



Informant Systems, Inc.

Informant Systems, Inc.

11135 23 A Avenue
Edmonton, AB T6J4P4 Canada
p: 780-908-6669 f: 780-434-8991
www.informant-systems.com

SNMP Informant™ Standard

Installation and Configuration Guide

Release 1.6



SNMP
Informant

"GET more out of Windows!"

**Windows SNMP support for
industry standard Network
Management Systems**

www.snmp-informant.com

Copyright

Copyright © 2004-2008 Informant Systems, Inc. All Rights Reserved.
Copyright © 1999-2004 Williams Technology Consulting Services

Restricted Rights Legend

This software and documentation is subject to and made available only pursuant to the terms of the Informant Systems License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the software except as specifically allowed in the agreement. This document may not, in whole or in part, be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from Informant Systems, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of Informant Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, INFORMANT SYSTEMS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Informant Systems may make changes to specifications and product descriptions at any time, without notice.

Trademarks or Service Marks

SNMP Informant is a registered trademark of Informant Systems, Inc. All other trademarks are the property of their respective companies.

Document Information

Version	Last Updated	Author	Edit Notes
Std 1.5	June 26, 2008	GKW	Creation of Installation and Configuration Guide (condensed from Commercial version to support SNMP Informant Standard).
Std 1.6	June 26, 2008	GEK	Updates for 1.6 release

Table of Contents

Introduction	1
About Informant Systems, Inc.	1
Statement of Limitations	2
NMS Compatibility	2
Warranty	2
SNMP Informant Overview	2
PDH Agents	3
System Requirements	4
64-bit Support	4
Installation and Configuration	4
Installing the Microsoft Windows SNMP service	4
Configuring the Microsoft SNMP service	5
Installing SNMP Informant	5
GUI Installation	5
Command Line Installation	10
Configuring SNMP Informant	12
Registry Settings and their Meanings	13
Using SNMP Informant	14
General Usage Notes	15
Using the SNMP Informant Standard Agent	15
Troubleshooting SNMP Informant	20
Troubleshooting Table	20
Troubleshooting SNMP Informant Standard	21

Table of Figures

Figure 1 – SNMP Informant Functional Overview	3
Figure 2 – SNMP Informant Application Structure (PDH Agents)	3
Figure 3 – Anatomy of an SNMP Informant OID	16

Introduction

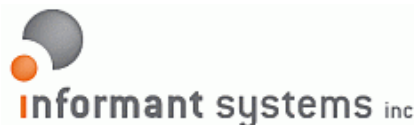
Thank you for downloading and using (or trying) SNMP Informant. We are sure you will like what you see, and recognize the value in our products. This document is intended to help you make the most of SNMP Informant. If you have any comments about this document (omissions, corrections, etc.), please contact product.support@informant-systems.com, and let us know.

We have always strived to provide excellent value for your money with SNMP Informant. If you are pleased with this product, please tell your colleagues and friends. If not, please tell *us*, so we can address your concerns as soon as possible.

About Informant Systems, Inc.

Informant Systems has been developing and providing the network management community with cost-effective SNMP extension agents for Windows operating systems and server applications since 1999. Our flagship product, SNMP Informant™ is in use by small, medium and large organizations around the world, including Universities, financial institutions, Fortune 500 companies and large multi-national organizations.

Resellers or commercial product developers interested in bundling or reselling SNMP Informant are encouraged to contact product.info@informant-systems.com in order to find out more information.



Informant Systems, Inc.

11135 – 23A Avenue
Edmonton, AB T6J4W5 Canada
Phone: 780-908-6669
Fax: 780-434-8991
Web: <http://www.informant-systems.com>

Product Information: product.info@informant-systems.com
Product Support: product.support@informant-systems.com

Primary Contact: **Garth K. Williams – President and Managing Director**
garth.williams@informant-systems.com

Statement of Limitations

Although we have attempted to find and correct any bugs in the software, we will not be held responsible for any damage or losses (of ANY kind) caused by the use (or misuse) of this product. Names, icons, functionality, file format, etc. are subject to change in future versions of SNMP Informant without notice.

Also, while we are well aware that we cannot control who downloads and/or uses SNMP Informant, we would like to make it clear that:

UNDER NO CIRCUMSTANCES IS SNMP INFORMANT DESIGNED TO MANAGE, SUPERVISE CONTROL, MONITOR OR OTHERWISE INTERACT WITH INSTRUMENTS AND/OR EQUIPMENT THAT MIGHT POTENTIALLY AFFECT HUMAN LIFE.

For example:

SNMP Informant is not designed for, nor is it intended to be used to monitor or interact with computer systems that might be used to construct, operate or maintain any type of the following facilities (including but not limited to):

- nuclear power
- Air traffic control or navigation
- Maritime control or navigation
- Other commuter transport (rail, bus, taxi, etc.)
- Military (operations, control, etc.)

NMS Compatibility

The SNMP Informant MIBs are written to comply with RFC standards, and are compiled and tested on several different MIB compilers and applications in order to ensure maximum compatibility. Nonetheless, we make NO guarantees that they will compile on any SPECIFIC product. In the event that you have problems using SNMP Informant (i.e. compiling SNMP Informant MIBs) with your particular NMS, please consult the Product Support Forums.

Warranty

All versions of SNMP Informant are warranted to operate EXACTLY as described on the SNMP Informant web site (www.snmp-informant.com). If you have ANY questions about SNMP Informant's ability to gather certain performance metrics, please contact product.info@informant-systems.com, and we will be pleased to help you out.

SNMP Informant Overview

SNMP Informant products are Simple Network Management Protocol (SNMP) extension agents that provide the capability to access Microsoft Windows Operating System and Application Server Performance Counters, WMI classes and other server information through the SNMP protocol. SNMP Informant agent information can be accessed using either SNMPv1 or SNMPv2 protocols from an SNMP Network Management System (NMS). Such applications include (but are not limited to) HP Network Node Manager, Sciencelogic EM7, Paessler IPCheck, Netmon, IPMonitor and others.

