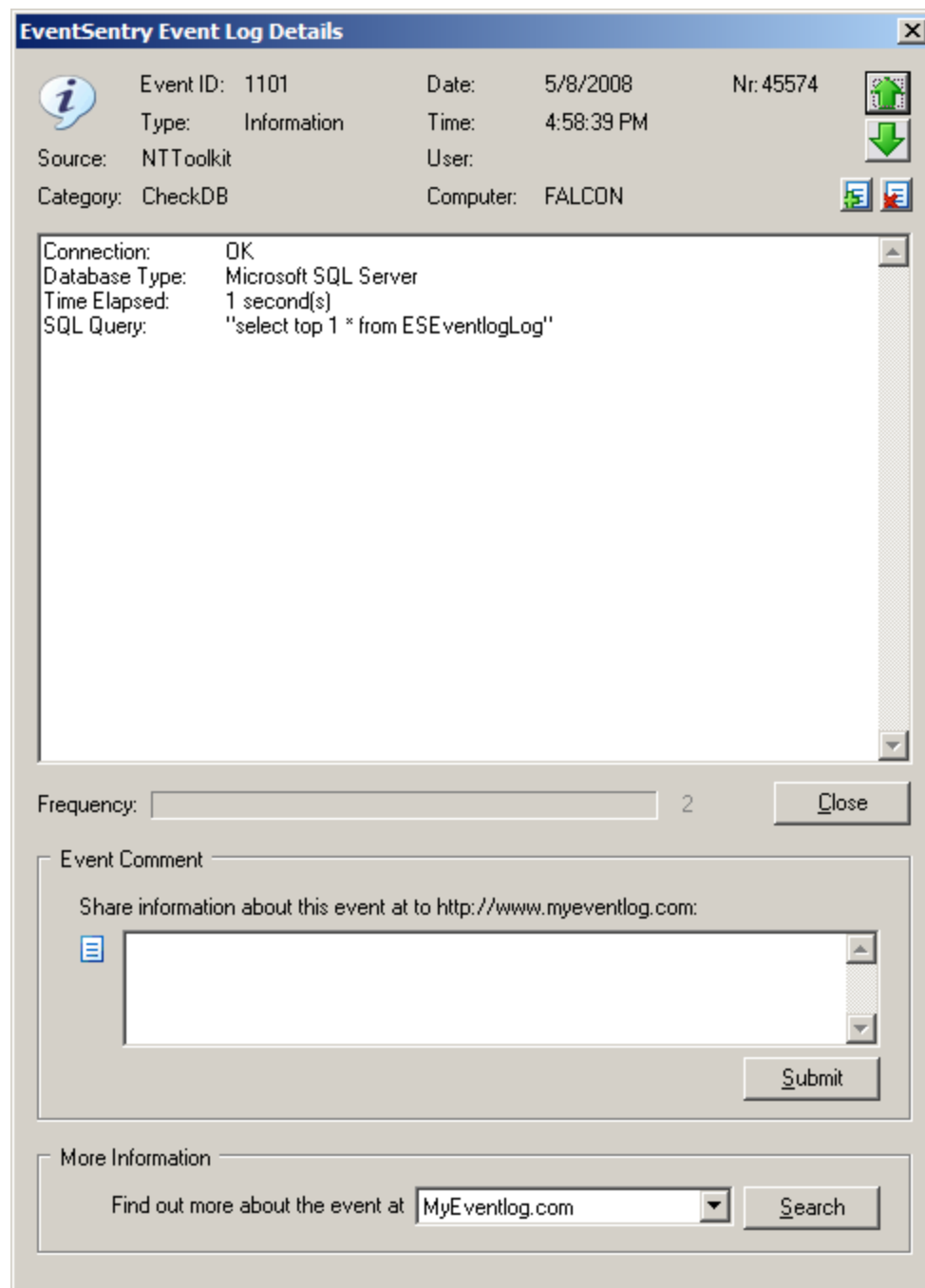
Example 3: Check whether the database defined in DSN **EventSentry** is available, verify that the table ESEventlogLog exists and log output to the console and event log

```
checkdb /u event sentry_web /p !$^&3j dk3 /q "select top 1 * from  
ESEventlogLog" /c /l Event Sentry
```

Sample Output

```
C:\>checkdb /u event sentry_web /p password /q "select top 1 * from  
ESEventlogLog" /c /l SQLSERVER
```

```
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

5.1.2 Event Log Logging

When specifying the `/le` option, CheckDB will log all actions to the event log with the event source **ESAdminTools** 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 Database Type: %1 Time Elapsed: %2
1101	Connection: OK Database Type: %1 Time Elapsed: %2 SQL Query: "%3"
1102	Connection: ERROR Reason: %1
1103	Connection: OK Database Type: %1 Time Elapsed: %2 SQL Query: "%3" -> ERROR Failure Reason: %4

5.2 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.

CheckURL can:

- verify that a web page exists and is accessible
- alert if a TLS certificate expires in fewer than X days
- 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
- login via a proxy login page

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.

Interface

Command-line

Files

checkurl.exe

Supported Platforms

Windows

5.2.1 Usage

Command Line Parameters

```
checkurl /auth <basic|digest|ntlm|kerberos> /u <USER> /p <PASS> /loginpage
<loginurl> /loginformdata <formdata for loginpage> /proxyhost
<proxyserver> /proxyport <proxy port> /proxyuser <proxy
user name> /proxypass <password for proxyuser> /checksum /checksums_clear /t
<TEXT> /lc /le /evt <OPTIONS> /certdays <DAYS> <URL>
```

/u MyUser	Authenticate as user MyUser to web page
/p "my pass"	Use specified password for /u option
/proxyhost	Host name or IP address of proxy server
/proxyport	IP port of proxy server
/proxyuser	Username for proxy server (if required)
/proxypass	Password for <proxyuser>
/loginpage <login page>	URL of page to login in prior to contacting URL
/loginformdata <form data>	Form data for "loginpage" in key value pairs (e.g. user=admin,pass=secret)
/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 (not case sensitive)
/certdays <days>	Alert if certificate it expires in <days> or fewer days, requires https URL
/certonly	Only performs certificate check and ignores errors related to authentication, requires /certdays
/f	Follow HTTP redirect (302) responses
/i	Ignore non-trusted certificates
/usewininet	Use built-in Windows (Internet Explorer) HTTP-engine
/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/downloads/version-history> changes:

```
checkurl /checksum /lc /le /evt
"CHECKSUM_CHANGE=Error,CHECKSUM_EQUAL=Ignore"
https://www.eventsentry.com/downloads/version-history
```

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" https://www.google.com/
```

Example 3: Log a warning to the event log when the string "Island Life" is not found in URL <https://www.dharmainitiative.com> and log results to the event log. Log in first via URL <https://www.dharmainitiative.com/login> with accepts the form elements "username" and "password":

```
checkurl /loginpage https://www.dharmainitiative.com/login /loginformdat a
"username=john@ocke.com,password=Iamlost" /t "Island Life" /le /evt
"TXT_FOUND=Information,TXT_NOTFOUND=Warning"
https://www.dharmainitiative.com/
```

Example 4: Connects to a HTTPS-enabled site to check a certificate, ignores any non-connection related errors such authentication

```
checkurl /certdays 60 /certonly https://myinternalsite.mycorp.com
```

5.2.2 Event Log Logging

When specifying the /le option, CheckURL will log all actions to the event log with the event source **ESAdminTools** 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
- CERTIFICATE The remote certificate expires

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.
1004	The TLS certificate for URL "%1" expires in %2 day(s), on "%3".

5.3 checktcp

CheckTCP determines whether a single or a range of TCP ports on a host are 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 uses multiple threads when scanning a range of ports for a fast port scan.

CheckTCP returns an **%ERRORLEVEL%** of 0 when the port is open and an **%ERRORLEVEL% > 0** when the port is not open.

Interface

Command-line

Files

checktcp.exe

Supported Platforms

Windows

5.3.1 Usage

Command Line Parameters

checkt cp /s /t:timeout <host name| i paddr ess> <port >

hostname / ipaddress	Hostname or IP address to connect to
port	TCP port on host to connect to. Specify a single port or a range of ports (e.g. 100-1000)
/s	Displays any data sent by the remote host through the TCP connection. Only supported when checking a single TCP port.
/t:timeout	Max amount of seconds to wait before interrupting a TCP port check (applies to TCP port checks only, default is 2 seconds)

Examples

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

```
checkt cp smtp.aol.com 25
```

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

```
checkt cp /s mail.hotmail.com 25
```

Example 3: List all ports in range 1000-5000 on server01

```
checkt cp server01 1000-5000
```

Sample Output

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

```
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
```

5.4 listsuspended

Lists any process which has at least one thread in a suspended state.

