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™

## Installation and Configuration Guide

Release 2008.1

SNMP
Informant
"GET more out of Windows!"
Windows SNMP support for industry standard Network Management Systems
www.snmp-informant.com

## Copyright

## 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 |
|---|---|---|---|
| 2008.1 | February 17, 2008 | GKW | Creation of Installation and Configuration Guide (complete rewrite, merging several documents to create this one). |

# 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
WMI Agents ..... 4
Custom Agents ..... 5
**System Requirements** ..... **5**
**Installation and Configuration** ..... **6**
Installing the Microsoft Windows SNMP service ..... 6
Configuring the Microsoft SNMP service ..... 6
Installing SNMP Informant ..... 7
GUI Installation ..... 7
Command Line Installation ..... 13
Configuring SNMP Informant ..... 15
Registry Settings and their Meanings ..... 16
Using SNMP Informant ..... 20
General Usage Notes ..... 20
Using the PDH Agents (Advanced/Application Plus Packs) ..... 21
Using the WMI-Exchange agent ..... 25
Using the WMI-OS agent ..... 30
Using the MSCS Agent ..... 32
Common SNMP Informant OIDs ..... 33
**Troubleshooting SNMP Informant** ..... **35**
Troubleshooting Table ..... 35
Troubleshooting PDH agents ..... 36
Troubleshooting WMI agents ..... 36

# Table of Figures

**Figure 1 – SNMP Informant Functional Overview** ..... 3
**Figure 2 – SNMP Informant Application Structure (PDH Agents)** ..... 3
**Figure 3 – SNMP Informant Application Structure (WMI Agents)** ..... 4
**Figure 4 – SNMP Informant Application Structure (WMI Agents with helper service)** ..... 5
**Figure 5 – Anatomy of an SNMP Informant OID** ..... 21

# 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.

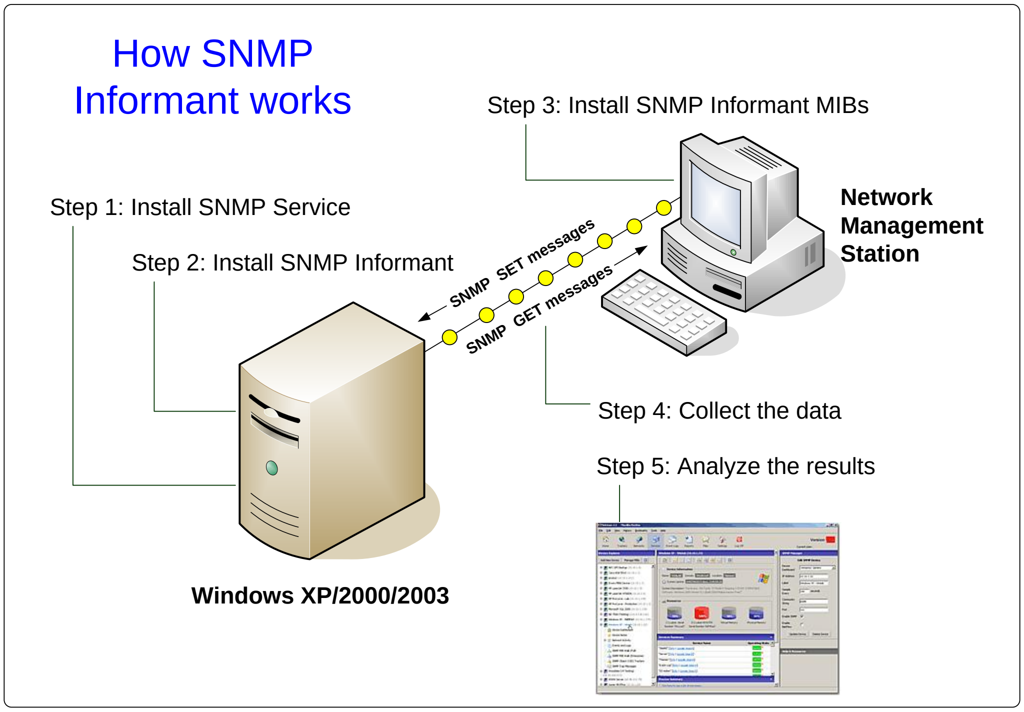

How SNMP Informant works
Step 3: Install SNMP Informant MIBs
Step 1: Install SNMP Service
Step 2: Install SNMP Informant
Network Management Station
SNMP SET messages
SNMP GET messages
Step 4: Collect the data
Step 5: Analyze the results
Windows XP/2000/2003

**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.

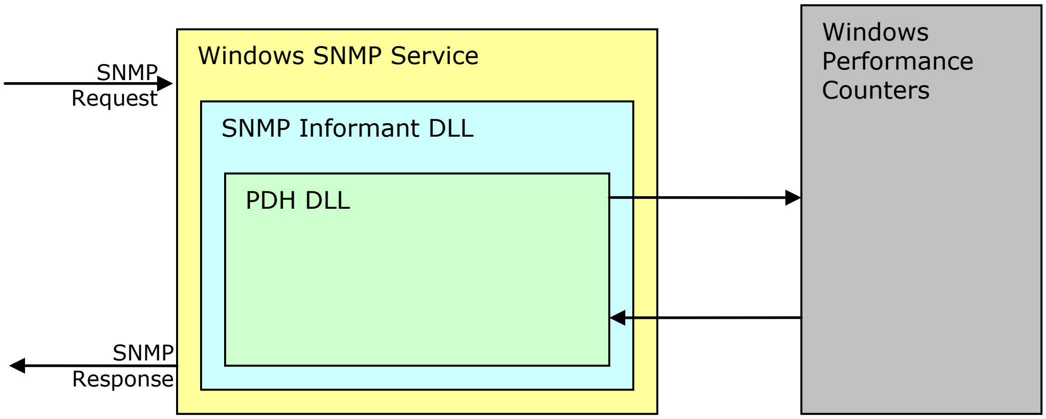


**Figure 2 – SNMP Informant Application Structure (PDH Agents)**

### 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.

### Application Plus Pack Specific Notes

Each Application Plus Pack extends SNMP Informant to support OIDs that allow you to query application specific performance counters using SNMP. *Application Plus Packs require that the SNMP Informant Advanced Agent be installed**.* You can install as many Application Plus Packs as you want.

** The SNMP Informant Premium Bundle removes this limitation.

## WMI Agents

Similar to the PDH agents, SNMP Informant WMI agents make data requests to the local WMI sub-system on the system where SNMP Informant is installed. See Figure 2 on the following page for a diagram representing the data flow for this type of agent.

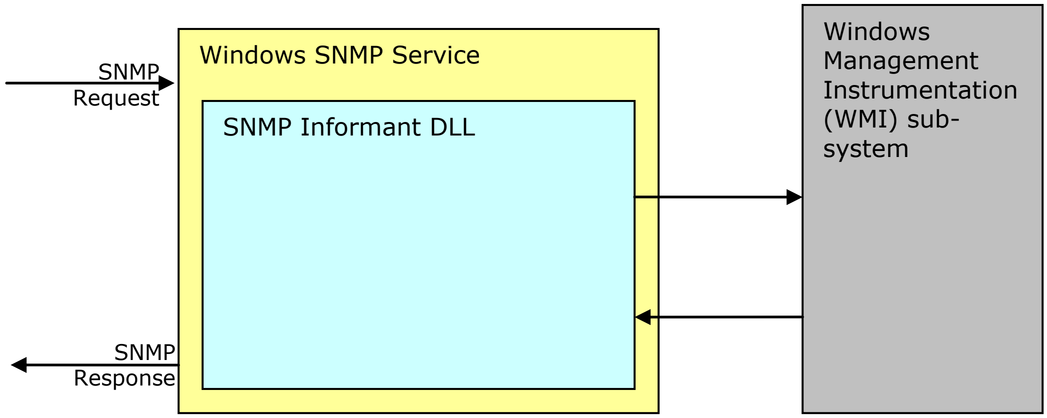


**Figure 3 – SNMP Informant Application Structure (WMI Agents)**

The SNMP Informant WMI-OS and WMI-Exchange agents incorporate the use of a “helper service”. This helper service sits between the extension agent DLL and the WMI sub-system.

SNMP requests are received (by the SNMP service) from the NMS for OIDs that are derived from a WMI class, and passed from the SNMP Informant extension agent DLL to the helper service. Then, the helper service passes (proxies) that request to the WMI sub-system, and waits for a response.

When a response is received, the helper service passes it back to the extension DLL, and the extension DLL passes it back to the SNMP service. Figure 3 below illustrates this data flow.