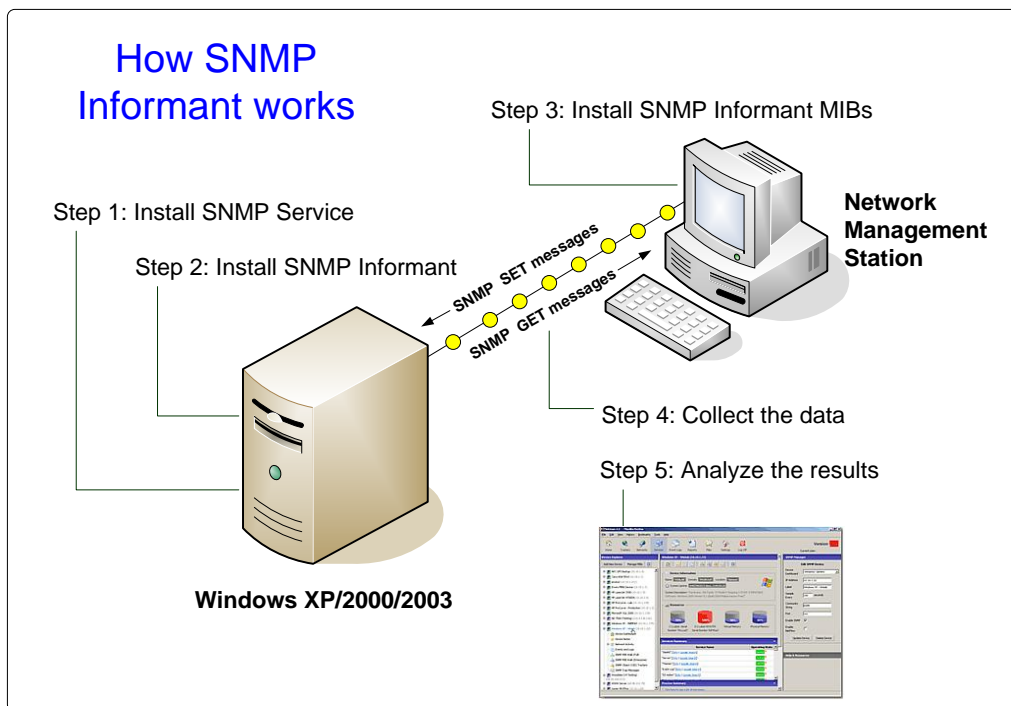


Figure 1 – SNMP Informant Functional Overview

SNMP Informant agents are DLL (Dynamic Link Libraries) extensions to the Microsoft Windows SNMP service. The Windows SNMP Service must be installed and running before the SNMP Informant agent would be available.

PDH Agents

SNMP Informant PDH agents (Advanced and Application Plus Packs) use the Windows Performance Data Handler library to access the performance counters, as shown below.

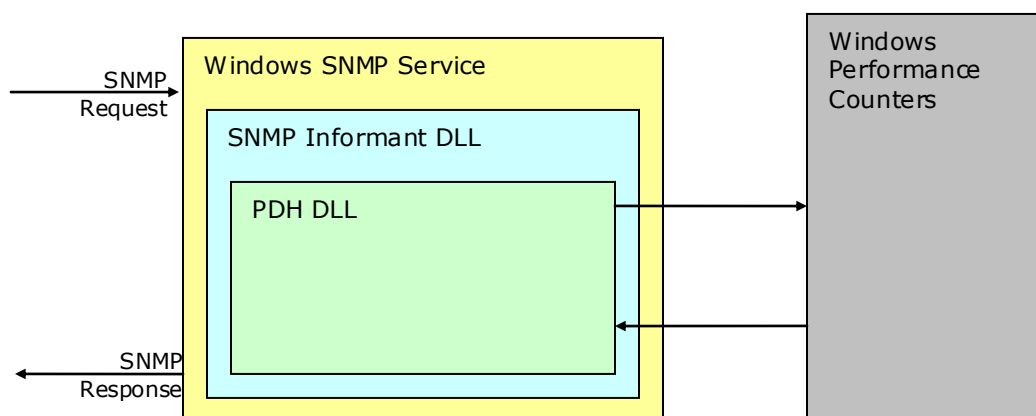


Figure 2 – SNMP Informant Application Structure (PDH Agents)

STANDARD AND ADVANCED AGENTS SPECIFIC NOTES

Unlike Windows XP* and Windows 2003*, Windows 2000 does not come “out of the box” with logical disk performance counters enabled. Unless activated, the only disk

counters accessible by SNMP Informant are the physical disk performance counters. In order to activate logical disk performance counters on Windows 2000, do this:

1. Open an OS prompt
2. Type "diskperf -y" (omit the "")
3. Close the OS Prompt
4. reboot the system

* Windows 2003 and Windows XP dynamically activate logical disk counters as needed.

System Requirements

The SNMP Informant Agent executes on the following operating systems. It does not run on Microsoft Windows 95, 98, ME, or NT.

- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows XP Home
- Microsoft Windows XP Professional (x86/x64)
- Microsoft Windows 2003, Standard Edition(x86/x64)
- Microsoft Windows 2003, Enterprise Edition (x86/x64)
- Microsoft Windows 2003, Datacenter Edition (x86/x64)
- Microsoft Windows 2003, Web Edition (x86)
- Microsoft Windows 2003, Small Business Server (x86)
- Microsoft Window 2008, Standard Edition (x86/x64)
- Microsoft Window 2008, Enterprise Edition (x86/x64)

SNMP Informant Advanced Agents requires a minimum of a Pentium II class processor, 32 MB of available memory and 2MB of available disk space.

64-bit Support

The SNMP Informant Standard Edition supports x86 and x64 bit Microsoft Windows operating systems. You must purchase the SNMP Advanced Edition to support ia64 based Windows operating systems.

Installation and Configuration

The SNMP Service is not installed by default on the Microsoft Windows operating systems and is not configured by default on the Microsoft Windows 2003 operating systems. **The SNMP Service must be installed and configured prior to installing the SNMP Informant agent.** If the SNMP Service is already installed and configured, then skip to the Installing SNMP Informant section.

Installing the Microsoft Windows SNMP service

Since the Microsoft Windows operating systems vary slightly, the steps to install the SNMP Service may deviate a little from this guide. You may also refer to the Microsoft Windows Help (Start\Help) under "SNMP Service (installing)" for more information on installing the SNMP Service.

You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In **Components**, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
3. Select the **Simple Network Management Protocol** check box, and click **OK**.
4. Click **Next**.
5. Insert the respective CD or specify the complete path of the location at which the files are stored.
6. **SNMP** starts automatically after installation.

Configuring the Microsoft SNMP service

The Microsoft Windows SNMP Service must be configured before it can be accessed by any SNMP Manager software. Since the Microsoft Windows operating systems vary slightly, the steps to configure the SNMP Service may deviate a little from this guide. You may also refer to the Microsoft Windows Help (Start\Help) under "SNMP Service (security, configuring)" for more information on configuring the SNMP Service.

To configure SNMP agent in Windows XP, 2000 and 2003 systems, follow the steps given below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools** and then double-click **Computer Management**.
2. In the console tree, click **Services and Applications** and then click **Services**.
3. In the details pane, scroll down and click **SNMP Service**.
4. On the **Action** menu, click **Properties**.
5. On the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
6. Under **Accepted community names**, click **Add**.
7. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
8. In **Community Name**, type a case-sensitive community name, and then click **Add**.
9. Specify whether or not to accept SNMP packets from a host:
10. To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
11. To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name and IP or IPX address, and then click **Add** again.
12. Click **Apply** to apply the changes.