Interface

Command-line

Files

listsuspended.exe

Supported Platforms

Windows

5.4.1 Usage

Command Line Parameters

```
listsuspended /m /n:<number> /p /l
```

/p	Show PIDs only
/n:<count>	Repeat query <count> times
/l	Loop indefinitely, assumes /m
/m	Minimal output, only show counter value

Examples

Example 1: List all processes with suspended threads

```
listsuspended
```

```
Suspended processes found:
```

```
=====
explorer.exe (3604)
livecomm.exe (3776)
HELPMAN.EXE (4400)
```

```
Suspended processes: 3
```

Example 2: List processes with suspended threads, show PIDs with minimal output:

```
listsuspended /p /m
```

```
3604
3776
4400
```

5.5 perfquery

Queries a performance counter or SNMP OID and displays its current, minimum, maximum and average value.



When querying remote SNMP values, only **numerical** values are supported.

Interface

Command-line

Files

perfquery.exe

Supported Platforms

Windows, remote hosts with SNMP support

5.5.1 Usage

Command Line Parameters

perfquery /n:<count> /l /m <query path | oid>

<query path>	Performance counter to read, e.g. "Processor(_Total)\% Processor Time"
/n:<count>	Repeat query <count> times
/l	Loop indefinitely
/i:<seconds>	When looping, sleep <milliseconds> between iterations, default is 500ms
/m	Minimal output, only show counter value
/s	Query SNMP instead of a local performance counter
/f	Display values as floating point (windows performance counters only)
/host:<remote host>	Host name to send SNMP GET request to
/instance:<instance>	When returning table data through SNMP, specify the OID which describes each instance
/u:<community user>	SNMP v1/v2c community name or SNMP v3 user name
/a:<MD5 or SHA>	SNMP v3 authentication algorithm
/passauth:<password>	SNMP v3 authentication password
/c:<DES 3DES AES>	SNMP v3 encryption algorithm
/passcrypto:<password>	SNMP v3 encryption password

Examples

Example 1: Query performance counter "Processor(_Total)\% Processor Time" 5 times with regular output:

```
perfquery.exe "Processor(_Total)\% Processor Time" /n: 5
```

```
Processor(_Total)\% Processor Time: [_Total] now=8, min=0, max=8, avg=7.61
Processor(_Total)\% Processor Time: [_Total] now=1, min=1, max=1, avg=4.45
Processor(_Total)\% Processor Time: [_Total] now=1, min=1, max=1, avg=3.46
Processor(_Total)\% Processor Time: [_Total] now=8, min=1, max=8, avg=4.61
Processor(_Total)\% Processor Time: [_Total] now=1, min=1, max=8, avg=3.95
```

Summary

=====

Iterations: 5

Dur at i on: 3 seconds

Processor (_Tot al) \ % Processor Ti me: [_Tot al] mi n=1, max=8, avg=3.95

Example 2: Query CPU usage from SNMP host 192.168.10.1 with SNMP community "secret" 5 times, wait 250ms between each query

```
perfquery.exe /s /host:192.168.10.1 /u:secret
"1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0" /n:5 /i:250

1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0: now=1, mi n=0, max=1,
avg=1.00
1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0: now=0, mi n=0, max=0,
avg=0.67
1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0: now=0, mi n=0, max=0,
avg=0.50
1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0: now=0, mi n=0, max=0,
avg=0.40
1.3.6.1.4.1.2021.11.9.0+1.3.6.1.4.1.2021.11.10.0: now=0, mi n=0, max=0,
avg=0.33
```

6 Network Tools

6.1 fping

fping (Fast Ping) includes the following functionality:

- Ping (sends ICMP requests) remote host
- Attempt a TCP port connection at a remote host (to determine whether the remote host or service are up and running)
- Scan a subnet to find IPs that are online

fping is intended to be a replacement for the ping.exe utility that ships with Windows and offers the following benefits over the built-in ping.exe utility:

- Faster
- Supports TCP port checks
- Finds active IPs
- Supports specifying partial IP addresses when pinging hosts in a local subnet
- Audio support
- Additional output options
- Support for storing presets

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

Interface

Command-line

Files

fping.exe

Supported Platforms

Windows

6.1.1 Usage

Command Line Parameters

fping /count *packets* /size *packet size* /delay *delay* /loop <host name|ip|partial-ip|host nameWithPort|ipWithPort>

/a	Resolve IP addresses to host names
/u	Shows unhelpful comments when performing a brief ping
/b	Performs a quick ping and only indicates whether target host is up or down. Cannot be used with /verbose
/v	Verbose output (default)
/x	Clears all stored defaults
/w	Use current options as default
/f <1 2 3 4>	Play one of 4 built-in sounds on ping failure
/p <1 2 3 4>	Play one of 4 built-in sounds on ping success
/c <i>packets</i>	Sets the number of ICMP packets to send, default are 4
/s <i>packet size</i>	Sets the payload size of the ICMP packets in bytes, default are 32
/t <i>timeout</i>	Max amount of seconds to wait before interrupting a TCP port check (applies to TCP port checks only, default is 2 seconds)
/d <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
hostname ip CIDR *	The host to ping, CIDR format to scan an entire subnet or * to scan the current subnet.

To connect to a TCP port instead of using ICMP, append the port separated with a colon (e.g. myserver:445)

A partial IP address may be specified by skipping up to the first three octets; fping will try to guess the remainder of the IP address based on the current IP address and subnet mask.

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 /c 8 /s 64 www.eventsentry.com
```

Example 3: Continuously ping 10.10.0.1 and play sound if ping times out

```
fping /l /f 1 10.10.0.1
```

Example 3: Ping www.netikus.net with 2 packets, play sound on success, and use these options as a default for all future pings

```
fping /c 2 /p 2 /w www.netikus.net
```


Example 4: Check if port 80 is available on host www.netikus.net

```
f pi ng www . net i kus . net : 80
```

Example 5: Discover all IPs that are online in the 192.168.1.0/24 subnet

```
f pi ng 192 . 168 . 1 . 0 / 24
```

Example 6: Discover all IPs in the current subnet with an open port 80

```
f pi ng * : 80
```

Example 7: Find all IPs in the current subnet

```
f pi ng *
```

Example 8: Ping 192.168.1.1 (with the local IP address being 192.168.1.50/255.255.255.0)

```
f pi ng 1
```

Sample Output

```
c:\>f pi ng / c 2 / s 128 / d 300 www . event sent ry . com
```

```
Bi ngi ng www . event sent ry . com@16 . 92 . 10 . 83
```

```
Repl y f rom 216 . 92 . 10 . 83: by tes=128 ti me=15ms ttl =49 seq=0
```

```
Repl y f rom 216 . 92 . 10 . 83: by tes=128 ti me=17ms ttl =49 seq=0
```

```
Roundt ri p Summary:
```

```
Average: 16 ms, M ni mum 15 ms, Maxi mum 17 ms, Rat e: 100%
```

6.2 gethttp

GetHTTP retrieves files through the **HTTP** protocol. Please note that SSL is not currently supported.

Interface

Command-line

Files

gethttp.exe

Supported Platforms

Windows

6.2.1 Usage

Command Line Parameters

```
get ht t p / u <USER> / p <PASS> / proxyhost <proxyserver> / proxyport <proxy  
port> / proxyuser <proxy username> / proxypass <password for proxyuser> / i / q  
/ a / r / t <timeout> / f <filename>
```

```
/u MyUser
```

Authenticate as user MyUser to web page

/p "my pass"	Use specified password for /u option
/proxyhost	Host name or IP address of proxy server
/proxyport	IP port of proxy server
/proxyuser	Username for proxy server (if required)
/proxypass	Password for <proxyuser>
/I	Ignore SSL certificate warnings
/r	Resume transfer (if supported by remote host)
/t <timeout>	Connection timeout in seconds
/q	Quiet output
/a	Print HTTP headers
/d	Display content (instead of downloading)
/f <filename>	Store downloaded file in this local file



Existing local files will be overwritten without a prompt.

Examples

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

```
get http 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`

```
get http /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`

```
get http /f answer.html http://www.experts-exchange.com/Programming/System/Windows__Programming/MFC/Q_22133017.html
```

Example 4: Display the most recent measurement of the average concentration of carbon dioxide in the atmosphere

```
get http /d http://www.hqcasanova.com/co2/
```

Sample Outputs

```
>get http www.netikus.net/downloads/getconfig.sh
```

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

```
>get http /d http://www.hqcasanova.com/co2/
```

410.20 ppm

6.3 ipmon

IPMon 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 [192.168.8.100]

[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] [spc1-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.sbnindin.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]
[TCP] [216.92.199.161] [80->56628] [netikus.net]

```

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

Requirements[WinPcap network driver](#)**Interface**

Command-line

Files

ipmon(.exe)