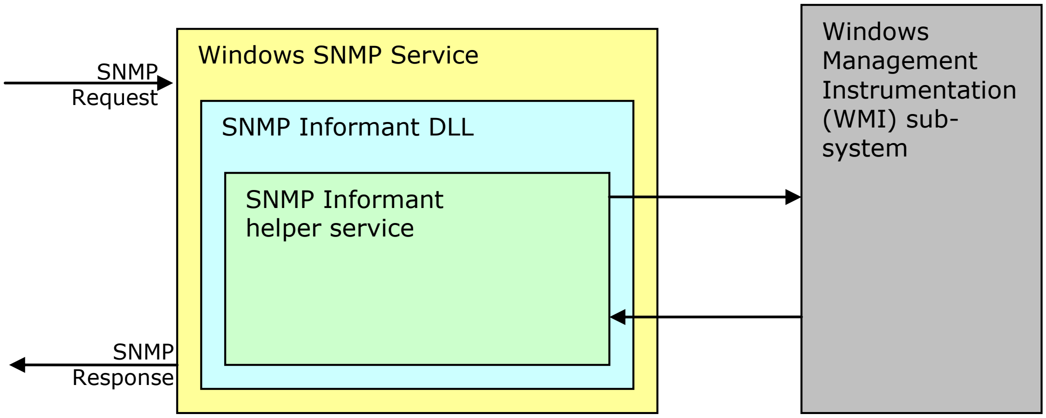

SNMP Request
Windows SNMP Service
SNMP Informant DLL
SNMP Informant helper service
SNMP Response
Windows Management Instrumentation (WMI) sub-system

**Figure 4 – SNMP Informant Application Structure (WMI Agents with helper service)**

### WMI-HW Specific Notes

The SNMP Informant WMI-HW Agent allows SNMP access to low level information on motherboards, hard drives, power supplies, etc.

*Note:* This agents' functionality will differ depending on motherboard hardware manufacturers' support for the Windows 2000 and 2003 WMI system.

## Custom Agents

SNMP Informant includes custom support for Microsoft Cluster Services and through APIs published for those products.

# 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/ia64)
- Microsoft Windows 2003, Enterprise Edition (x86/x64/ia64)
- Microsoft Windows 2003, Datacenter Edition (x86/x64/ia64)
- Microsoft Windows 2003, Web Edition (x86/x64/ia64)
- Microsoft Windows 2003, Small Business Server (x86/x64/ia64)
- Microsoft Window 2008, Standard Edition (x86/x64/ia64)
- Microsoft Window 2008, Enterprise Edition (x86/x64/ia64)

SNMP Informant Advanced Agents requires a minimum of a Pentium II class processor, 32 MB of available memory and 30MB of available disk space.

# 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 be 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 be 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:

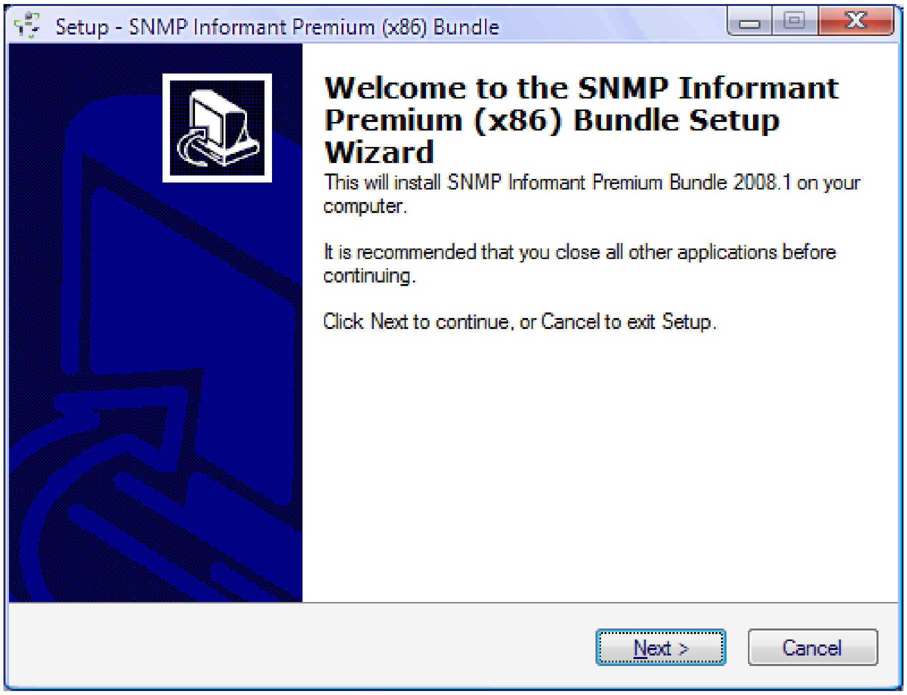
- Graphic user interface (GUI) – A graphics wizard based installation requiring input from the user either with the mouse and keyboard.
- Command line interface – An interface where you can install the software without any intervention from the user. Also known as an unattended install.

For the purposes of documentation, this section will illustrate the installation of the SNMP Informant Premium Bundle, which includes all SNMP Informant software. Individual installs of various SNMP Informant agents will differ somewhat, and specific requirements will be noted.

## GUI Installation

Start the informant executable.

Click the Next button in the welcome screen. The installer will detect whether or not the host OS is a 32 or 64 bit version. Click Next.



Setup - SNMP Informant Premium (x86) Bundle

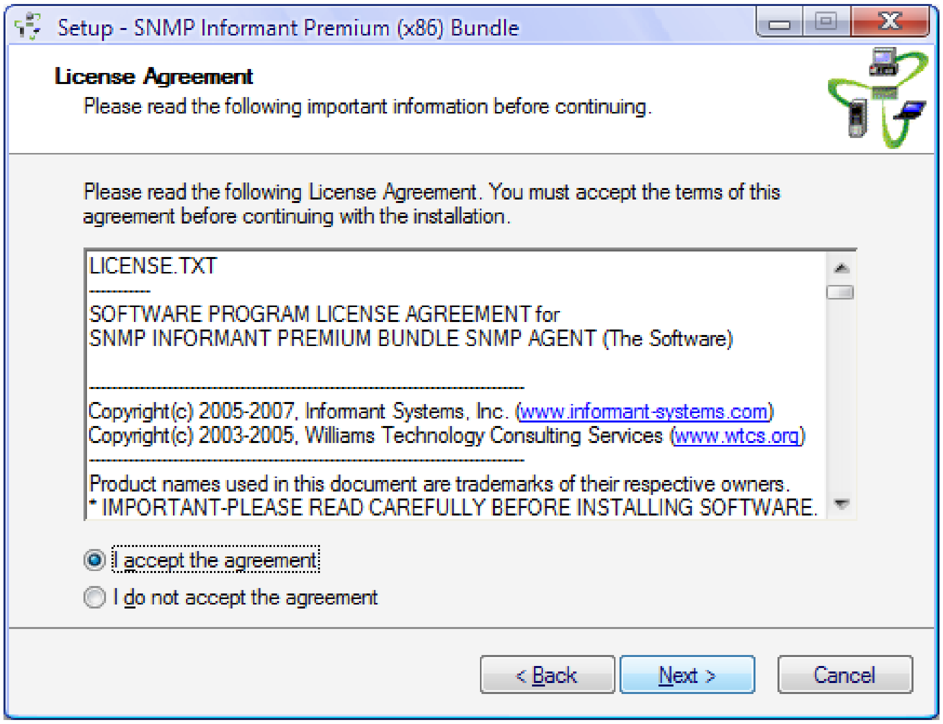
**Welcome to the SNMP Informant Premium (x86) Bundle Setup Wizard**

This will install SNMP Informant Premium Bundle 2008.1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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



Setup - SNMP Informant Premium (x86) Bundle

**License Agreement**

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

LICENSE.TXT

-----------

SOFTWARE PROGRAM LICENSE AGREEMENT for
SNMP INFORMANT PREMIUM BUNDLE SNMP AGENT (The Software)

--------------------------------------------------------------------------

Copyright(c) 2005-2007, Informant Systems, Inc. (www.informant-systems.com)
Copyright(c) 2003-2005, Williams Technology Consulting Services (www.wtcs.org)

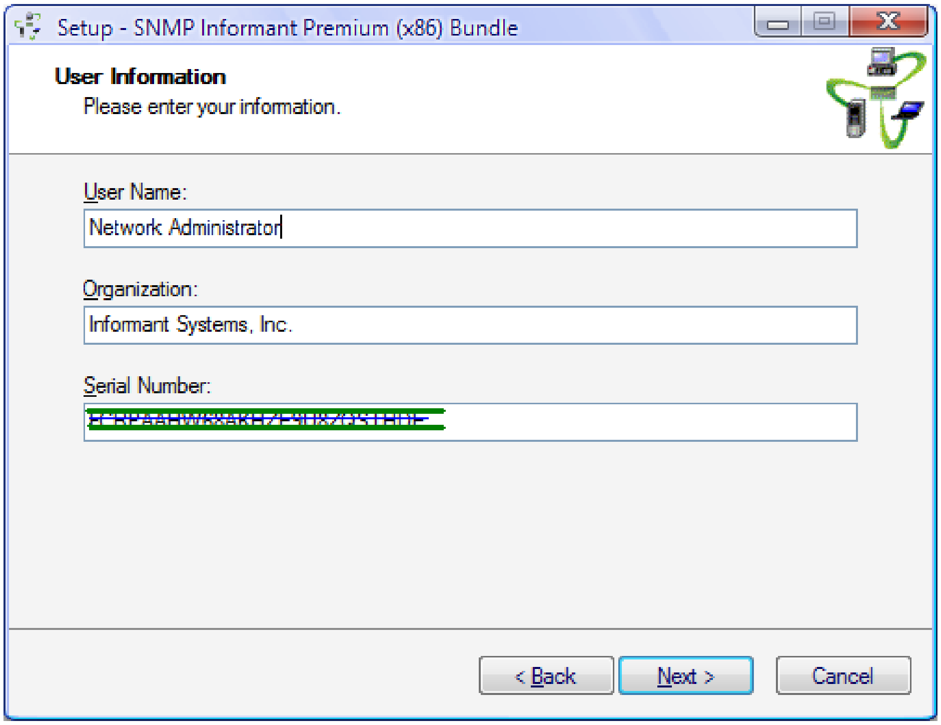
--------------------------------------------------------------------------

Product names used in this document are trademarks of their respective owners.
* IMPORTANT-PLEASE READ CAREFULLY BEFORE INSTALLING SOFTWARE.