Installing SNMP Informant

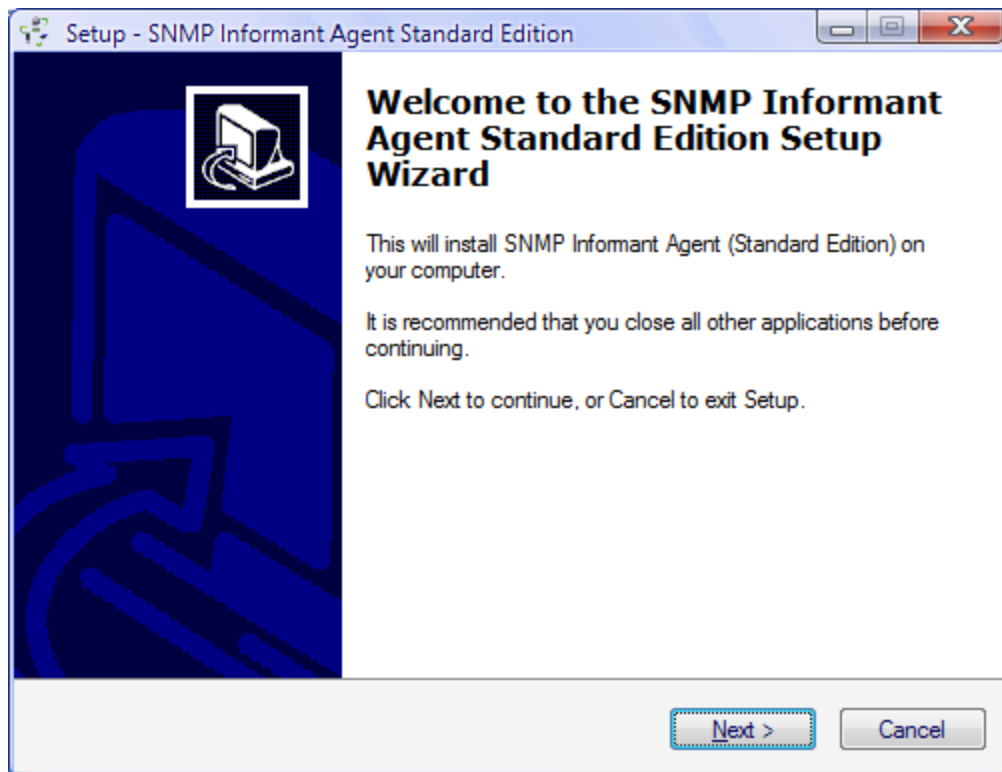
SNMP Informant Agent installation programs provide two methods to install:

- **Graphic user interface (GUI)** – A graphics wizard based installation requiring input from the user either with the mouse and keyboard.
- **Command line interface** – An interface where you can install the software without any intervention from the user. Also known as an unattended install.

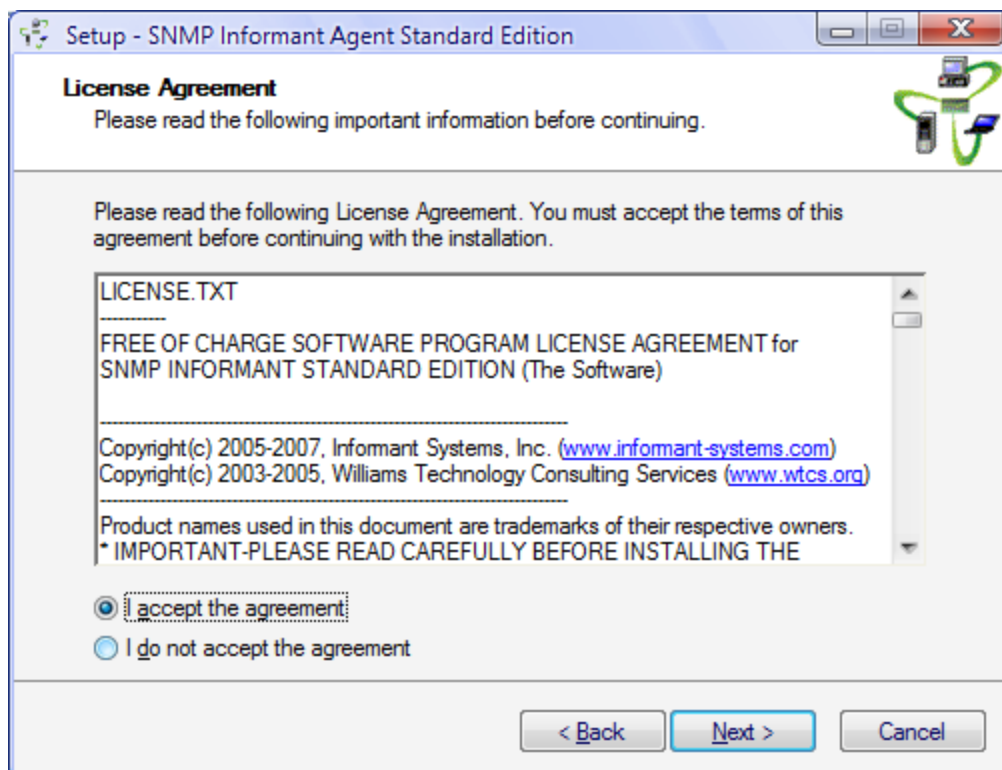
GUI Installation

Start the informant executable.

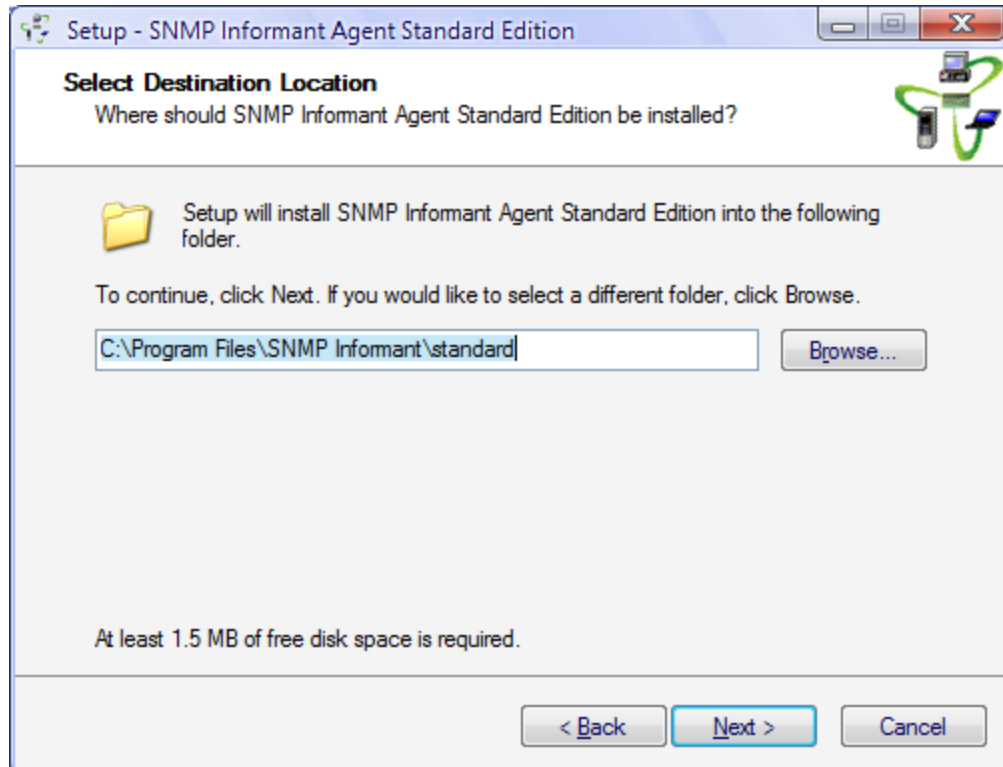
Click the **Next** button in the welcome screen.