Supported Platforms

Windows

Linux

FreeBSD
OS X

6.3.1 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.
- /u /udp** Capture UDP traffic (activated by default)
- /t /tcp** Capture TCP traffic (activated by default)
- /c /icmp** Capture ICMP traffic (**not** activated by default)
- /d PORT** Only include UDP/TCP packets that are sent to local port **PORT**
- /s PORT** Only include UDP/TCP packets that are sent from remote port **PORT**
- /l** List all available interfaces (always prompt)
- /g /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.
- /r /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

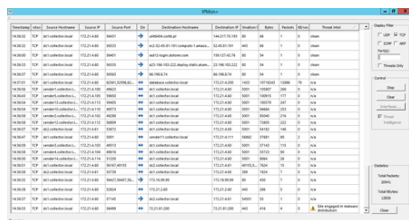
```
ipmon /udp /tcp /icmp /resolve
```

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
```

6.4 IPMon+

IPMon+ is the graphical version of IPMon, and also offers additional functionality not available in the command-line version. IPMon+ shows all TCP, UDP, ICMP and ARP connection endpoints between the local computer (default) and remote hosts, including the amount of data being transmitted, current transfer rate and threat intel. IPMon+ also supports promiscuous mode.



Source IP	Destination IP	Protocol	Status
192.168.1.1	192.168.1.2	TCP	Established
192.168.1.1	192.168.1.2	UDP	Established
192.168.1.1	192.168.1.2	ICMP	Established
192.168.1.1	192.168.1.2	ARP	Established

IPMon+ is primarily intended for:

- Troubleshooting network connections
- Revealing incoming and outgoing network traffic
- Discovering traffic to potentially malicious hosts

IPMon+ monitors all network traffic on the specified interface, and shows:

- which hosts communicate with the local host
- how much data is being transferred between IP connection
- the direction of traffic
- which UDP/TCP ports are used in the communication

If IPMon+ runs in promiscuous mode then traffic from hosts not involved with local traffic is displayed as well if the switch is configured to send all traffic.

More information:

- [Usage](#)
- [Screenshots](#)

Requirements

[Npcap packet sniffing library](#) (recommended) or [WinPcap network driver](#)



Since WinPcap is no longer under active development, it's recommended to install the Npcap driver instead.

When installing, make sure that **Install Npcap in WinPcap API-compatible Mode** is checked.

Interface

Graphical

Files

ipmonplus(.exe)

Supported Platforms

Windows

Linux (NTToolkit v2.0 only)

FreeBSD (NTToolkit v2.0 only)

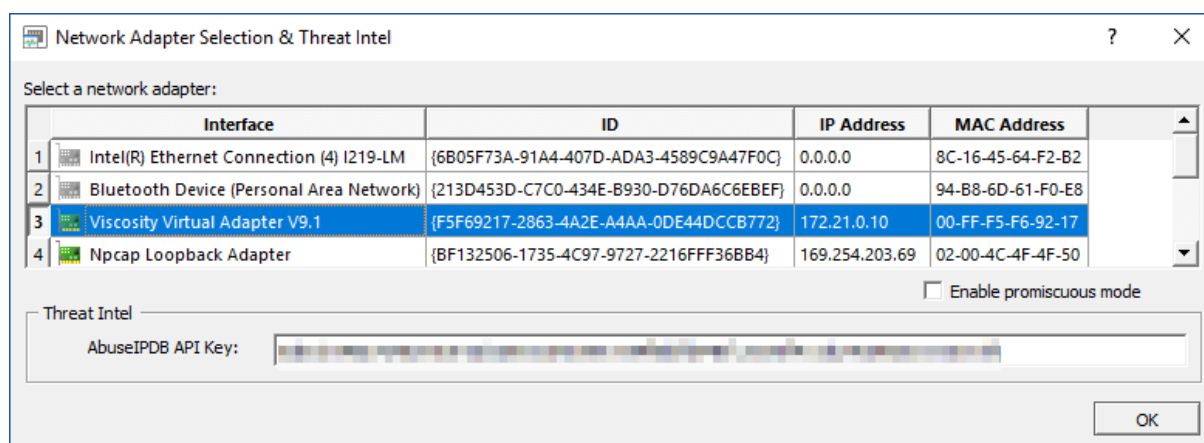
OS X (NTToolkit v2.0 only)

6.4.1 Usage

Capturing Traffic

To capture traffic, click the **Options** button and select the interface to capture traffic on. The first interface with a valid IP address will be selected by default. As such, you will only need to manually select an interface if the computer that you are capturing on has more than one network interface with a valid IP address.

The **Options** dialog also allows you to enable promiscuous mode, which ensures that all packets, even when not sent to the local MAC address, are captured and displayed. If the network card is connected to a switch, then the port to which the NIC is connected to will need to be configured to forward all network traffic to this port. Most managed switches support this functionality.

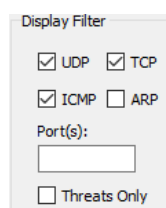


Once the correct interface is selected, clicking the **Start** button will start capturing traffic. Once clicked, the start button will be renamed to **Stop**. Click **Stop** to suspend capturing traffic. Clicking the **Stop** button will not automatically clear collected information. Clicking the **Clear** button will erase all collected information from the display.

Threat Intel

IPMon+ can provide threat intel on all processed IP addresses in real time utilizing the OTX black list along with supplemental threat details from [AbuseIPDB](#). Supplemental threat details are only available if an AbuseIPDB API key (free plan available as of 4/2019) is configured in the Options dialog. Checking the "Threat Intelligence" check box will enable the collection of threat intel, also checking the "Threats Only" check box will only display traffic with hosts that are deemed potentially malicious.

Filtering Traffic



By default, all UDP, TCP, ICMP, ARP traffic statistics are displayed in the main grid window. By toggling the check boxes next to a protocol name (e.g. TCP), all traffic matching this protocol will immediately be hidden. Toggling the check boxes will not affect traffic being captured, it will only filters information from the main grid. All UDP, TCP, ICMP, ARP traffic statistics are always captured, regardless of the display filter.

You can also filter traffic based on UDP/TCP ports. Simply enter the port number in the **Port(s)** field, and only traffic that was sent to or from those ports will be displayed. You can specify multiple ports by separating them with a comma (e.g. 80, 443).

Threats Only

Requires that "Threat Intelligence" is checked. Will only display traffic from hosts that are deemed potentially malicious.