● I accept the agreement

○ I do not accept the agreement

Enter your registration information and the Serial Number/Validation Key supplied with your product. Click the Next button after entering the correct Serial Number/Validation Key.



Setup - SNMP Informant Premium (x86) Bundle

**User Information**

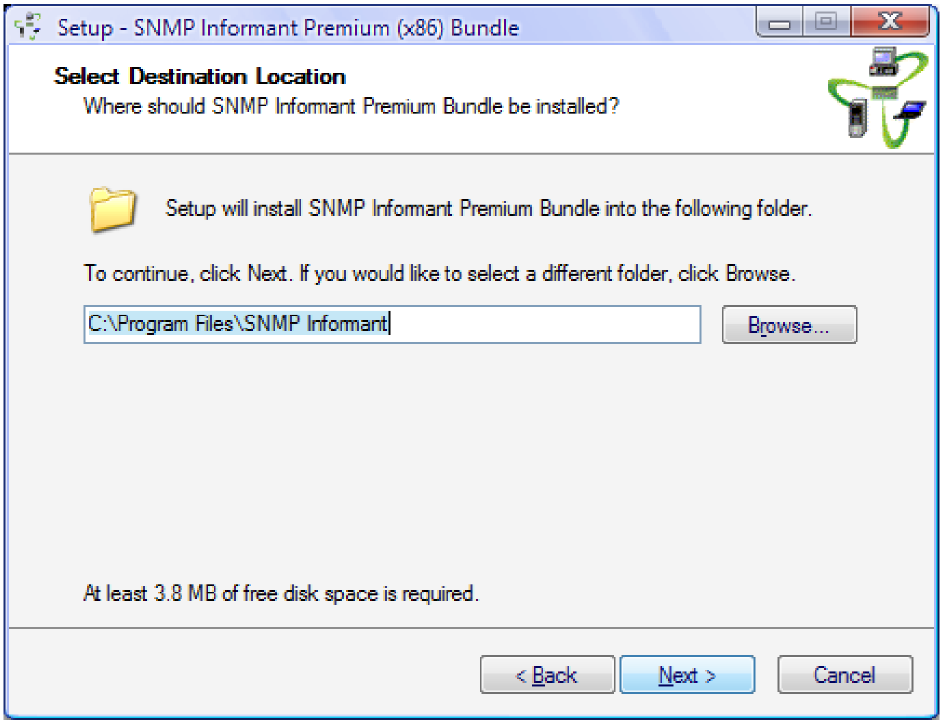
Please enter your information.

User Name: Network Administrator

Organization: Informant Systems, Inc.

Serial Number: [redacted]

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



**Select Destination Location**

Where should SNMP Informant Premium Bundle be installed?

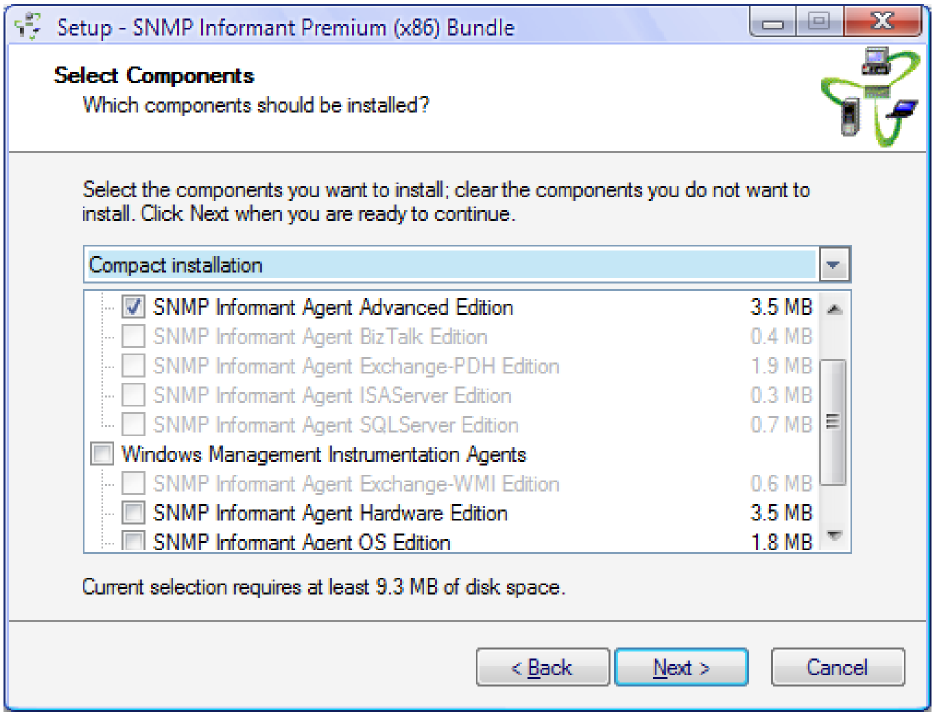
Setup will install SNMP Informant Premium Bundle into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\SNMP Informant

At least 3.8 MB of free disk space is required.

Select the components you would like to install.  If you are installing an individual agent, you will not be prompted.



**Select Components**

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

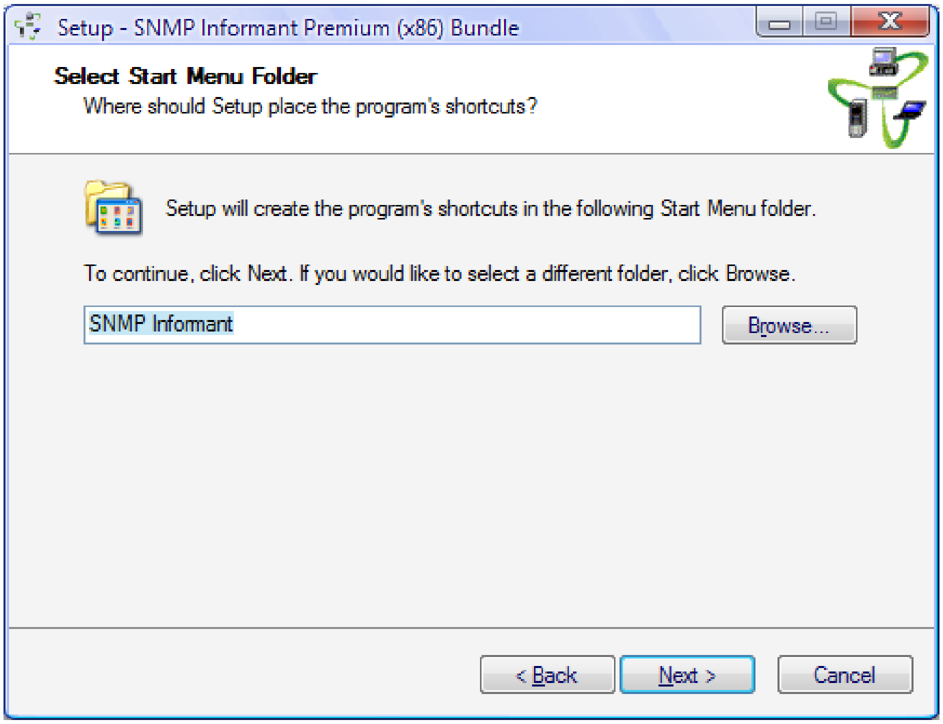
Compact installation

| | |
|---|---|
| ☑ SNMP Informant Agent Advanced Edition | 3.5 MB |
| □ SNMP Informant Agent BizTalk Edition | 0.4 MB |
| □ SNMP Informant Agent Exchange-PDH Edition | 1.9 MB |
| □ SNMP Informant Agent ISAServer Edition | 0.3 MB |
| □ SNMP Informant Agent SQLServer Edition | 0.7 MB |
| □ Windows Management Instrumentation Agents | |
| □ SNMP Informant Agent Exchange-WMI Edition | 0.6 MB |
| □ SNMP Informant Agent Hardware Edition | 3.5 MB |
| □ SNMP Informant Agent OS Edition | 1.8 MB |

Current selection requires at least 9.3 MB of disk space.

If you are installing the Premium Bundle, the installer will check to see what support exists for various component items.  If items are greyed out, it is because SNMP Informant has determined that installing the agent for that component is not applicable. For example, if SQL Server is not installed on the server where SNMP Informant is being installed, then the SQL Server component will be greyed out.

Enter the name of the menu under the Start Menu Folder. Click the Next button.