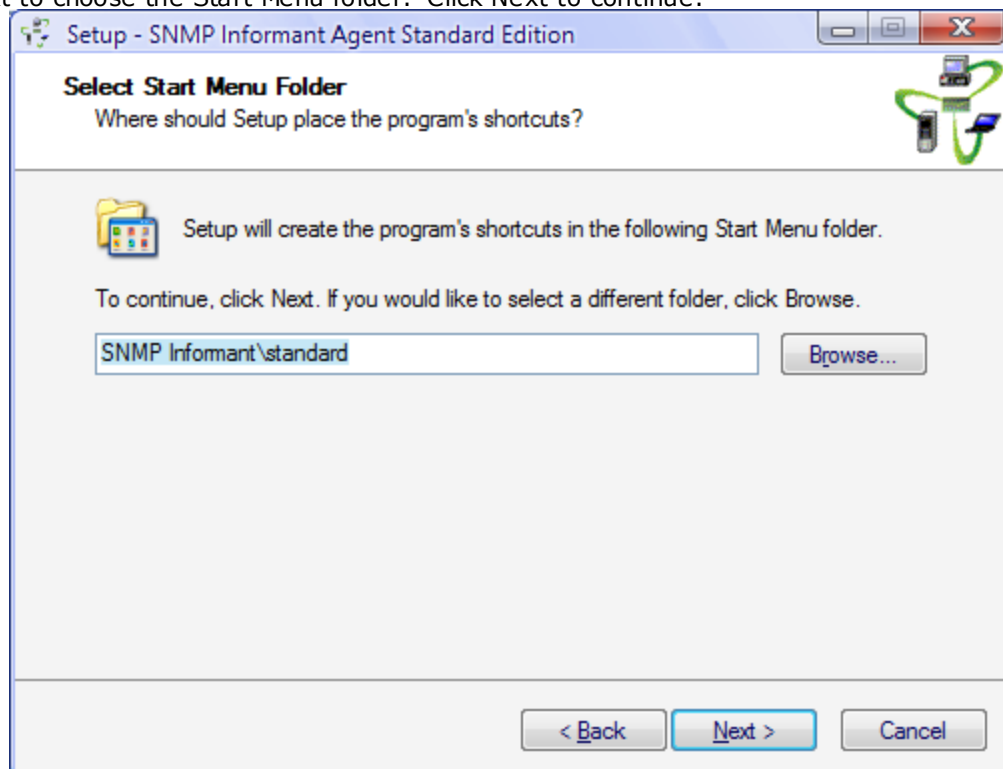
Read the License Agreement and click the "I accept the agreement" radio button if you agree with the license. Click the Next button.



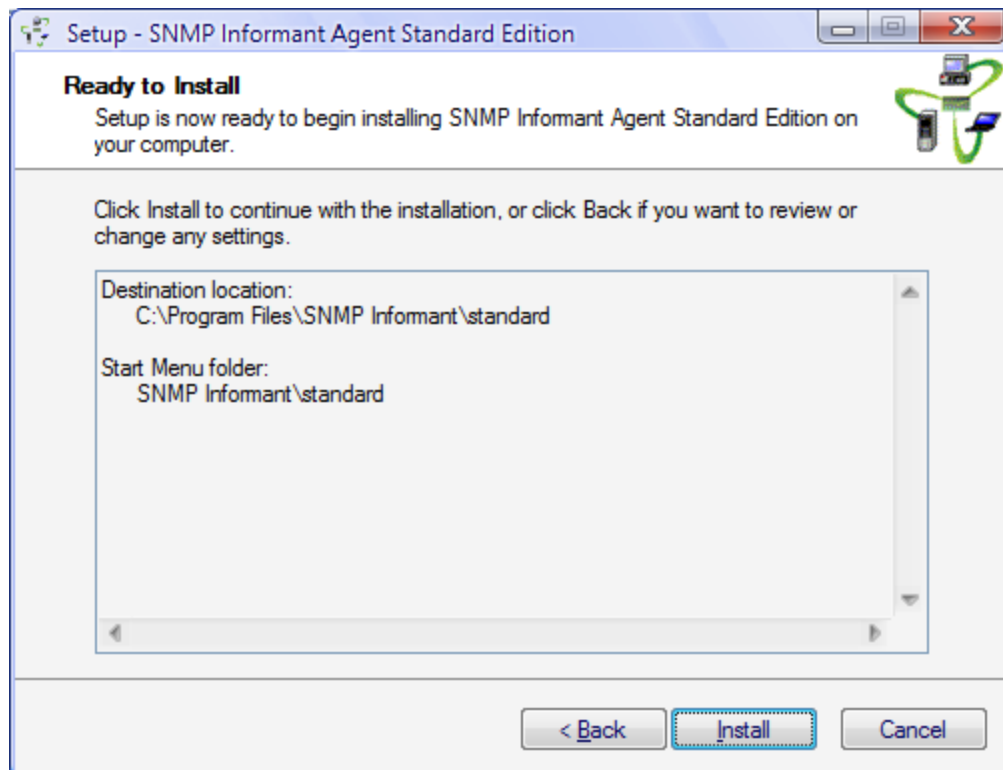
Enter where you would like to install the SNMP Informant Agent. Click the Next button.



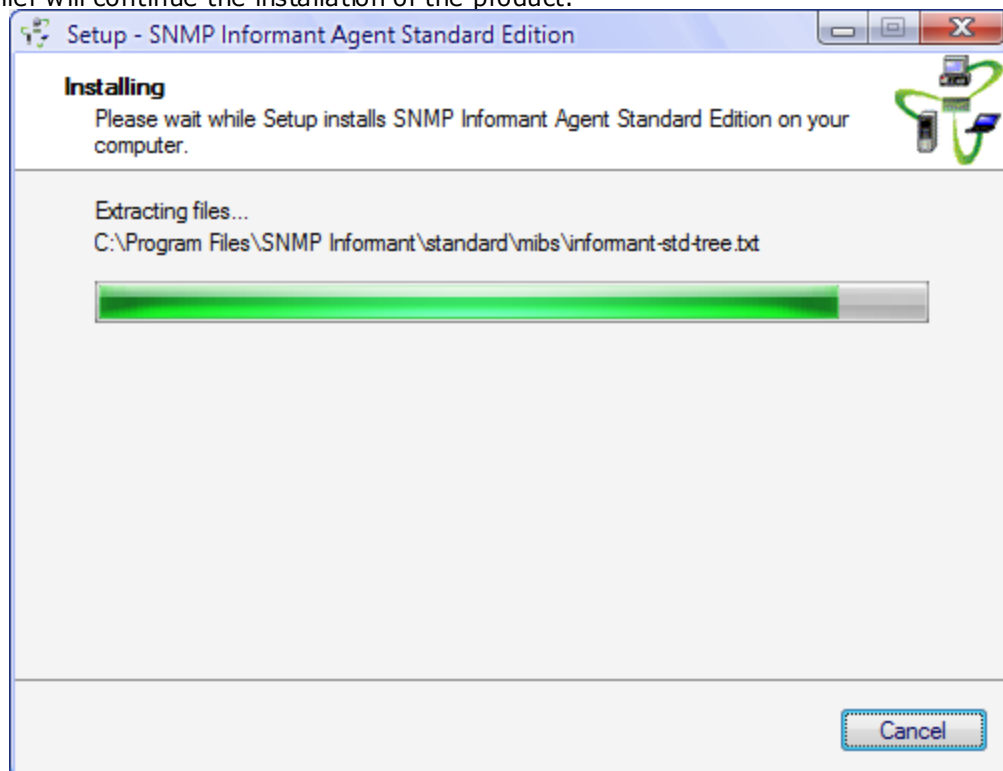
Click Next to choose the Start Menu folder. Click Next to continue.