Statistics

Displays how many network packets and total number of kbytes that have been captured. Changing the current filter has no effect on the statistics, which always show the overall total.

Sorting, Copy & Paste

Data in the grid can be sorted by clicking any of the column headers. Rows in the grid can be selected and copied to the clipboard by pressing the CTRL+C key combination.

6.4.2 Screenshots

Timestamp	Protocol	Source Hostname	Source IP	Source Port	Dir	Destination Hostname	Destination IP	Destination Port	Bytes	Packets	KB/sec	Threat Intel
14:36:32	TCP	dc1.collector.local	172.21.4.60	56431	→	uht6404.corb.pl	144.217.70.193	80	66	1	0	clean
14:36:32	TCP	dc1.collector.local	172.21.4.60	56533	→	ec2-52-45-81-191.compute-1.amazo...	52.45.81.191	443	66	1	0	clean
14:36:00	TCP	dc1.collector.local	172.21.4.60	56401	→	iad12-login.dotomi.com	159.127.42.76	80	54	1	0	clean
14:36:33	TCP	dc1.collector.local	172.21.4.60	56535	→	a23-196-183-222.deploy.static.akam...	23.196.183.222	80	54	1	0	clean
14:36:37	TCP	dc1.collector.local	172.21.4.60	56563	→	66.198.8.74	66.198.8.74	80	54	1	0	clean
14:37:01	TCP	dc1.collector.local	172.21.4.60	62561,52596,62...	↔	database.collector.local	172.21.4.200	1433	10718243	12886	79	n/a
14:36:56	TCP	sender1.collector.l...	172.21.4.100	49623	↔	dc1.collector.local	172.21.4.60	5001	105807	268	0	n/a
14:36:43	TCP	sender5.collector.l...	172.21.4.105	59650	↔	dc1.collector.local	172.21.4.60	5001	100915	177	0	n/a
14:36:54	TCP	sender13.collector.l...	172.21.4.113	59405	↔	dc1.collector.local	172.21.4.60	5001	100379	247	0	n/a
14:36:54	TCP	sender10.collector.l...	172.21.4.110	49573	↔	dc1.collector.local	172.21.4.60	5001	94664	253	0	n/a
14:36:58	TCP	sender2.collector.l...	172.21.4.102	49288	↔	dc1.collector.local	172.21.4.60	5001	85040	216	0	n/a
14:36:58	TCP	sender12.collector.l...	172.21.4.112	56809	↔	dc1.collector.local	172.21.4.60	5001	72605	222	0	n/a
14:36:57	TCP	dc2.collector.local	172.21.4.61	53672	↔	dc1.collector.local	172.21.4.60	5001	54182	146	0	n/a
14:36:47	TCP	dc1.collector.local	172.21.4.60	5001	↔	sender11.collector.local	172.21.4.111	56862	37681	80	2	n/a
14:36:59	TCP	sender3.collector.l...	172.21.4.103	49513	↔	dc1.collector.local	172.21.4.60	5001	37143	115	0	n/a
14:36:58	TCP	sender4.collector.l...	172.21.4.104	49616	↔	dc1.collector.local	172.21.4.60	5001	35723	90	0	n/a
14:36:50	TCP	sender14.collector.l...	172.21.4.114	51230	↔	dc1.collector.local	172.21.4.60	5001	8064	26	0	n/a
14:36:51	TCP	dc1.collector.local	172.21.4.60	56167,49155	↔	dc2.collector.local	172.21.4.61	49155,5...	7624	15	0	n/a
14:36:58	TCP	dc2.collector.local	172.21.4.61	55739	↔	dc1.collector.local	172.21.4.60	389	1824	7	0	n/a
14:36:32	TCP	dc1.collector.local	172.21.4.60	56427,56407,56...	→	172.16.99.99	172.16.99.99	80	450	7	0	n/a
14:36:38	TCP	dc1.collector.local	172.21.4.60	52824	↔	172.21.2.60	172.21.2.60	445	286	5	0	n/a
14:36:37	TCP	dc1.collector.local	172.21.4.60	57145	→	dc2.collector.local	172.21.4.61	54501	55	1	0	n/a
14:36:53	TCP	dc1.collector.local	172.21.4.60	56499	↔	72.21.81.200	72.21.81.200	443	416	4	0	Site engaged in malware distribution

Stopping ...

IPMon+ running on Windows Server 2012R2

IPMon+							
Timestamp	Protocol	Source IP	Source Port	Dir	Destination IP	Destination Port	Bytes
16:10:10	TCP	192.168.6.154	47850,47851,47853	↔	216.92.10.83	80	43672
16:10:01	TCP	192.168.6.154	60305	↔	74.125.113.100	80	10156
16:10:18	UDP	192.168.6.154	51717,55350,59875,50454...	↔	192.168.6.50	53	5517
16:10:15	TCP	192.168.6.154	40502,40501,40500,40497...	↔	64.34.80.163	443	2891
16:10:18	UDP	192.168.6.137	137	→	192.168.6.255	137	2852
16:10:18	ICMP	192.168.6.154	Echo Request	↔	66.39.154.155	Echo Reply	980
16:09:56	UDP	192.168.6.17	36979	→	192.168.6.255	3052	511
16:10:12	UDP	192.168.6.108	138	→	192.168.6.255	138	486
16:10:14	UDP	192.168.6.71	138	→	192.168.6.255	138	486
16:10:18	UDP	192.168.6.106	138	→	192.168.6.255	138	486
16:10:15	UDP	192.168.6.55	138	→	192.168.6.255	138	265
16:10:10	TCP	212.58.226.77	80	↔	192.168.6.154	48178	264
16:10:00	UDP	192.168.6.149	138	→	192.168.6.255	138	243
16:10:06	UDP	192.168.6.72	138	→	192.168.6.255	138	243
16:10:16	UDP	192.168.6.78	138	→	192.168.6.255	138	243
16:10:05	UDP	192.168.6.153	17500	→	255.255.255.255	17500	160
16:10:05	UDP	192.168.6.153	17500	→	192.168.6.255	17500	160

Display Filter

☒ UDP
☒ TCP
☒ ICMP
☒ ARP
☐ Resolve IPs

Port(s):

Control

Start

Clear

Interfaces ...

Statistics

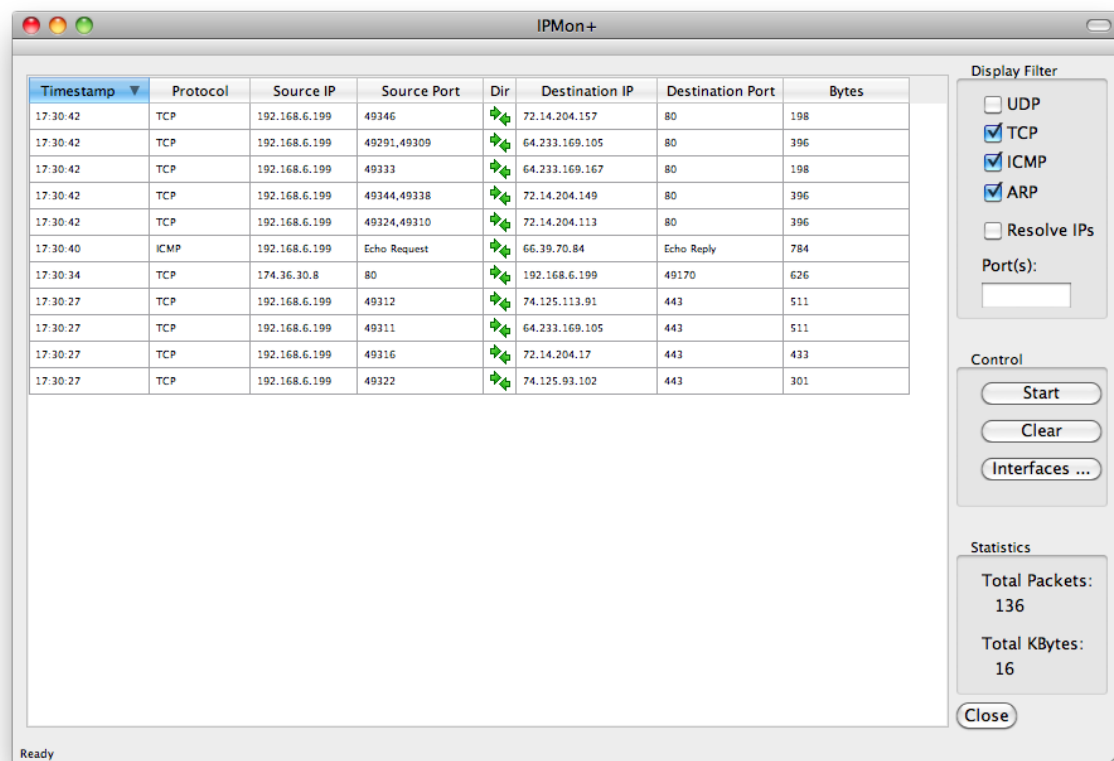
Total Packets:
932

Total KBytes:
451

Close

Ready

IPMon+ running on Ubuntu Linux (deprecated)



IPMon+ running on OS X 10.6 (deprecated)

6.5 MXQuery

MXQuery displays all MX records associated with a domain or email address, including the MX preference level. Simple only shows the first (best) mail server. MXQuery can also attempt to connect to port 25 of the mail server to verify that the SMTP service is reachable.

Interface

Command-line

Files

gethttp.exe

Supported Platforms

Windows

6.5.1 Usage

Command Line Parameters