**Select Start Menu Folder**

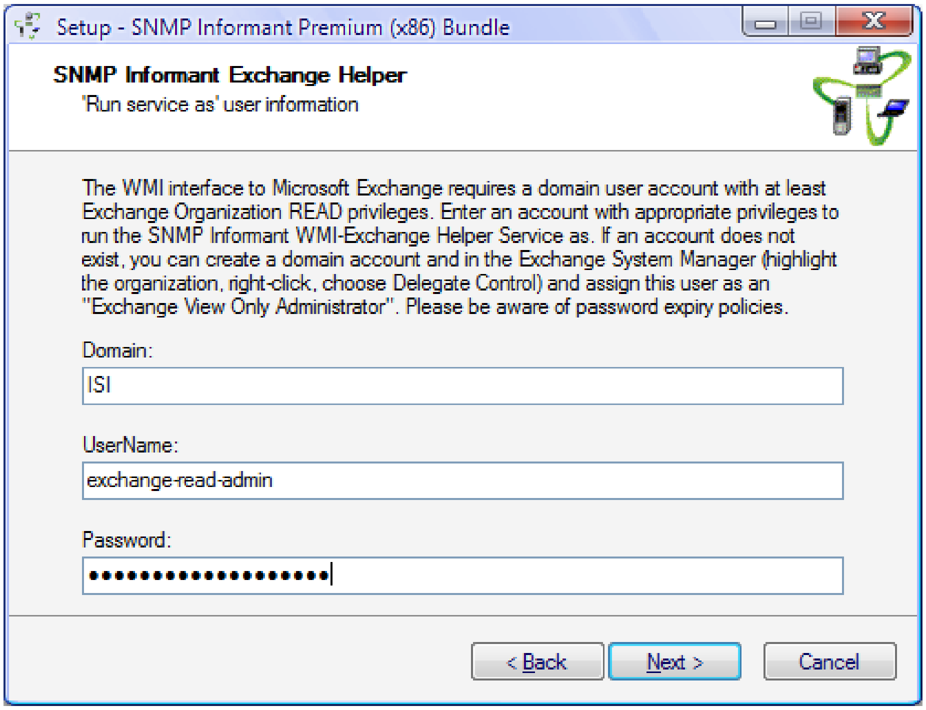
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

SNMP Informant

If you are installing the Exchange WMI Edition agent, you will be prompted for a domain account to start the SNMP Informant Exchange Helper Service.  Enter a valid domain user that has delegated Exchange View Only Administrator privileges at least.



**SNMP Informant Exchange Helper**

'Run service as' user information

The WMI interface to Microsoft Exchange requires a domain user account with at least Exchange Organization READ privileges. Enter an account with appropriate privileges to run the SNMP Informant WMI-Exchange Helper Service as. If an account does not exist, you can create a domain account and in the Exchange System Manager (highlight the organization, right-click, choose Delegate Control) and assign this user as an "Exchange View Only Administrator". Please be aware of password expiry policies.

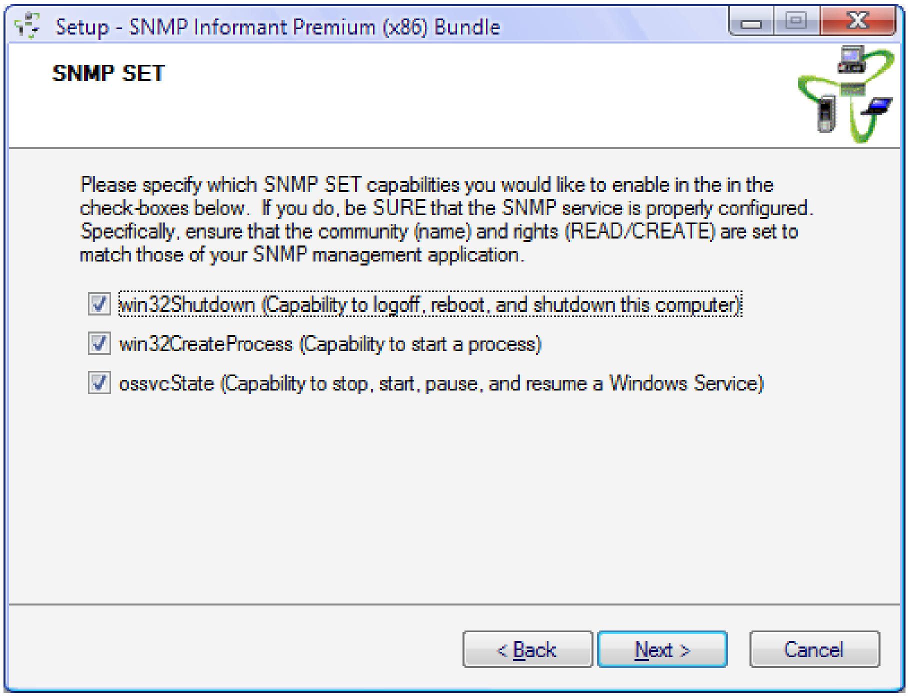
Domain: ISI

UserName: exchange-read-admin

Password: ••••••••••••••••••••

For more information about configuring Exchange 2003 and SNMP Informant, see "Using SNMP Informant"

If you are installing the WMI-OS Agent, you will be prompted for SNMP SET functionality you desire to activate within SNMP Informant.



SNMP SET

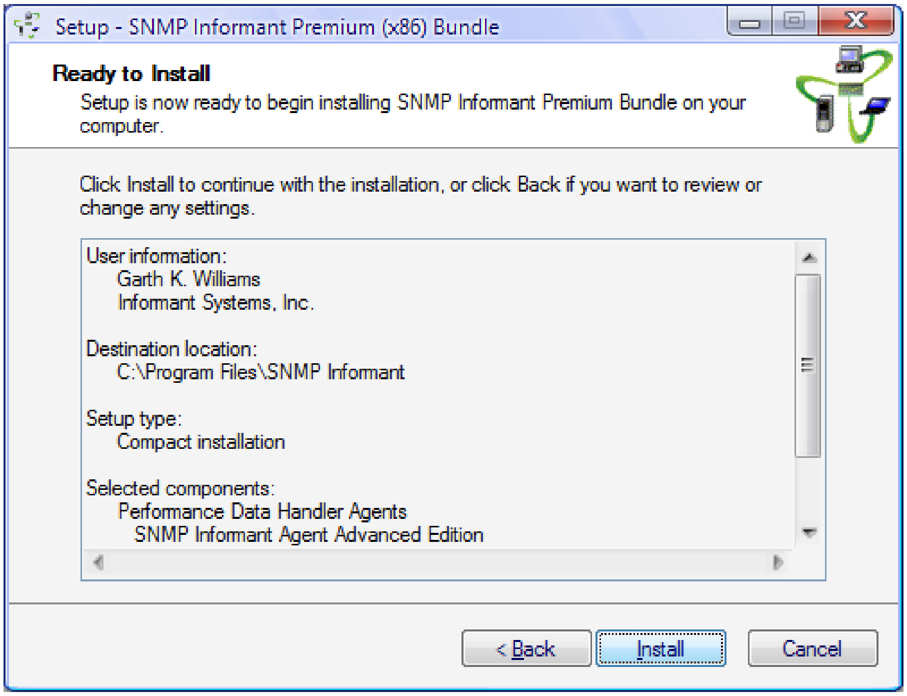
Please specify which SNMP SET capabilities you would like to enable in the in the check-boxes below. If you do, be SURE that the SNMP service is properly configured. Specifically, ensure that the community (name) and rights (READ/CREATE) are set to match those of your SNMP management application.

☑ win32Shutdown (Capability to logoff, reboot, and shutdown this computer)

☑ win32CreateProcess (Capability to start a process)

☑ ossvcState (Capability to stop, start, pause, and resume a Windows Service)

Verify the installation parameters and click the Install button.



Ready to Install

Setup is now ready to begin installing SNMP Informant Premium Bundle on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

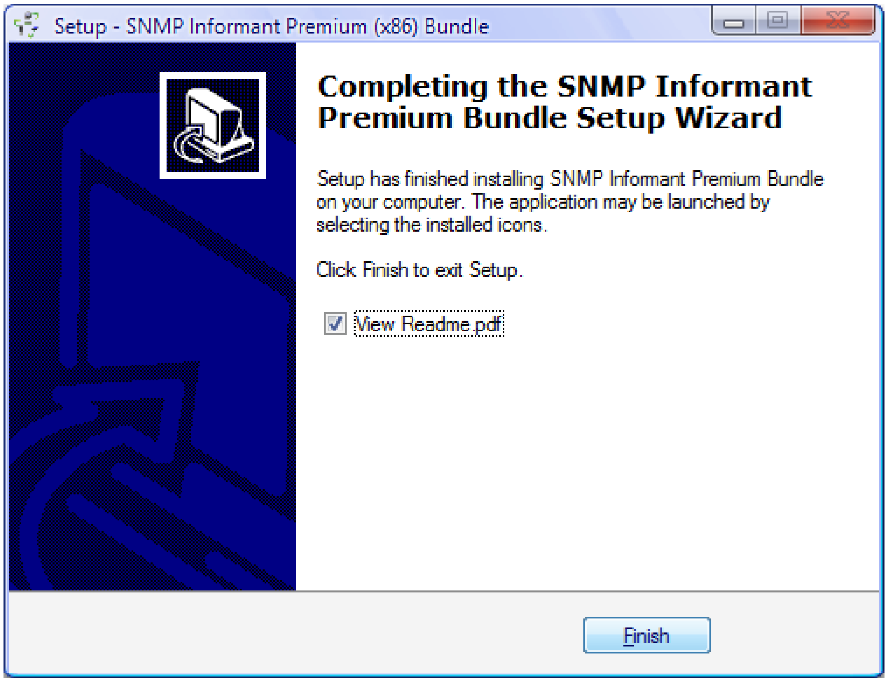
```
User information:
    Garth K. Williams
    Informant Systems, Inc.

Destination location:
    C:\Program Files\SNMP Informant

Setup type:
    Compact installation

Selected components:
    Performance Data Handler Agents
      SNMP Informant Agent Advanced Edition
```

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.