Verify the installation parameters and click the Install button.



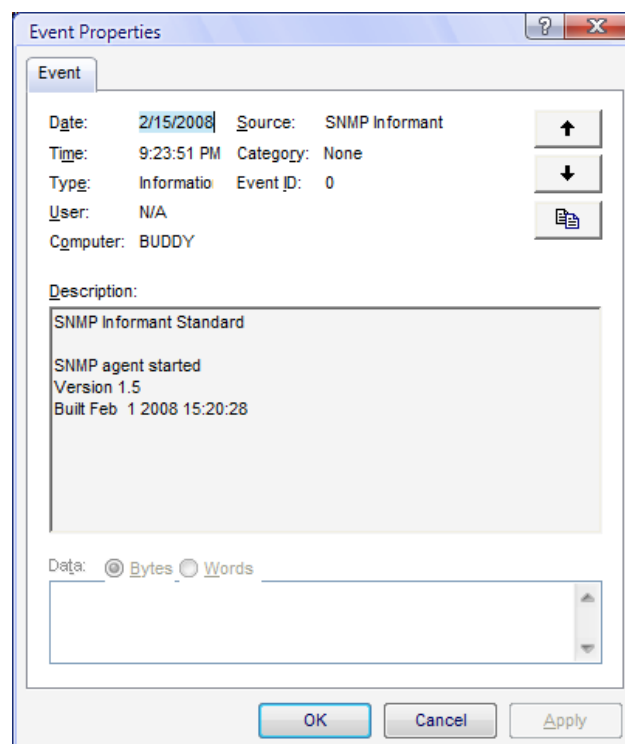
The installer will continue the installation of the product.



Click the Finish button after installing the SNMP Informant agent. Clear the "View Readme.pdf" check-box if you do not want to view the readme document.



That's it! You've now installed and configured the SNMP Informant agent(s). Next, you should check the Windows Application Event Log to confirm successful start-up. SNMP Informant will add its own startup message to the Application Event log.



Command Line Installation

The Setup program accepts optional command line parameters. These can be useful to system administrators, and to other programs calling the Setup program.

/SILENT, /VERYSILENT

Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed.

If a restart is necessary and the '/NORESTART' command isn't used (see below) and Setup is silent, it will display a Reboot now? message box. If it's very silent it will reboot without asking.

/SUPPRESSMSGBOXES

Instructs Setup to suppress message boxes. Only has an effect when combined with '/SILENT' and '/VERYSILENT'.

The default response in situations where there's a choice is:

- Yes in a 'Keep newer file?' situation.
- No in a 'File exists, confirm overwrite.' situation.
- Abort in Abort/Retry situations.
- Cancel in Retry/Cancel situations.

Yes (=continue) in the following situations:

- DiskSpaceWarning
- DirExists
- DirDoesntExist
- NoUninstallWarning
- ExitSetupMessage
- ConfirmUninstall

Yes (=restart) in a FinishedRestartMessage/UninstalledAndNeedsRestart situation.

5 message boxes are not suppressible:

- The About Setup message box.
- The Exit Setup? message box.
- The FileNotInDir2 message box displayed when Setup requires a new disk to be inserted and the disk was not found.
- Any (error) message box displayed before Setup (or Uninstall) could read the command line parameters.
- Any message box displayed by [Code] support function MsgBox.

/LOG

Causes Setup to create a log file in the user's TEMP directory detailing file installation and [Run] actions taken during the installation process. This can be a helpful debugging aid. For example, if you suspect a file isn't being replaced when you believe it should be (or vice versa), the log file will tell you if the file was really skipped, and why.

The log file is created with a unique name based on the current date. (It will not overwrite or append to existing files.)

The information contained in the log file is technical in nature and therefore not intended to be understandable by end users. Nor is it designed to be machine-parseable; the format of the file is subject to change without notice.

/LOG="filename"

Same as /LOG, except it allows you to specify a fixed path/filename to use for the log file. If a file with the specified name already exists it will be overwritten. If the file cannot be created, Setup will abort with an error message.

/NOCANCEL

Prevents the user from cancelling during the installation process, by disabling the Cancel button and ignoring clicks on the close button. Useful along with '/SILENT' or '/VERYSILENT'.

/NORESTART

Instructs Setup not to reboot even if it's necessary.

/RESTARTEXITCODE=exit code

Specifies the custom exit code that Setup is to return when a restart is needed. Useful along with '/NORESTART'. Also see Setup Exit Codes.

/LOADINF="filename"

Instructs Setup to load the settings from the specified file after having checked the command line. This file can be prepared using the '/SAVEINF=' command as explained below. Don't forget to use quotes if the filename contains spaces.

/SAVEINF="filename"

Instructs Setup to save installation settings to the specified file. Don't forget to use quotes if the filename contains spaces.

/DIR="x:\dirname"

Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified.

/GROUP="folder name"

Overrides the default folder name displayed on the Select Start Menu Folder wizard page. If the [Setup] section directive DisableProgramGroupPage was set to yes, this command line parameter is ignored.

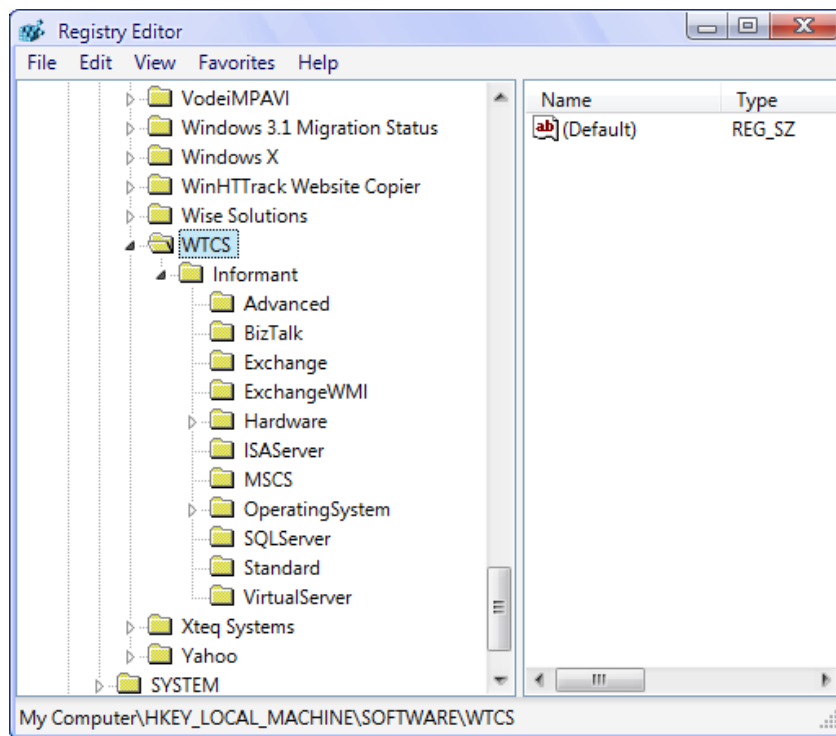
/NOICONS

Instructs Setup to initially check the Don't create any icons check box on the Select Start Menu Folder wizard page.

Configuring SNMP Informant

SNMP Informant has matured significantly over the past several years, and as a result, has an array of configuration options that you can adjust for optimal performance.