```
mxquery /s /v <domain|email>
```

/s Simple mode, only returns the best mail server. Cannot be used with /v.
 /v Verifies connectivity by attempting to connect to port 25 of each mail server returned. Cannot be used with /s

Examples

Example 1: Return all mail servers registered for domain **netikus.net**

```
mxquery netikus.net
```

Example 2: Return only the best mail server for domain **bbc.co.uk**

```
mxquery /s bbc.co.uk
```

Example 3: Return all mail servers for domain **bbc.co.uk** and verify connectivity with each one

```
mxquery /v bbc.co.uk
```

6.6 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.

Interface

Command-line

Files

ntpclient.exe

Supported Platforms

Windows

6.6.1 Usage

Command Line Parameters

```
ntpcl i ent /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

```
ntpcl i ent t i me- a. ni st . gov
```

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

```
ntpcl i ent /set mydc. mydomai n. l ocal
```

6.7 pagesnpp

PageSNPP (SNPP stands for *Simple Network Paging Protocol*) 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.

Interface

Command-line

Files

pagesnpp.exe

Supported Platforms

Windows

6.7.1 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 use 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  
Event Sentry"
```

6.8 snmpinfo

Snmpinfo retrieves and displays a variety of information from a SNMP-enabled host. The information displayed depends on the data made available by the remote host and may include the following:

- System Information (e.g. Description, Operating System)
- CPU Usage
- Uptime
- Network Interfaces
- Disks (mount points)
- Running processes
- Virtual Machines (VMWare ESXi)

- Switch port mappings

The type of information retrieved reflects the data utilized by EventSentry, more data will likely be added over time.

Interface

Command-line

Files

snmpinfo.exe

Supported Platforms

Windows

6.8.1 Usage

Command Line Parameters

```
snmpinfo /u public <host>
```

<host>	Host name or IP address of host to query
/u <community user>	SNMP v1/v2c community name or SNMP v3 user name
/a <MD5 or SHA>	SNMP v3 authentication algorithm
/passauth <password>	SNMP v3 authentication password
/c <DES 3DES AES>	SNMP v3 encryption algorithm
/passcrypto <password>	SNMP v3 encryption password
/e <EngineID>	SNMP v3 EngineID
/co <Context Name>	SNMP v3 Context Name
/coeid <Context EngineID>	SNMP v3 Context Engine ID

Examples

Example 1: Retrieve all available SNMP information from host webserver1.plasticoceans.org

```
snmpinfo.exe webserver1.plasticoceans.org
```

6.9 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.

if a router supports direct broadcasts, magic packets can also be sent to a router.

Interface

Command-line

Files

wakeonlan.exe

Supported Platforms

Windows

6.9.1 Usage

Command Line Parameters

`wakeonlan /i <ip-address> <mac-address>`

`/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.

`mac address` The MAC address of the NIC that is to be woken up

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

7 Security Tools

7.1 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](#) has the same functionality than Password Assistant, plus many more features such as manipulating the remote registry, rebooting servers, controlling services and more.

Password Assistant v1.3 -- by NETIKUS.NET Ltd

User Password Information

Username: JonDoeTheThird New Password: [masked]

Old Password: [masked] Confirmation: [masked]

Select Computer(s) From Network

Filter: [empty]

Select Computer(s) From File

Filename: P:\temp\computers.txt Browse ...

Logging

Log File: [empty] Browse ... Fill List

4 computers will be updated

Computename	Status	Error Message
member_srv_1	<not changed>	
member_srv_2	<not changed>	
member_srv_3	<not changed>	
member_srv_4	<not changed>	

Update Close

Interface

Graphical

Files

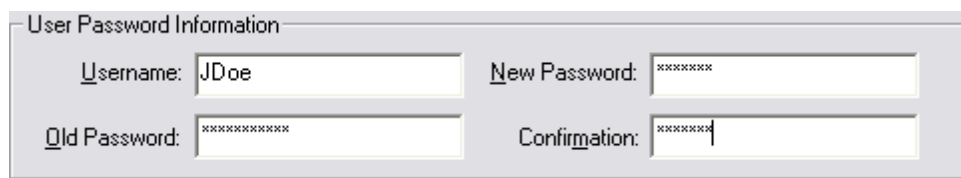
PasswordAssistant.exe

Supported Platforms

Windows

7.1.1 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.

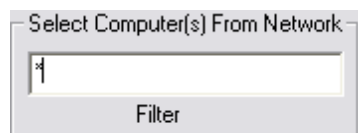


User Password Information

Username: JDoe New Password: [masked]

Old Password: [masked] Confirmation: [masked]

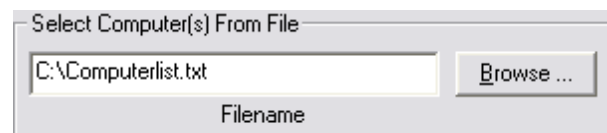
Then you need specify which computers to update. Either choose a **file** that contains one computername per row or enter a **wildcard** into the "Filter" field:



Select Computer(s) From Network

Filter: [1]

Specifying a filter



Select Computer(s) From File

Filename: C:\Computerlist.txt Browse ...

Getting computers from a text file

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



Logging

Log File: C:\test.log Browse ...

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.

7.1.2 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.

7.2 servicesecure

ServiceSecure resets 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).

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

Interface

Command-line

Files

svsec.exe

Supported Platforms

Windows

7.2.1 Usage

Command Line Parameters

svsec /r /c /u <user name> /p <password> <host name>

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

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

/u <username> List only services running under the specified **username**

/p <password> Set the password to **password**. Only valid in conjunction with **username**.

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

`/r /restart` Restart running service(s) after the password has been changed. Only valid in conjunction with the `/u` and `/p` options.

Examples

Example 1: Enumerate all services on host `\\server1`

```
srvsec \\server1
```

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

```
srvsec /u DOMAIN Administrator \\fileserver
```

Example 3: Change the service password of all services that are using the **DOMAINSrvAcc** username to `yUye$#34ww:`

```
srvsec /u DOMAIN SrvAcc /p 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 /u .User1 /p blaUip432 /r \\dbserver1
```

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 /u wupdup /p blaUip432 /c /r \\dbserver1
```

7.2.2 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 `"DOMAINUser1"`.

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.

7.2.3 Screenshots

```

Administrator: Command Prompt

[Security Accounts Manager]
[Server]
[Service Scheduler]
[Shell Hardware Detection]
[Smart Card Removal Policy]
[Special Administration Console Helper]
[System Event Notification Service]
[Task Scheduler]
[User Profile Service]
[Virtual Disk]
[Visual Studio 10 Remote Debugger]
[Volume Shadow Copy]
[Windows Audio Endpoint Builder]
[Windows CardSpace]
[Windows Driver Foundation - User-mode Driver Framework]
[Windows Error Reporting Service]
[Windows Installer]
[Windows Management Instrumentation]
[Windows Modules Installer]
[Windows Update]
[Wired AutoConfig]
[WMI Performance Adapter]

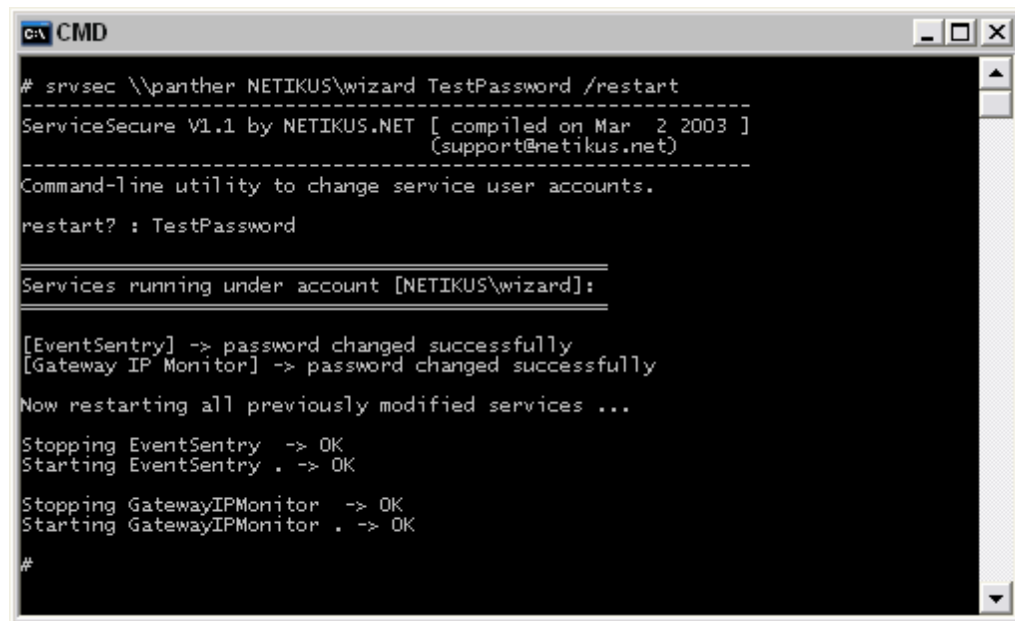
=====
Services running under account [nt authority\localservice]:
=====

[Application Identity]
[Application Layer Gateway Service]
[Base Filtering Engine]
[COM+ Event System]
[DHCP Client]
[Diagnostic Policy Service]
[Diagnostic Service Host]
[Function Discovery Provider Host]
[Function Discovery Resource Publication]
[Hyper-V Data Exchange Service]
[Hyper-V Time Synchronization Service]
[Link-Layer Topology Discovery Mapper]
[Microsoft Fibre Channel Platform Registration Service]
[Net.Pipe Listener Adapter]
[Net.Tcp Listener Adapter]
[Net.Tcp Port Sharing Service]
[Network List Service]
[Network Store Interface Service]
[Performance Counter DLL Host]
[Performance Logs & Alerts]
[Remote Access Quarantine Agent]
[Remote Registry]
[Secure Socket Tunneling Protocol Service]
[Smart Card]
[SNMP Trap]
[SPP Notification Service]
[SSDP Discovery]
[TCP/IP NetBIOS Helper]
[Thread Ordering Server]
[TPM Base Services]
[UPnP Device Host]
[Windows Audio]
[Windows Color System]
[Windows Event Log]
[Windows Firewall]
[Windows Font Cache Service]
[Windows Presentation Foundation Font Cache 3.0.0.0]
[Windows Time]
[WinHTTP Web Proxy Auto-Discovery Service]

=====
Services running under account [nt authority\networkservice]:
=====

[ASP.NET State Service]

```



```
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

#
```

7.3 tasksecure

TaskSecure resets 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.

TaskSecure can 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.