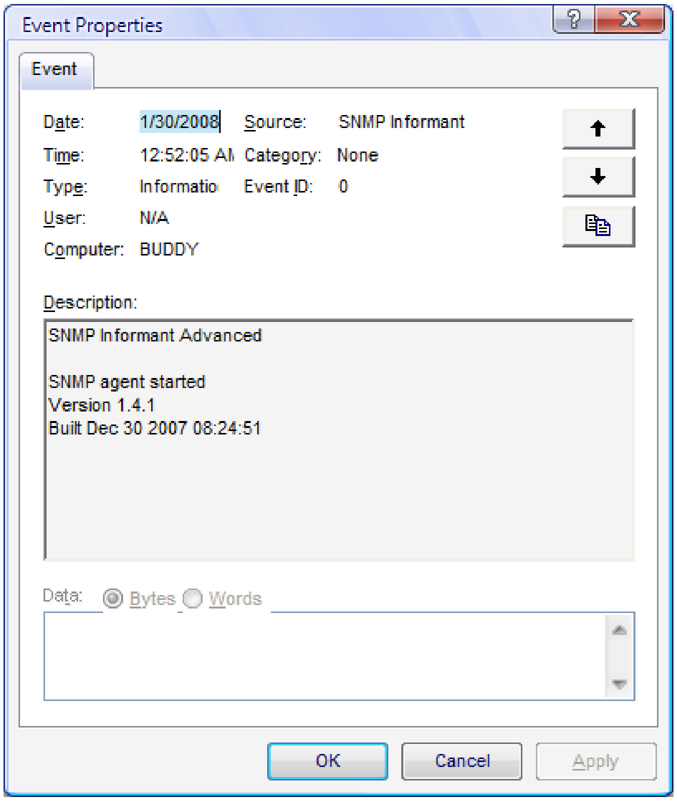
Completing the SNMP Informant Premium Bundle Setup Wizard

Setup has finished installing SNMP Informant Premium Bundle on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ View Readme.pdf

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. Each component of SNMP Informant will add its own startup message to the Application Event log.



Date: 1/30/2008 Source: SNMP Informant
Time: 12:52:05 AM Category: None
Type: Informatio Event ID: 0
User: N/A
Computer: BUDDY

Description:

```
SNMP Informant Advanced

SNMP agent started
Version 1.4.1
Built Dec 30 2007 08:24:51
```

Data: ● Bytes ○ Words

## 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.

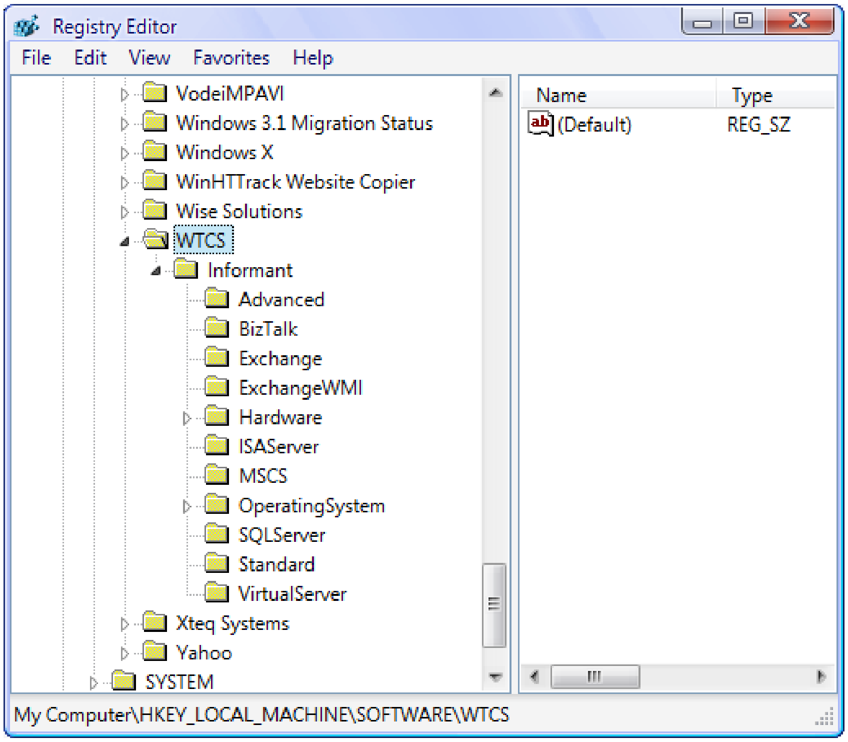
### /COMPONENTS="comma separated list of component names"

Overrides the default components settings. Using this command line parameter causes Setup to automatically select a custom type.

## 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:



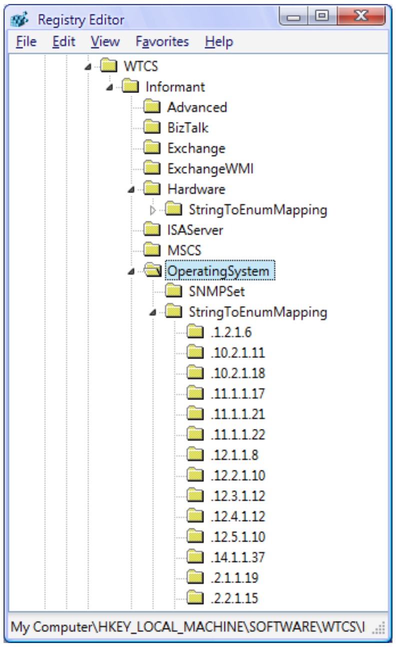
| Name | Type |
|---|---|
| (Default) | REG_SZ |

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WTCS

**Note**: on this system, SNMP Informant Standard (free) version is also 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.

**Note:** The WTCS/Informant/Hardware and WTCS/Informant/OperatingSystem keys will have sub-hives called StringToEnumMapping. **DO NOT MODIFY THESE SUB-HIVES!**



## 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 or WMI – Windows Management Instrumentation), 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/<product>. 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

**Applies to:** All Agents

**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

**Applies to:** PDH Agents (Advance, BizTalk, Exchange PDH, ISA Server, SQL Server).

**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 whenver 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

**Applies to:** PDH Agents (Advance, BizTalk, Exchange PDH, ISA Server, SQL Server).

**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

**Applies to:** PDH Agents (Advance, BizTalk, Exchange PDH, ISA Server, SQL Server).

**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 per agent. 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

**Applies to:** PDH and WMI Agents

**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.

**Setting:** GetNextInstanceTimeSpan

**Applies to:** WMI Agents (OS, Hardware, Exchange, Virtual Server)

**Registry Type:** DWORD

**Default Value:** 60000

**Units:** milliseconds

This registry setting is used to identify when to look for new instances of a WMI class. There is a performance hit whenever a new iterator is used to look for new instance of a WMI class. 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 WMI class. Setting this value to a lower value will update the iterator more often, but will do as at the expense of longer response time as a new iteration is performed.

**Setting:** GetNextRefreshRate

**Applies to:** WMI Agents (OS, Hardware, Exchange, Virtual Server)

**Registry Type:** DWORD

**Default Value:** 30000

**Units:** milliseconds

This registry setting applies only to GETNEXT query operations. It is used to determine how often the value is refreshed from a GETNEXT query. Decreasing this value with provide updates more often but at the expense of performance. A user would decrease this value if they were performing an SNMP GETNEXT/WALK less than 30 seconds between iterations.

**Setting:** MaxQueryCacheSize

**Applies to:** WMI Agents (OS, Hardware, Exchange, Virtual Server)

**Registry Type:** DWORD

**Default Value:** 1000

**Units:** Number of queries

The number of different queries that can be cached for **only** GET queries per agent. 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.

**Setting:** HelperResponseTimeout

**Applies to:** WMI-OS and WMI-Exchange Agents

**Registry Type:** DWORD

**Default Value:** 4500

**Units:** milliseconds

This registry setting applies to SNMP Informant WMI agents only, and refers to the number of milliseconds the agent (extension DLL) should wait for a response from the SNMP Informant helper service before timing out.

**Setting:** SpawnDirectory

**Applies to:** WMI-OS Agent

**Registry Type:** REG_SZ

**Default Value:** <installdirectory\spawn> (eg. C:\Program Files\SNMP Informant\operating_system\spawn\)

**Units:** alphanumeric

This registry setting tells the SNMP Informant WMI-OS agent where scripts and executables that might be remotely spawned should start from.

# Using SNMP Informant

For the most part, once the SNMP service is properly installed and configured, SNMP Informant agents are usable immediately after install. Most agents require little or no configuration at all. If you 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. The following sections discuss the OID syntax and the differences between SNMP GET and GETNEXT/WALK requests.

## General Usage Notes

### OID Tree Listings

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

- [install loc]\SNMP Informant\advanced\mibs\informant-adv-tree.txt
- [install loc]\SNMP Informant\sqlserver\mibs\informant-sqlserver-tree.txt
- [install loc]\SNMP Informant\hardware\mibs\informant-hw-tree.txt
- [install loc]\SNMP Informant\operating_system\mibs\informant-os-tree.txt
- [install loc]\SNMP Informant\ExchangeWMI\mibs\informant-exchange-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\[product]\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\[product] directory yourself after the uninstall program has completed.