These configuration options are managed by way of registry settings for each agent. If you were to do a full installation of SNMP Informant, you would see an HKEY_LOCAL_MACHINE/Software/WTCS registry hive that looked like this:



Note: on this system, all SNMP Informant agents are shown as installed.

Within each sub-tree below WTCS Informant are various settings to configure that specific agent. Some setting categories (names) are common across all agents, and some are unique to a specific agent. When SNMP Informant is installed, default values are assigned to the registry setting categories. You may need to operate your Network Management System for a period of time to determine what values need to be adjusted.

Registry Settings and their Meanings

This section describes the registry settings used to control SNMP Informant's behaviour. First of all, let's define what we call a query...

Query: A request made by SNMP Informant to the local subsystem (PDH - Performance Data Helper), based on the SNMP GET, GETNEXT, or WALK request that SNMP Informant receives from a network management application or tool.

Below is a list of registry settings that can be adjusted by the user. Registry setting modifications for SNMP Informant are made at HKEY_LOCAL_MACHINE/SOFTWARE/WTCS/informant/standard. The changes you make are at the <product> level are unique for that agent. **Any other registry settings not described below within the WTCS/informant registry should **not** be changed and modifying the value may cause unpredictable results.**

Setting: EventFilterMask

Registry Type: DWORD

Default Value: 7

Units: numeric (decimal)

The EventFilterMask value controls the level of messages SNMP Informant posts into the Application Event Log. Valid values and their meanings are:

Value	Meaning
7	Log Information, Error and Warning messages
6	Log Warning and Information messages
5	Log Information and Error messages
4	Log Information messages
3	Log Error and Warning messages
2	Log Warning messages
1	Log Error messages
0	Log no messages

Setting: GetInstanceTimeSpan

Registry Type: DWORD

Default Value: 60000

Units: milliseconds

This registry setting is used to identify when to look for new instances a PDH object. For example, when iterating across the "process" PDH object, there is a performance hit whenever you looked for a new instances. To minimize response time, we only look for new instances whenever the GetNextInstanceTimeSpan (default time is 60000 seconds) expires or we switch to a different PDH counter/object. Setting this value to a lower number will keep your process list more accurate (current), but will do as at the expense of longer response time as a new iteration is performed.

Setting: MinimumQueryRate

Registry Type: DWORD

Default Value: 5000

Units: milliseconds

This registry setting determines how often a new PDH raw value is gathered and a calculation is performed. SNMP uses the UDP (a lossy network protocol) to communicate with the managing station. Since the response can be lost or the managing station would timeout on the SNMP query and many calculation are based on the difference between the last raw value and the current raw value, the SNMP Informant agent will return the previous calculated value if the same request is made within the MinimumQueryRate registry defined period. This is done to prevent returning false calculated due to the SNMP Managing Station requerying the request assuming that the packet was lost. A user would reduce this value if they are querying the same OID less than every 5 seconds.

Setting: MaxQueryCacheSize

Registry Type: DWORD

Default Value: 300 PDH

Units: Number of queries

The number of different queries that can be cached for **both** GET and GETNEXT queries. When a request comes in, it looks for the query associated with the OID in the cache. If it doesn't exist, then it creates a query and caches it. The cache only contains entries that require multiple samples. For example, the CPU object will be in the cache, but the Memory usage will not, because the memory object counters are an "as at" (right now) sample. CPU on the other hand, is a calculated average value based on two separate samples. Both the last value and the query itself is stored. The query is used to take another sample. The last value is used for the computation to determine the average value. Increase this value for the necessary agent if you are receiving an error message from SNMP Informant stating that the query cache size was exceeded.

Entry: QueryLifeSpan

Registry Type: DWORD

Default Value: 21600000

Units: milliseconds

This is the length of time a query (and the accompanying value) can exist in the cache without being requested before it is purged. Default time is 6 hours. If the query lifespan expires, then the query (and accompanying value) is deleted. Once this query is purged from the cache, a computation between it and a new query cannot be performed. Should this be the case, the new query is stored in the cache with a sample value of 0 (in preparation for a second query, where the new value and 0 will be used to calculate an average). If a query that exists in the cache is re-requested, the QueryLifeSpan counter restarts for that query. Increase this value if you are querying the same OID more than 6 hours between samples.

Using SNMP Informant

For the most part, once the SNMP service is properly installed and configured, SNMP Informant Standard is usable immediately after install. SNMP Informant Standard

requires little or no configuration at all. If you DO need to “tune” SNMP Informant, see the “Configuring SNMP Informant” section.

After the agent is loaded and initialized, it can be queried by the SNMP Manager software.

General Usage Notes

OID Tree Listings

Please see the file in [install loc]\SNMP Informant\standard\mibs\informant-std-tree.txt for a complete tree listing of the OIDs supported by SNMP Informant STD. For example:

- C:\Program Files\SNMP Informant\standard\mibs\informant-std-tree.txt

Use the Correct MIBS

Be sure to select the correct SNMP version of MIBS for your monitoring application or MIB Browser. SNMP Informant comes with both SMIV1 (SNMPv1) and SMIV2 (SNMPv2) MIBS. You can access the SNMP Informant MIBS in the product install directory. Their location will be in directories similar to the following:

- C:\Program Files\SNMP Informant\standard\mibs\SMIV1 or SMIV2

SNMPv3

Since SNMP Informant is an SNMP Extension Agent, it does not in and of itself support SNMPv3. It is the job of the SNMP service “stack” to support SNMPv3. The native Windows 2000, XP and 2003 SNMP service only supports SNMPv1 and SNMPv2. However, there are some Windows SNMP service replacements in the market today that claim to be 100% compatible with extension agents like SNMP Informant. One such product is NuDesign Team’s “Agent Service for MS Windows”. You can find out more about this product at <http://www.nudesignteam.com/agent.html>.

SNMP Traps

At present, SNMP Informant does not generate SNMP traps.

Uninstalling SNMP Informant

The uninstall program included with SNMP Informant will remove the registry entries and clean up quite nicely, but you may need to manually remove the \Program Files\SNMP Informant\standard directory yourself after the uninstall program has completed.

Using the SNMP Informant Standard Agent

The SNMP Informant Standard agent is a bridge between the standardized SNMP protocol and the non-standard Windows performance information. Understanding how Performance Counters are referenced is necessary before grasping the SNMP OID structure.

As seen when adding a performance counter using the Windows Performance Monitor, a specific counter item is referenced using at least two names (object and counter) and where required a third name (instance).

The object name is the group the performance item is associated with (e.g. memory, processor, process, etc).

The counter name is the specific type of performance information queried for that object (e.g., the percentage of CPU time for the processor object).

The instance name is the specific instance that the query is being performed on (e.g., CPU 0 for the processor object, the lsass.exe process, etc). The instance name is always referenced as a string.

Refer to <http://technet2.microsoft.com/windowsserver/en/library/3fb01419-b1ab-4f52-a9f8-09d5eb9ef21033.mspx?mfr=true> for more information on performance object, counters, and instances.