Interface

Command-line

Files

tasksec.exe

Supported Platforms

Windows

7.3.1 Usage

Command Line Parameters

tasksecure /a /u <user name> /p <password> /s <\\host name>

<without options> enumerates all scheduled tasks, grouped by account username

/s <\\hostname> Perform all actions on host "**servername**"

/u /username List only scheduled tasks running under the specified **username**

/p /password For all tasks running under <username> set the password to **password**.
Requires /u

Examples

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

```
tasksecure /s \\server1
```

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

```
tasksecure /u DOMAIN Administrator /s \\fileserver
```

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

```
tasksecure /u DOMAIN SrvAcc /p yUye$#34ww.
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tasksecure

LOCAL SERVICE
=====
Microsoft\Windows\Autochk\Proxy [Ready] [4/10/2014 3:35:40 AM]
Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask [Ready] [4/17/2014 3:30:00 AM]
Microsoft\Windows\Customer Experience Improvement Program\UsbCeip [Ready] [4/21/2014 1:30:00 AM]
Microsoft\Windows\RAC\RacTask [Ready] []
Microsoft\Windows\Ras\MobilityManager [Ready] []
Microsoft\Windows\Time Synchronization\SynchronizeTime [Ready] [4/20/2014 1:00:00 AM]
N/A
====
Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Manual) [Ready] []
Microsoft\Windows\CertificateServicesClient\UserTask [Ready] [4/21/2014 5:42:01 PM]
Microsoft\Windows\MemoryDiagnostic\CorruptionDetector [Ready] []
Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector [Ready] []
Microsoft\Windows\NetTrace\GatherNetworkInfo [Ready] []
Microsoft\Windows\Server Manager\ServerManager [Ready] [4/21/2014 5:41:59 PM]
Microsoft\Windows\Task Manager\Interactive [Ready] []
Microsoft\Windows\Tcpip\IpAddressConflict1 [Ready] []
Microsoft\Windows\Tcpip\IpAddressConflict2 [Ready] []
Microsoft\Windows\TextServicesFramework\MsCtfMonitor [Running] [4/21/2014 5:41:59 PM]
Microsoft\Windows\WMI\ResolutionHost [Ready] [4/21/2014 5:55:00 PM]
Microsoft\Windows\Windows Error Reporting\QueueReporting [Ready] [4/21/2014 5:55:00 PM]
Microsoft\Windows\Wininet\CacheTask [Running] [4/21/2014 5:41:59 PM]
SYSTEM
=====
Microsoft\Windows\Application Experience\AitAgent [Ready] [4/21/2014 2:30:00 AM]
Microsoft\Windows\Application Experience\ProgramDataUpdater [Ready] [4/21/2014 12:30:00 AM]
Microsoft\Windows\CertificateServicesClient\SystemTask [Ready] [4/21/2014 11:06:26 AM]
Microsoft\Windows\Customer Experience Improvement Program\Consolidator [Ready] [4/21/2014 1:00:00 AM]
Microsoft\Windows\Customer Experience Improvement Program\Server\ServerCeipAssistant [Ready] [4/20/2014 5:22:47 PM]
Microsoft\Windows\Customer Experience Improvement Program\Server\ServerRoleCollector [Ready] [4/17/2014 12:47:53 AM]
Microsoft\Windows\Customer Experience Improvement Program\Server\ServerRoleUsageCollector [Ready] [4/21/2014 1:23:10 PM]
Microsoft\Windows\Defrag\ScheduledDefrag [Ready] []
Microsoft\Windows\MUI\LPmpv [Ready] [4/10/2014 3:30:39 AM]
Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem [Ready] [4/15/2014 9:07:23 AM]
Microsoft\Windows\Registry\RegIdleBackup [Ready] [4/19/2014 12:39:17 AM]
Microsoft\Windows\UPnP\UPnPHostConfig [Ready] []
Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange [Ready] []
TESTGROUND\WIZARD
=====
Task with Error [Ready] [12/20/2013 6:42:52 PM]
[41 tasks configured, 33 displayed]
```

7.4 Compliance Validator

A graphical utility which utilizes [EventSentry's validation scripts](#) to compare security (and other) settings of the local host with best practices, security frameworks and compliance requirements such as NIST, STIG, CMMC and many more.



[EventSentry](#) can continuously evaluate all applicable validation scripts on your entire network infrastructure - automatically in the background. Extensive reporting capabilities show results in seconds, and ensure that the entire network is in compliance.

Usage

The status bar (bottom left) will show the number of available scripts, tags and the release date of the validation scripts. Click the "Tags" button to display the list of available tags. Select one or more tags and click the "Run" button to start the verification. Individual checks can be skipped by clearing the check box. Results can be exported to a text file using the "Export" button.

Tags

To select a single tag, simply double-click the tag. Use either the CTRL or SHIFT buttons to select multiple tags and then click OK. Click the "X" button to clear the selected tags and display the scripts stats in the status bar. Tags are stored in the registry when the application is closed, and restored when the application is re-opened.

Results

Clicking the "Run" button will start the evaluation process, by launching each listed (and checked) scripts sequentially. Each script has 4 possible statuses:

- PASS
- FAIL
- WARNING
- N/A

PASS: Indicates that the test was successful and the system passed the check.

FAIL: Indicates that the current (security) settings on the host did not pass the check.

WARNING: Indicates that the test was successful and the system passed the check, but that additional steps may be necessary for full compliance.

N/A: Indicates that the check is not applicable to the local host, e.g. if the local system is a workstation but the check is for domain controllers.

The result of the check is displayed in the "Status" column and also indicated in the icon on the left side. Clicking a respective row will display details about the validation script status on the bottom of the dialog. To learn more about the check, including how to resolve a failure, either double-click the row or click the "More Information" button.

The status bar will show how many checks were successful and how many failed in the status bar, along with the overall duration of checks so far.

Export

Clicking the "Export" button will export the results to a text file, similar to the text shown below:

```
Time,Hostname,ID,Status,Executed,Errorlevel,Duration(s),Description
2023-10-31 20:04:27,somehost.somedomain.local,b505fc16-70d3-4275-bcc5-02fac2fdb3af,FAIL,OK,1,0,Acc
2023-10-31 20:04:29,somehost.somedomain.local,3f0d630e-d744-450e-8e8a-6478118649fb,PASS,OK,0,0,Exp
2023-10-31 20:04:30,somehost.somedomain.local,bf06c136-7223-41ac-8288-e0940126a884,FAIL,OK,1,0,Ger
2023-10-31 20:04:31,somehost.somedomain.local,20a8c861-e142-4e51-bf82-b0ef8bd1343c,PASS,OK,0,0,Ren
```

Interface

Graphical

Files

ComplianceValidator.exe

Supported Platforms

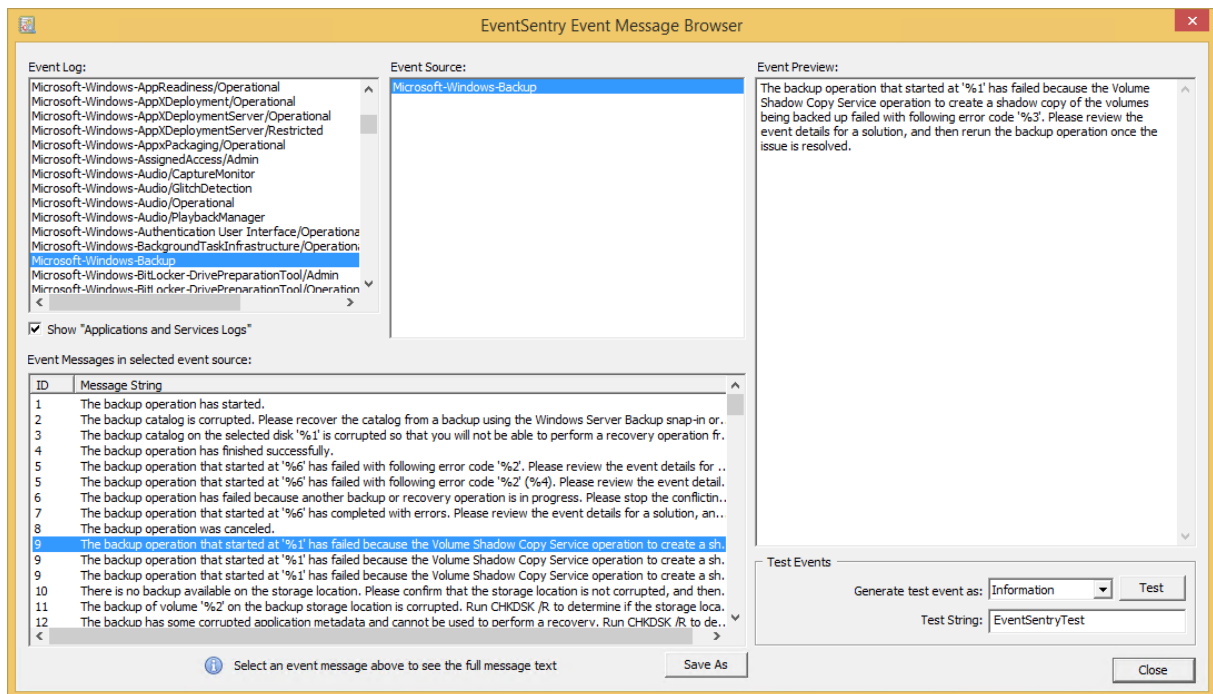
Windows

8 Windows Tools

8.1 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.