## Using the PDH Agents (Advanced/Application Plus Packs)

The SNMP Informant PDH agents are 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-a9f8-09d5ebeb9ef21033.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):

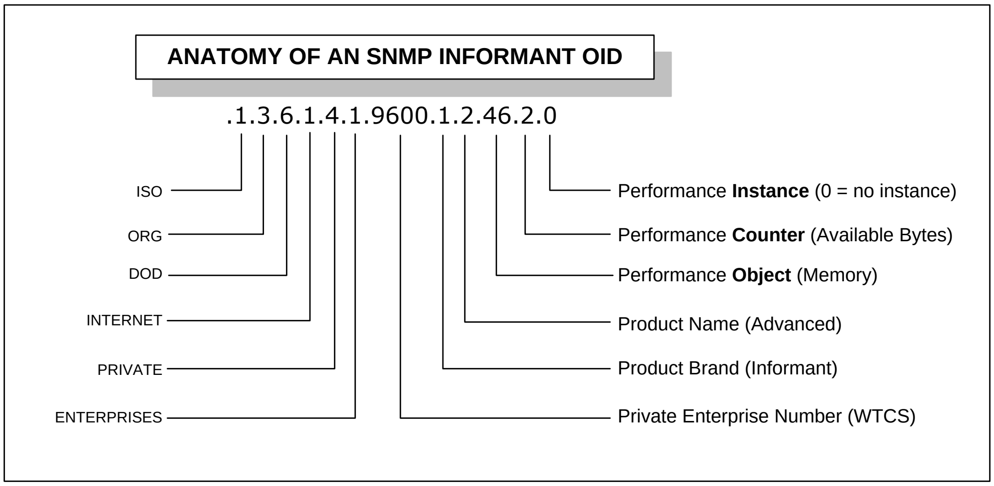

ANATOMY OF AN SNMP INFORMANT OID
.1.3.6.1.4.1.9600.1.2.46.2.0
ISO
ORG
DOD
INTERNET
PRIVATE
ENTERPRISES
Performance **Instance** (0 = no instance)
Performance **Counter** (Available Bytes)
Performance **Object** (Memory)
Product Name (Advanced)
Product Brand (Informant)
Private Enterprise Number (WTCS)

**Figure 5 – Anatomy of an SNMP Informant OID**

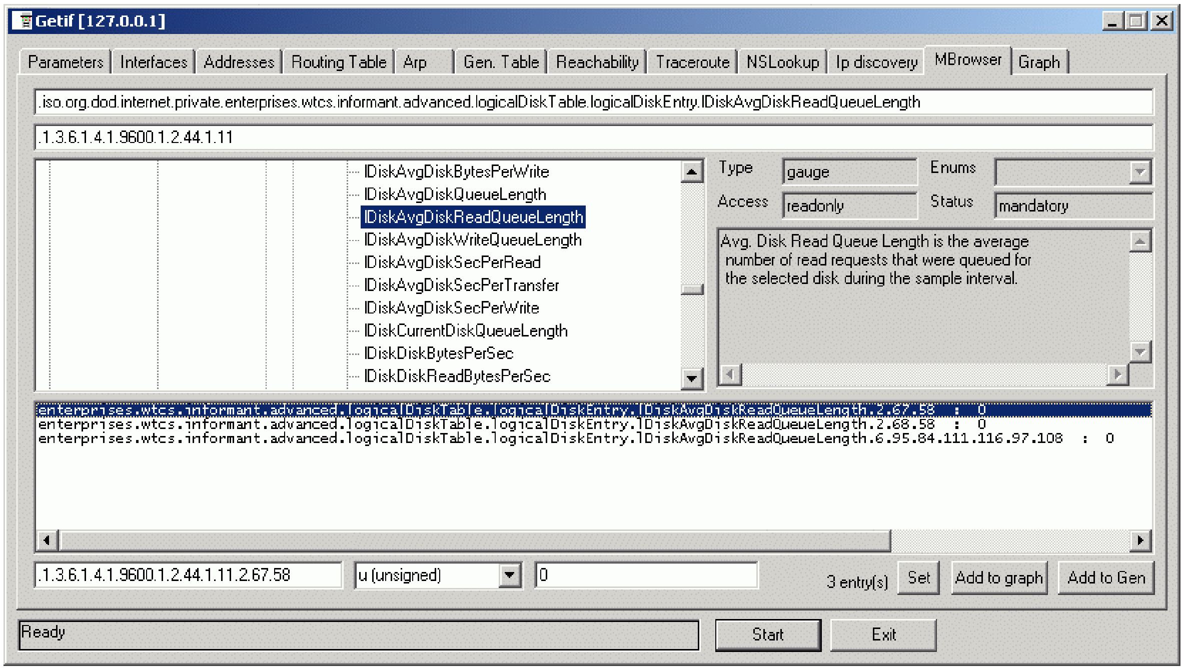
More detailed OIDs can contain instance names. For example, it is not uncommon for a server to have multiple disks, processors and network adapters. Therefore, OIDs for these performance objects will have multiple instances.

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 Advanced version, and the prefix will be .iso.org.dod.internet.private.enterprises.wtcs.informant.advanced (.1.3.6.1.4.1.9600.1.2), 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)



.iso.org.dod.internet.private.enterprises.wtcs.informant.advanced.logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength

.1.3.6.1.4.1.9600.1.2.44.1.11

Type: gauge

Access: readonly

Status: mandatory

Avg. Disk Read Queue Length is the average number of read requests that were queued for the selected disk during the sample interval.

```
enterprises.wtcs.informant.advanced.logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength.2.67.58  :  0
enterprises.wtcs.informant.advanced.logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength.2.68.58  :  0
enterprises.wtcs.informant.advanced.logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength.6.95.84.111.116.97.108  :  0
```

.1.3.6.1.4.1.9600.1.2.44.1.11.2.67.58 | u (unsigned) | 0

Ready

| Fully qualified SNMP Informant OID (walk from here) | SNMP Informant Instance (Decimal) OID response | Character (ASCII) Equivalent |
|---|---|---|
| .logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength | **.2.67.58** | **C:** |
| .logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength | **.2.68.58** | **D:** |
| .logicalDiskTable.logicalDiskEntry.lDiskAvgDiskReadQueueLength | **.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.networkInterfaceEntry.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

### Example 4: PhysicalDisk: Physical Disk Average Disk Queue Length

| Fully qualified SNMP Informant OID (walk from here) | SNMP Informant Instance (Decimal) OID response | Character (ASCII) Equivalent |
|---|---|---|
| .physicalDiskTable.physicalDiskEntry.pDiskAvgDiskQueueLength | **.4.48.32.67.58** | **0 C:** |
| .physicalDiskTable.physicalDiskEntry.pDiskAvgDiskQueueLength | **.4.49.32.68.58** | **1 D:** |
| .physicalDiskTable.physicalDiskEntry.pDiskAvgDiskQueueLength | **.6.95.84.111.116.97.108** | **_Total** |

**.4** indicates that 4 **characters** follow
**.6** indicates that 6 **characters** follow

## SNMP Informant Decimal OID instance to ASCII Character Conversion Table

| Decimal Value | Character Value | Decimal Value | Character Value | Decimal Value | Character Value | Decimal Value | Character Value |
|---|---|---|---|---|---|---|---|
| 0 | | 33 | ! | 64 | @ | 97 | a |
| 1 | | 34 | " | 65 | A | 98 | b |
| 2 | | 35 | # | 66 | B | 99 | c |
| 3 | | 36 | $ | 67 | C | 100 | d |
| 4 | | 37 | % | 68 | D | 101 | e |
| 5 | | 38 | & | 69 | E | 102 | f |
| 6 | | 39 | ' | 70 | F | 103 | g |
| 7 | | 40 | ( | 71 | G | 104 | h |
| 8 | | 41 | ) | 72 | H | 105 | i |
| 9 | | 42 | * | 73 | I | 106 | j |
| 10 | | 43 | + | 74 | J | 107 | k |
| 11 | | 44 | , | 75 | K | 108 | l |
| 12 | | 45 | - | 76 | L | 109 | m |
| 13 | | 46 | . | 77 | M | 110 | n |
| 14 | | 47 | / | 78 | N | 111 | o |
| 15 | | 48 | 0 | 79 | O | 112 | p |
| 16 | | 49 | 1 | 80 | P | 113 | q |
| 17 | | 50 | 2 | 81 | Q | 114 | r |
| 18 | | 51 | 3 | 82 | R | 115 | s |
| 19 | | 52 | 4 | 83 | S | 116 | t |
| 20 | | 53 | 5 | 84 | T | 117 | u |
| 21 | | 54 | 6 | 85 | U | 118 | v |
| 22 | | 55 | 7 | 86 | V | 119 | w |
| 23 | | 56 | 8 | 87 | W | 120 | x |
| 24 | | 57 | 9 | 88 | X | 121 | y |
| 25 | | 58 | : | 89 | Y | 122 | z |
| 26 | | 59 | ; | 90 | Z | 123 | { |
| 27 | | 60 | < | 91 | [ | 124 | \| |
| 28 | | 61 | = | 92 | \ | 125 | } |
| 29 | | 62 | > | 93 | ] | 126 | ~ |
| 30 | | 63 | ? | 94 | ^ | 127 | DEL |
| 31 | | | | 95 | _ | | |
| 32 | SPACE | | | 96 | ` | | |

🟩 = commonly seen values

## Using the WMI-Exchange agent

Exchange Server 2003 has different levels of administrative responsibility, and supports three types of administrative roles: Exchange Full Administrator, Exchange Administrator and Exchange View Only Administrator.

**Exchange Full Administrator**: This role has total control over the Exchange organization, and can delegate administrative roles to other users.