The illustration below shows how to relate Performance Counters, Objects and Instances to an SNMP Informant OID (in this case for Memory: Available bytes):

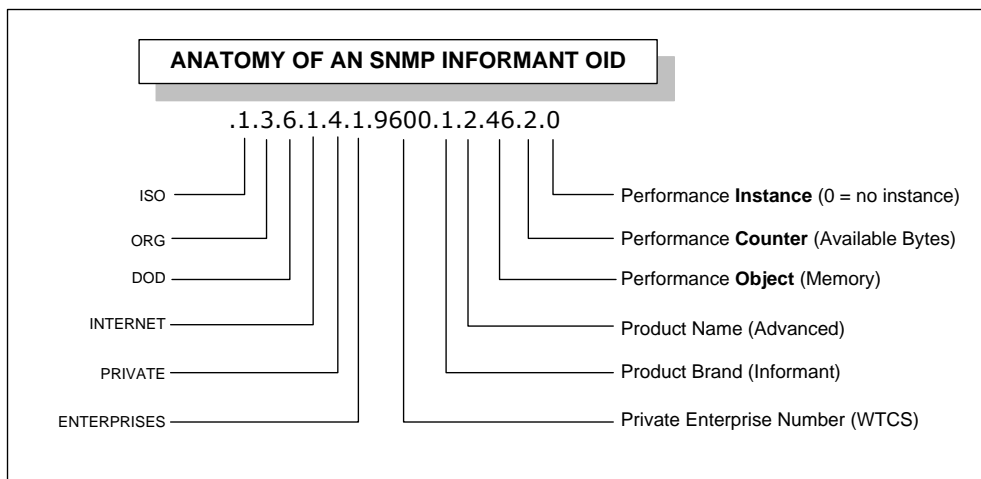


Figure 3 – Anatomy of an SNMP Informant OID

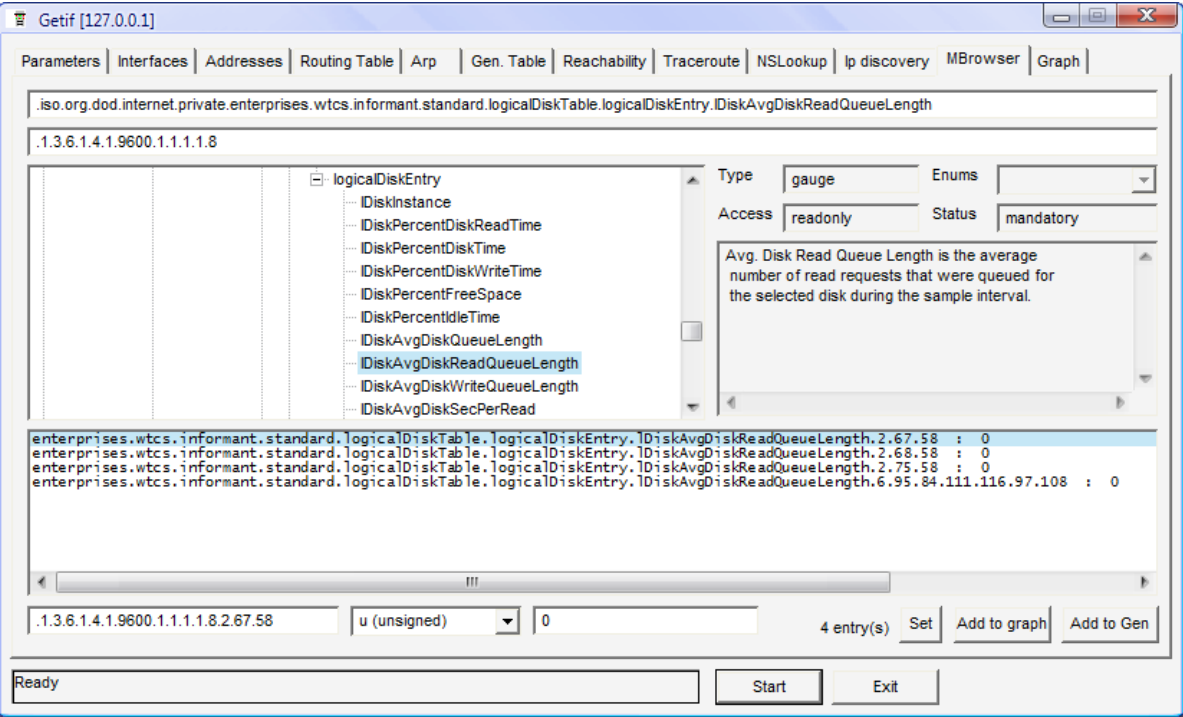
More detailed OIDs can contain instance names. For example, it is not uncommon for a server to have multiple disks, processors and network adapters. Therefore, OIDs for these performance objects will have multiple instances.

Use the modified ASCII chart below to make it easier to read SNMP Informant instance OID values, and convert them to their ASCII equivalent. We have removed the Hex and Octal values, leaving only the Decimal values.

Decimal to ASCII conversion applies to many SNMP Informant PDH agent tables, where the information (name) is pulled directly from the Performance Data Helper (we don't make the names up).

Here are four examples of this chart being used to convert an SNMP Informant Instance to an ASCII (character) equivalent. For ease of reading, we will always assume that SNMP Informant agent is the Standard version, and the prefix will be .iso.org.dod.internet.private.enterprises.wtcs.informant.standard (.1.3.6.1.4.1.9600.1.1), and the walk will occur below that point. The **first number** after the fully qualified OID (in the first couple of examples a 2) tells us how many characters follow. The dots between the **characters** can be removed from the Character (ASCII) Equivalents.

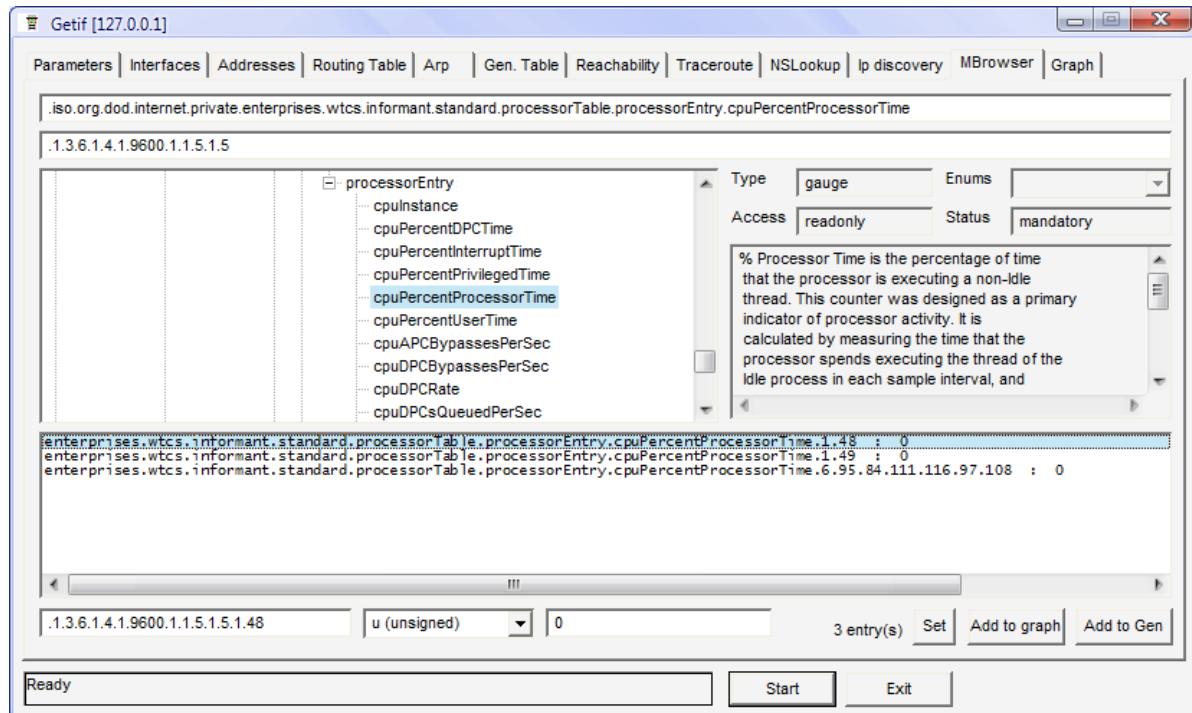
Example 1: LogicalDisk: Logical Disk Average Read Queue Length
(we've included a Getif Screenshot in this example to provide further detail)