Interface

Graphical

Files

EventMessageBrowser.exe

Supported Platforms

Windows

8.1.1 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.

8.2 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.

Interface

Command-line

Files

isadmin.exe

Supported Platforms

Windows

8.2.1 Usage

Command Line Parameters

When executing isAdmin, either batch mode (/b) or debug mode (/d) always need to be specified.

i s a d m i n / b | d / e / f / u <user name>

/b /Batchmode	Batch-mode, only outputs TRUE or FALSE. Cannot be used with /d
/d /Debugmode	Debug-mode, logs additional output. Cannot be used with /b
/e /uac	Only outputs "TRUE" if app is running inside an elevated shell (use with /b)
/f /ForceDomain	Always check the domain's Administrators group (instead of local Administrators group)
/q /NoQuickCheck	Disables a quick check which evaluates the security token of the current process instead of enumerating security groups. Quick check only works if the process is elevated.
<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.

Examples

Example 1: Check if user "john.doe" is a local Administrator
i s a d m i n / b / u j o h n . d o e

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

```
i sadmin /f /d
```

Example 3: Output "TRUE" if isadmin.exe is running inside an elevated shell

```
i sadmin /b /uac
```

8.3 LogEvent

LogEvent writes an event from the specified event source and event id to the application event log.

Interface

Command-line

Files

logevent.exe

Supported Platforms

Windows

8.3.1 Usage

Command Line Parameters

```
logevent /s <eventsourc> /i eventid /c <eventcategory> /<logInformation|logWarning|logError> insertionString1 insertionString2 ...
```

/s <eventsourc>	The event source under which to log the event (required)
/i <eventid>	The event id of the event (required)
/c	The event category of the event (optional). This is a numerical ID that is defined in the
<eventcategory>	event message file that is associated with the event source.
/logInformation	Log as information event
/logWarning	Log as warning event
/logError	Log as error event

Examples

Example 1: Log event id 500 from event source "Saturn Surveillance" to the event log with the warning severity

```
logevent /s "Saturn Surveillance" /i 500 /logWarning
```

Example 2: Log event id 550 from event source "Milky Way Reporting" with the insertion strings "15:00" and "Successful" to the event log as an information event

```
logevent /s "Milky Way Reporting" /i 550 /logInformation 15:00 Successful
```

In this example, the string "15:00" will be insertion string 1 (%1) and "Successful" will be insertion string 2 (%2). See [this article](#) for more information on insertion strings in event messages.

8.4 Logoff Delay

Logoff Delay logs 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.

Interface

Command-line / None

Files

logoffdel.exe

Supported Platforms

Windows

8.4.1 Usage

Command Line Parameters

```
logoffdel /t <timeout> /l <logfile> /f /i
```

/t timeout Seconds after which the user will be logged off

/l logfile Full path to a debug log file

/f Force a logoff, no questions will be asked and unsaved data will be lost

/i 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

```
logoffdel /i /t 300
```

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

```
logoffdel /l c:\logoff_delay.txt /f /i /t 600
```

8.5 ProcessDmp

ProcessDmp creates a process (memory) dump of the specified process that can later be used by various debugging tools such as WinDbg. Dump files can be optionally compressed. The file name used is comprised of the process name, PID and a timestamp, e.g. **notepad.exe_17576_1586210388.dmp**.

Interface

Command-line

Files

processdmp.exe

Supported Platforms

Windows

8.5.1 Usage

Command Line Parameters

```
processdmp /f /c /o <outputdirectory> processName
```

/f Create full memory dump instead of minidump

/c Compress dump file

/o Change output directory, default is current directory

<outputdirectory>

processName The name of the process for which the dump file should be created, e.g. "notepad.exe". ProcessDmp will create multiple dump files if multiple instances of the process exist

Examples

Example 1: Create a dump file for Notepad in the current directory

```
processdmp notepad.exe
```

Example 2: Create a compressed dump file for all instances of myapp.exe in C:\Dumps at 15:00 and *Successful* to the event log as an information event

```
processdmp /c /o C:\Dumps myapp.exe
```

8.6 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.

Logging

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

Interface

None

Files

servicescheduler.exe
servicescheduler.ini

service file, will be copied to %systemroot%\system32
configuration file, needs to be present in %systemroot%

Supported Platforms

Windows

8.6.1 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. Copy the **servicescheduler.ini** to the same directory where **servicescheduler.exe** is located
3. Configure the service configuration file **servicescheduler.ini** (see next chapter on syntax)
4. Run `servicescheduler.exe /start` to start the service

8.6.2 Configuration

The ServiceScheduler service is configured with the configuration file **servicescheduler.ini** which needs to be located in the same directory as **servicescheduler.exe** (the installation directory by default).

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
- restart
- 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 Print Spooler ("spooler") service weekdays at 10pm, and start the service again at 10:15pm

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

Example 2: Stop the MS SQL Server service daily at 3am and restart it again at 4am

```
MSSQLServer, stop, 03:00, Mon. Tue. Wed. Thu. Fri. Sat. Sun  
MSSQLServer, start, 04:00, 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.

8.6.3 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 **servicescheduler.ini** in the installation directory.

8.7 sleep

Sleep sleeps for X milliseconds and is designed to be used in batch files.

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

Interface

Command-line

Files

sleep.exe

Supported Platforms

Windows

8.7.1 Usage

Command Line Parameters

sl eep m i l l i seconds

milliseconds Milliseconds to wait

Examples

Example 1: Sleep for 1 second