**Exchange Administrator**: This role is identical to the Exchange Full Administrator role, but the Exchange Administrator role lacks have the power to delegate administrative roles to other users.

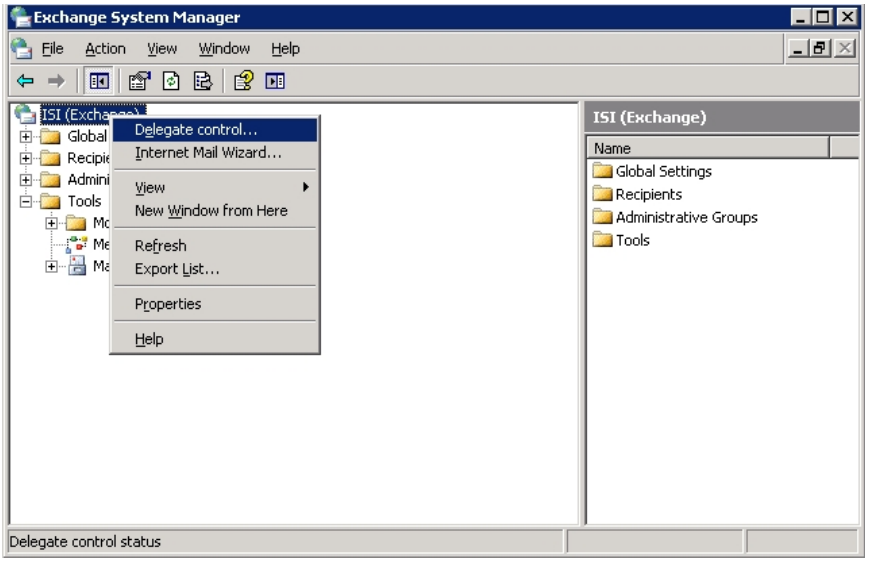
**The Exchange View Only Administrator**: In Exchange Server 2003, this role is intended for administrators to use during training. The Exchange View Only Administrator role gives administrators-in-training the ability to browse through the Exchange System Manager (ESM), but no power to make any changes.

The SNMP Informant Exchange Helper service must be configured to automatically start and run (Log On As) a user with at least Exchange View Only Administrator privileges.

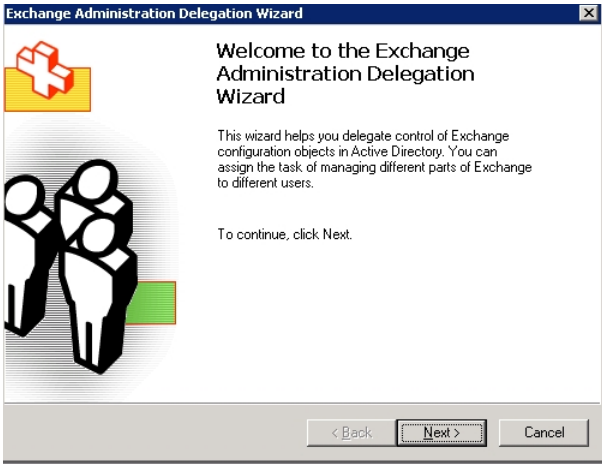
Assuming that no Exchange View Only Administrator exists, one can be created. Simply create a domain account called exchange-read-admin. Assign a password that you can remember, and set it to no expiry. While this is not optimal, if password expiry is allowed, the SNMP Informant Exchange Helper service will eventually stop working.

Next, create a domain group called Exchange-Read-Admins, and put the user you just created above in that group.

Then, start the Exchange System Manager (ESM) as a user with Exchange Full Administrator privileges. Then, select the Organization name, right click it, and choose Delegate Control.



This will start the Exchange Administration Delegation Wizard.

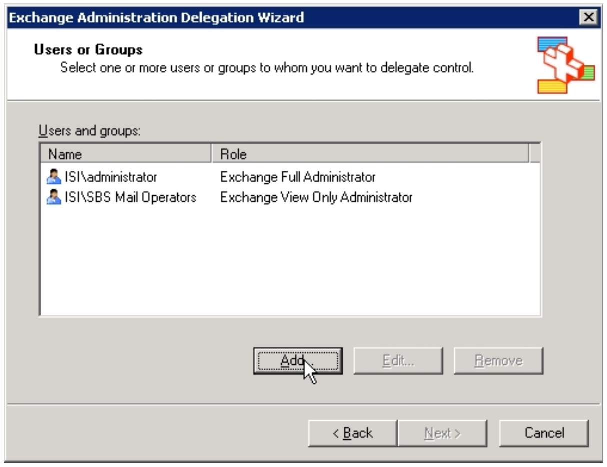

Exchange Administration Delegation Wizard

Welcome to the Exchange Administration Delegation Wizard

This wizard helps you delegate control of Exchange configuration objects in Active Directory. You can assign the task of managing different parts of Exchange to different users.

To continue, click Next.

Click Next, and add the Exchange-Read-Admins domain group you just created.

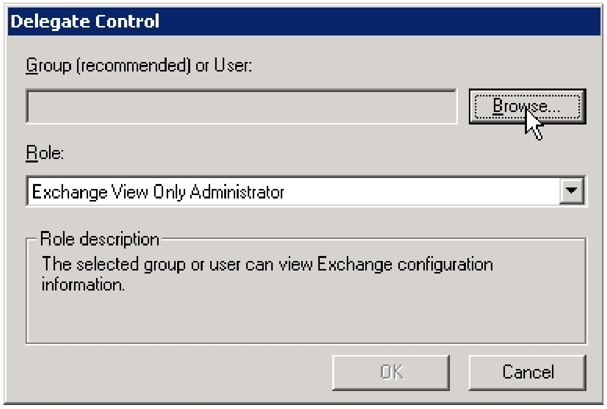

Exchange Administration Delegation Wizard

Users or Groups
Select one or more users or groups to whom you want to delegate control.

Users and groups:

| Name | Role |
|---|---|
| ISI\administrator | Exchange Full Administrator |
| ISI\SBS Mail Operators | Exchange View Only Administrator |

Click Add, then Browse

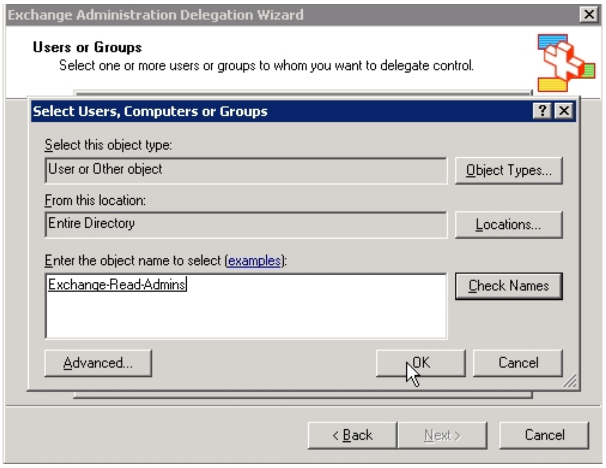

Delegate Control

Group (recommended) or User:

Role: Exchange View Only Administrator

Role description
The selected group or user can view Exchange configuration information.

Type **Exch** in the box, and press Check Names. You should then be able to pick the domain group called Exchange-Read-Admins, created earlier.



Users or Groups
Select one or more users or groups to whom you want to delegate control.

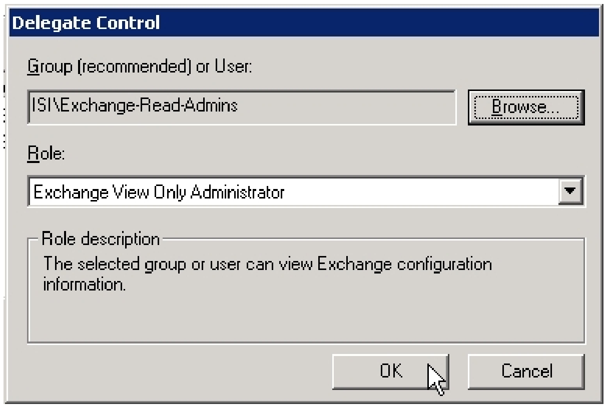
Select Users, Computers or Groups

Select this object type:
User or Other object

From this location:
Entire Directory

Enter the object name to select (examples):
Exchange-Read-Admins

Click OK.

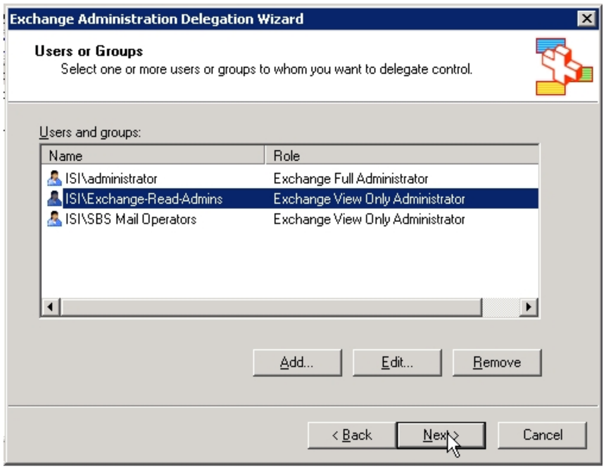


Group (recommended) or User:
ISI\Exchange-Read-Admins

Role:
Exchange View Only Administrator

Role description
The selected group or user can view Exchange configuration information.