Fully qualified SNMP Informant OID (walk from here)	SNMP Informant Instance (Decimal) OID response	Character (ASCII) Equivalent
.logicalDiskTable.logicalDiskEntry.IDiskAvgDiskReadQueueLength	.2.67.58	C:
.logicalDiskTable.logicalDiskEntry.IDiskAvgDiskReadQueueLength	.2.68.58	D:
.logicalDiskTable.logicalDiskEntry.IDiskAvgDiskReadQueueLength	.2.75.58	K:
.logicalDiskTable.logicalDiskEntry.IDiskAvgDiskReadQueueLength	.6.95.84.111.116.97.108	_Total

- .2 indicates that 2 **characters** follow
- .6 indicates that 6 **characters** follow

Example 2: Processor: % Processor Time



Fully qualified SNMP Informant OID (walk from here)	SNMP Informant Instance (Decimal) OID response	Character (ASCII) Equivalent
.processorTable.processorEntry.cpuPercentProcessorTime	.1.48	0
.processorTable.processorEntry.cpuPercentProcessorTime	.1.49	1
.processorTable.processorEntry.cpuPercentProcessorTime	.6.95.84.111.116.97.108	_Total

.1 indicates that 1 **character** follows

.6 indicates that 6 **characters** follow

Example 3: Network Interface: netBytesTotalPerSecond

Fully qualified SNMP Informant OID (walk from here)	.networkInterfaceTable.networkInterfaceEntry.netBytesTotalPerSec
SNMP Informant Instance (Decimal) OID response	.25.77.83.32.84.67.80.32.76.111.111.112.98.97.99.107.32.105.110.116.101.114.102.97.99.101
Character (ASCII equivalent)	MS TCP Loopback interface

.25 indicates that 25 **characters** follow

Fully qualified SNMP Informant OID (walk from here)	.networkInterfaceTable.net work InterfaceEntry.netBytesTotalPerSec
SNMP Informant Instance (Decimal) OID response	.27.72.80.32.78.67.51.49.54.51.32.70.97.115.116.32.69.116.104.101.114.110.101.116.32.78.73.67
Character (ASCII equivalent)	HP NC3163 Fast Ethernet NIC

.27 indicates that 27 **characters** follow

SNMP Informant Decimal OID instance to ASCII Character Conversion Table

Decimal Value	Character Value
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	SPACE

Decimal Value	Character Value
33	!
34	"
35	#
36	\$
37	%
38	&
39	'
40	(
41)
42	*
43	+
44	,
45	-
46	.
47	/
48	0
49	1
50	2
51	3
52	4
53	5
54	6
55	7
56	8
57	9
58	:
59	;
60	<
61	=
62	>
63	?

Decimal Value	Character Value
64	@
65	A
66	B
67	C
68	D
69	E
70	F
71	G
72	H
73	I
74	J
75	K
76	L
77	M
78	N
79	O
80	P
81	Q
82	R
83	S
84	T
85	U
86	V
87	W
88	X
89	Y
90	Z
91	[
92	\
93]
94	^
95	_
96	`

Decimal Value	Character Value
97	a
98	b
99	c
100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o
112	p
113	q
114	r
115	s
116	t
117	u
118	v
119	w
120	x
121	y
122	z
123	{
124	
125	}
126	~
127	DEL

= commonly seen values

Troubleshooting SNMP Informant

SNMP Informant logs events to the Application Event log. Depending on your actions, and the results of queries performed by SNMP Informant, these messages will differ. *If SNMP Informant does not seem to be working, checking the Application Event Log should be one of your first courses of action.*

- You should also check the SNMP Informant Knowledge base at: <http://www.snmp-informant.com/Knowledgebase.htm>

The table below lists some troubleshooting steps to take if you find SNMP Informant is not working the way it is supposed to:

Troubleshooting Table

Problem	Check	Solution
I can't query any data from SNMP Informant.	Is the Windows SNMP Service installed?	Install the SNMP Service according to this guide.
	Is the Windows SNMP Service running?	Start the SNMP Service using the Windows Service Manager.
	Can you request any SNMP data from the SNMP service?	Check that your community names match your SNMP Manager. Check that the security settings are correct for your environment.
	Check that the Windows Application Event Log for any SNMP Informant errors or warnings.	Check the various SNMP Informant web pages for related information <ul style="list-style-type: none">• http://www.wtcs.org/informant/support.htm Check the Microsoft Windows support website for related information <ul style="list-style-type: none">• http://support.microsoft.com
	Check to see if the Windows Performance Monitor works on that computer.	Check the Microsoft Windows support website for related information <ul style="list-style-type: none">• http://support.microsoft.com
I can't query a specific SNMP Informant OID.	Check to see that you are referencing the SNMP OID correctly by using SNMP GETNEXT/WALK operations.	Use the returned SNMP OID from the GETNEXT/WALK operation.
	That performance counter may not be available on the computer/software you are using.	Check the various SNMP Informant web pages for related information <ul style="list-style-type: none">• http://www.wtcs.org/informant/support.htm Check the Microsoft Windows support website for related information <ul style="list-style-type: none">• http://support.microsoft.com
	Check that the Windows Application Event Log for any SNMP Informant errors or warnings.	Check the various SNMP Informant web pages for related information <ul style="list-style-type: none">• http://www.wtcs.org/informant/support.htm Check the Microsoft Windows support website for related information <ul style="list-style-type: none">• http://support.microsoft.com

Troubleshooting SNMP Informant Standard

If you are trying to do an SNMP GET of a particular OID, and cannot seem to get data, remember that what performance counters you *can* access all depends on the OS version where SNMP Informant is installed.

For example, Windows 2003 has performance counters that do not exist on Windows 2000, so SNMP GET requests to OIDs that map to Windows 2003 performance counters will fail on Windows 2000 systems.

The general "can I use SNMP Informant to collect data from the <insert name here> performance counter?" test is this:

Check the Performance Monitor applet (Start/Run/Perfmon) on the system you want to collect data from. If you can see the performance object and counter and instances you want (or are trying) to track, then you should be able to install SNMP Informant on that server, and (using the proper OID, of course) use SNMP to GET that data. If you are unable to see the performance object, counter and instances, then you will NOT be able to get that data using SNMP Informant.

Remember: *SNMP Informant Standard Edition does not support the full compliment of Windows performance counters as does SNMP Informant Advanced Agent.*

End of Document