```
sl eep 1000
```

Example 2: Sleep for 2.5 seconds

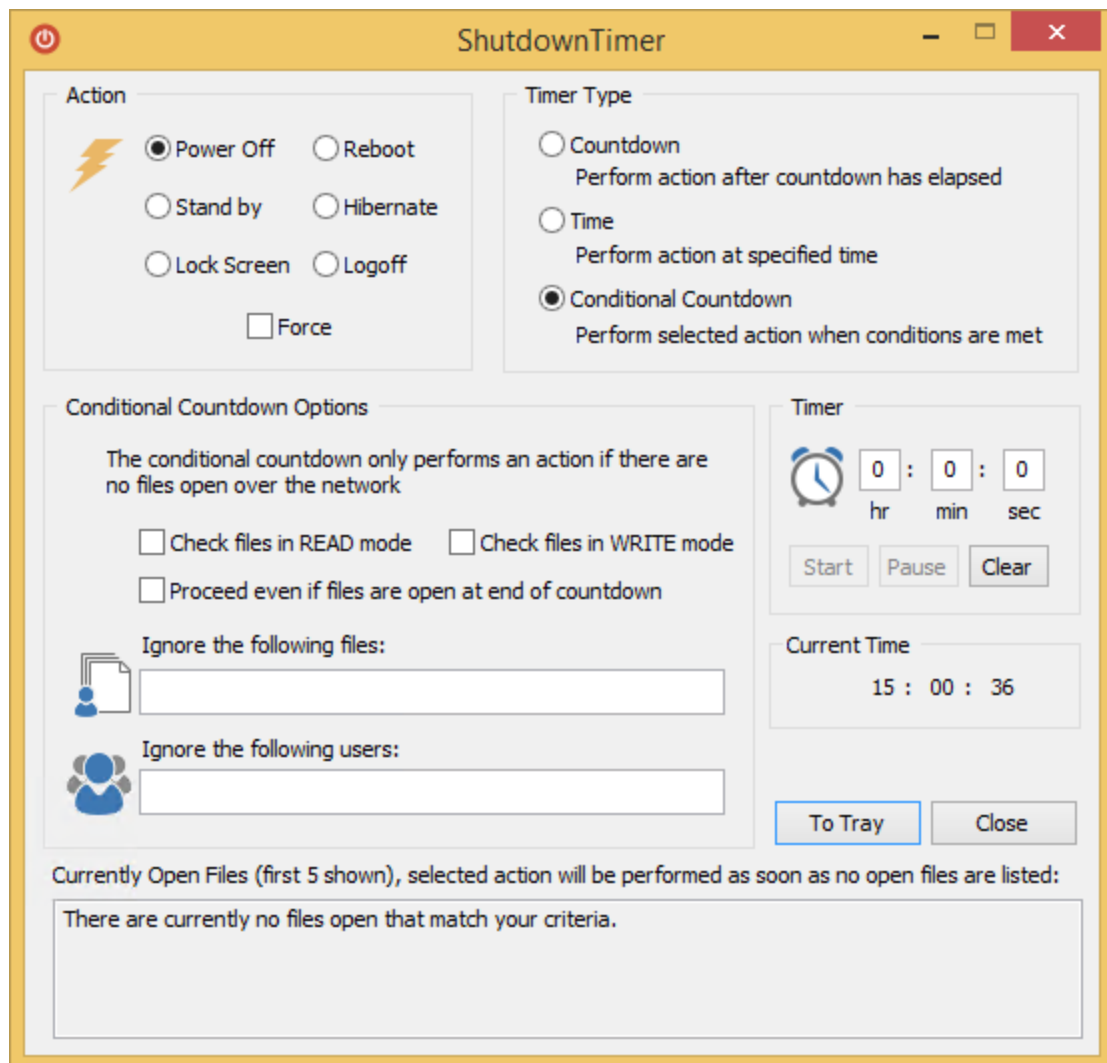
```
sl eep 2500
```

8.8 ShutdownTimer

ShutdownTimer performs certain system actions either at a certain time or in a specified amount of time. The 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

**Interface**

Graphical

Files

ShutdownTimer.exe

Supported Platforms

Windows

8.8.1 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

Forcing applications to close: Check the **Force** checkbox to force applications to close when you perform a **Power Off**, **Reboot** or **Logoff** action.



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.

8.8.1.1 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.

8.8.2 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.

8.9 uptime

Uptime displays 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.

Interface

Command-line

Files

uptime.exe

Supported Platforms

Windows

8.9.1 Usage

Command Line Parameters

`upt i me / s / o`

`/o /once`

displays the current uptime one time and returns

`/s /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

`upt i me`

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

`upt i me / o / s`

8.10 EventSentry (Tray App)

EventSentry is a background application that resides in the system tray and provides the user with a system status of the host where it's running on.

Tray Icon

The tray icon is dynamic and will show the EventSentry logo by default. Hovering over the icon will show the current host name along with the current uptime. The app monitors the CPU and disk queue length in the background and will dynamically change the tray icon to either a CPU or DISK icon if high utilization is detected:



CPU Alert: CPU usage 85% or higher



CPU Warning: CPU usage 70% or higher



Disk Warning: Disk queue length 3 or higher

Internet Test

Verifies the current Internet connection by performing a number of tests every second.

DNS: Verifies whether a DNS query was successful.

Gateway: If available, pings the gateway IP address

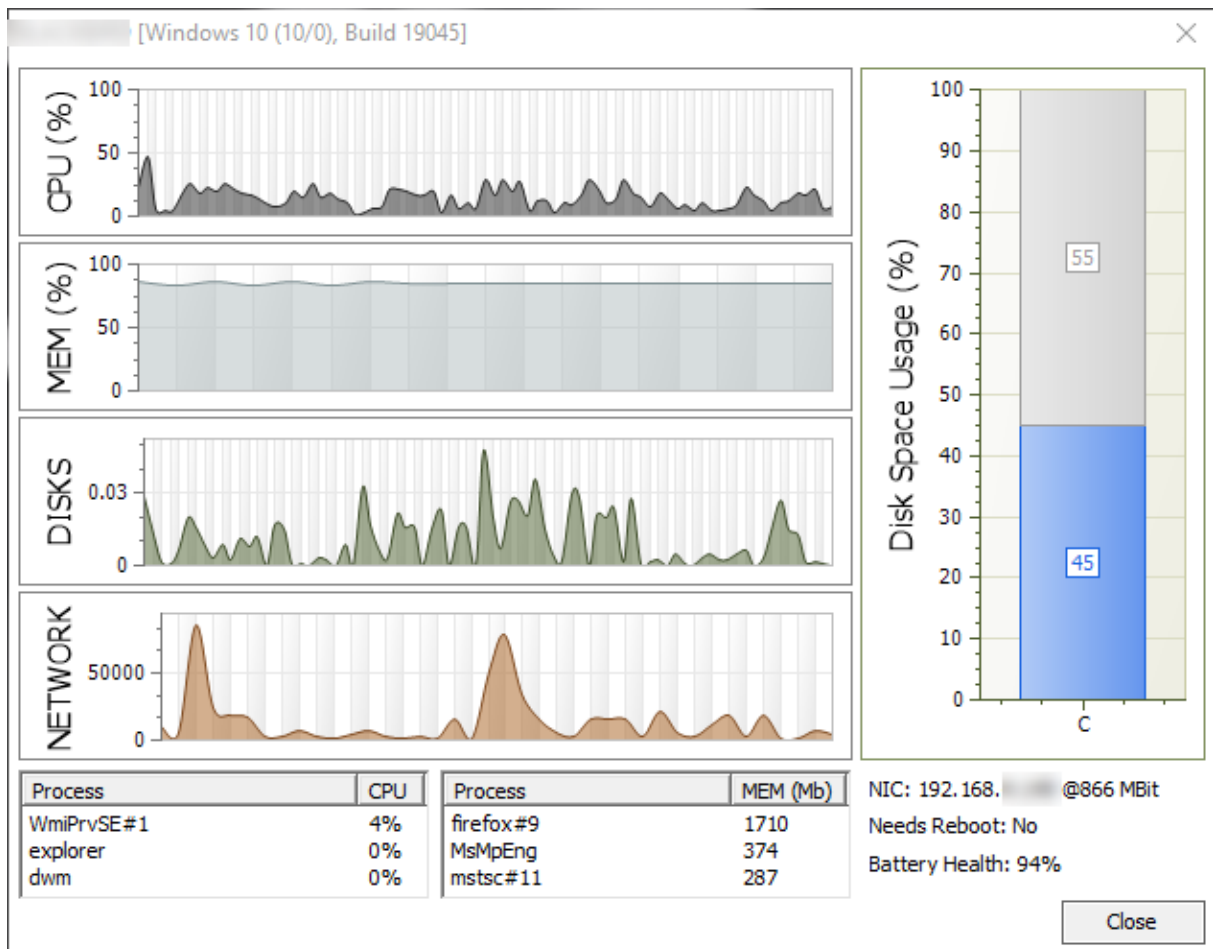
Packet Loss / Delay: Ping results

IP Address / Hostname: Public IP address and host name (if available)

WiFi SSID: The current Wifi SSID, if adapter is connected to a WiFi network

System Information

The system information dialog shows additional performance stats and system information and can be displayed by either double-clicking the tray icon or by right-clicking the icon and selecting "System Information".



The system information dialog shows the following information:

- CPU utilization
- Memory utilization
- Disk utilization
- Disk space usage of all physical disks
- Top 3 processes (CPU utilization)
- Top 3 processes (memory utilization)
- Current IP address and link speed
- Indication whether host needs a reboot
- Battery health (when applicable)
- Other logged on users (if any)



Since the EventSentry application does not run elevated, the top processes shown may not include system processes or processes from other users that are not accessible with the default process elevation level.

8.11 SeriMon

Serimon reads data from a COM port and displays it in the command line. Data is either displayed as is in ASCII mode, or formatted for select sensors (currently only the DEVMO SDS011 is supported).

Interface

Command-line

Files

serimon.exe

Supported Platforms

Windows

8.11.1 Usage

Command Line Parameters

```
serimon /c <COMPORT> /s DEVMO_SDS011 /l /d <DELAY>
```

/c COM[1..9]	the COM port to open, virtual COM ports are fully supported
/s DEVMO_SDS011 ASCII	how to interpret the data
/l	lquery data indefinitely, abort with CTRL-C
/delay	use with "/l", delay in ms between continuous iterations
/header	shows header (only useful when used with /s other than ASCII)

Examples

Example 1: Display all data returned on COM3 as text

```
serimon /c COM3 /s ASCII
```

Example 2: Display results from the DEVMO SDS011 sensors on COM4 and keep refreshing every 2 seconds

```
seri mon /c COM4 /s DEVMO_SDS011 /l /d 2000
```

9 Credits

We would like to thank the following companies and projects, without which the EventSentry SysAdmin Tools in its current form would not be possible:

- [Artua](#)
- [tcpdump/libpcap project](#)
- [WinPcap project](#)

9.1 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.

10 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 EventSentry SysAdmin Tools is running
- The version of EventSentry SysAdmin Tools
- Your question

Problems

If you are experiencing problems with EventSentry SysAdmin Tools then please visit our support forums:

forums.netikus.net

and include the following information:

- The Operating System (incl. Service Pack Version) on which EventSentry SysAdmin Tools is running
- The version of EventSentry SysAdmin Tools
- 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?

11 Suggestions?

Nobody is perfect and neither is EventSentry SysAdmin Tools. 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 EventSentry SysAdmin Tools.

12 Other Software from NETIKUS.NET

If you like the EventSentry SysAdmin Tools then you might just 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
EventSentry Admin Assistant	Software to automate common tasks of Administrators	Freeware
Gateway IP Monitor	Monitor the IP address of your default gateway when using NAT	Freeware