Verify that the right group is in the Exchange View Only Administrator’s Role, and press OK.  Press Next

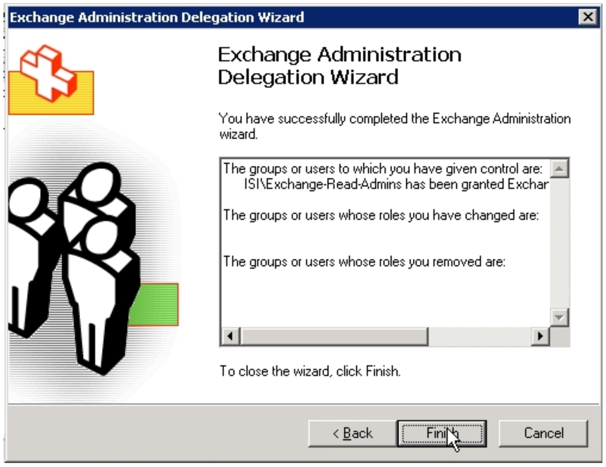


Users or Groups
Select one or more users or groups to whom you want to delegate control.

Users and groups:

| Name | Role |
|---|---|
| ISI\administrator | Exchange Full Administrator |
| ISI\Exchange-Read-Admins | Exchange View Only Administrator |
| ISI\SBS Mail Operators | Exchange View Only Administrator |

Press Finish to complete the role assignment.



Exchange Administration Delegation Wizard

You have successfully completed the Exchange Administration wizard.

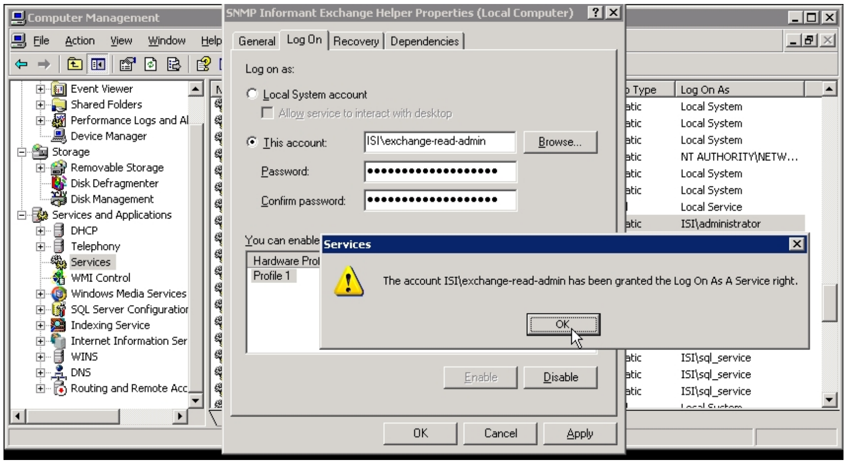
The groups or users to which you have given control are:
ISI\Exchange-Read-Admins has been granted Exchar

The groups or users whose roles you have changed are:

The groups or users whose roles you removed are:

To close the wizard, click Finish.

Now, set the SNMP Informant Exchange Helper service to start and run logged in as the exchange-read-admin account created earlier.



Log on as:

○ Local System account

□ Allow service to interact with desktop

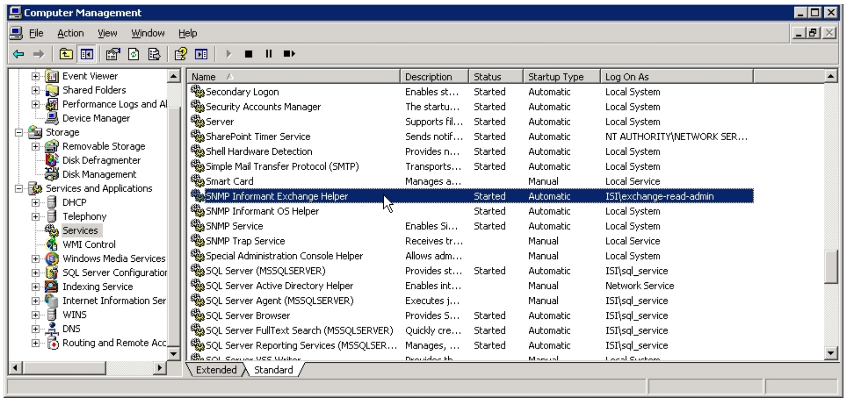
● This account: ISI\exchange-read-admin

Password: •••••••••••••••••••

Confirm password: •••••••••••••••••••

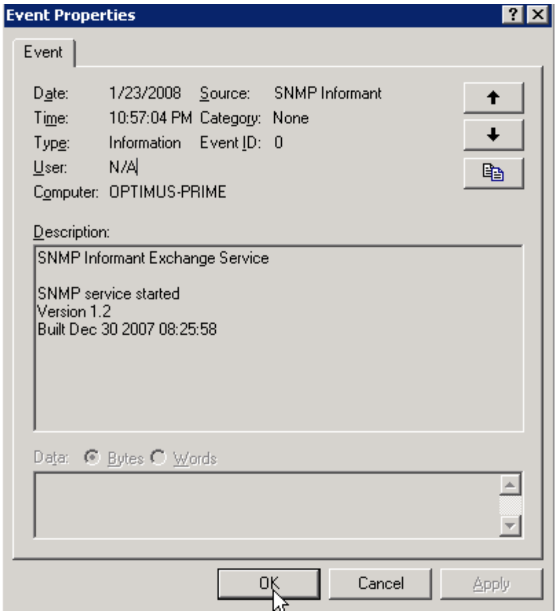
The account ISI\exchange-read-admin has been granted the Log On As A Service right.

Once you have completed the service configuration, restart the SNMP Informant Exchange Helper Service. Check to make sure it started with no error.



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Secondary Logon | Enables st... | Started | Automatic | Local System |
| Security Accounts Manager | The startu... | Started | Automatic | Local System |
| Server | Supports fil... | Started | Automatic | Local System |
| SharePoint Timer Service | Sends notif... | Started | Automatic | NT AUTHORITY\NETWORK SER... |
| Shell Hardware Detection | Provides n... | Started | Automatic | Local System |
| Simple Mail Transfer Protocol (SMTP) | Transports... | Started | Automatic | Local System |
| Smart Card | Manages a... |  | Manual | Local Service |
| SNMP Informant Exchange Helper |  | Started | Automatic | ISI\exchange-read-admin |
| SNMP Informant OS Helper |  | Started | Automatic | Local System |
| SNMP Service | Enables Si... | Started | Automatic | Local System |
| SNMP Trap Service | Receives tr... |  | Manual | Local Service |
| Special Administration Console Helper | Allows adm... |  | Manual | Local System |
| SQL Server (MSSQLSERVER) | Provides st... | Started | Automatic | ISI\sql_service |
| SQL Server Active Directory Helper | Enables int... |  | Manual | Network Service |
| SQL Server Agent (MSSQLSERVER) | Executes j... |  | Manual | ISI\sql_service |
| SQL Server Browser | Provides S... | Started | Automatic | ISI\sql_service |
| SQL Server FullText Search (MSSQLSERVER) | Quickly cre... | Started | Automatic | ISI\sql_service |
| SQL Server Reporting Services (MSSQLSER... | Manages, ... | Started | Automatic | ISI\sql_service |
| SQL Server VSS Writer | Provides th... |  | Manual | Local System |

Finally, check the Application event log for a successful start message from SNMP Informant.



Date: 1/23/2008 Source: SNMP Informant
Time: 10:57:04 PM Category: None
Type: Information Event ID: 0
User: N/A
Computer: OPTIMUS-PRIME

Description:

SNMP Informant Exchange Service

SNMP service started
Version 1.2
Built Dec 30 2007 08:25:58

## Using the WMI-OS agent

Like the WMI-Exchange agent, the WMI-OS agent also has a helper service. It includes support for SET commands sent to it from the NMS. By populating an OID with a value, and sending a SET command, you can control the WMI-OS agent.

### Win32Shutdown (.1.3.6.1.4.1.9600.1.22.8.9.0)

The win32Shutdown OID allows a user to remotely logoff, restart, or shutdown a destination computer using SNMP SET. Make sure to add the .0 to the end of the OID when setting the value. The OID must be set to an INTEGER value representing one of the following states:

| Value | Meaning |
|---|---|
| 12 | Forced Power Off |
| 8 | Power Off |
| 6 | Forced Reboot |
| 5 | Forced Shutdown |
| 4 | Forced Log Off |
| 2 | Reboot |
| 1 | Shutdown |
| 0 | Log Off |

### Win32CreateProcess (.1.3.6.1.4.1.9600.1.22.9.3.0)

The win32CreateProcess OID allows a user to remotely start a process on the destination computer using SNMP SET. Make sure to add the .0 to the end of the OID when setting the value. The OID must be set to a STRING value representing the start command you wish to run. For security reasons, the initial program can ONLY be run out of the "spawn" sub-directory below where the agent is installed on the computer (example below). You can configure the location of the spawn directory using SNMP Informant registry settings (See the "Configuring SNMP Informant" section for more information on how to do this).

C:\Program Files\SNMP Informant\operating_system\spawn\).

The initial program (in the "spawn" directory could then call or execute programs in other directories if necessary/as required.

Below are some examples of acceptable and not acceptable forms of strings for the SNMP SET command.

| Acceptable Forms |
|---|
| Start_prog.cmd |
| progA.vbs |
| mytool.exe |
| start_prog.cmd C:\winnt\system32\notepad.exe |
| mytool.exe C:\temp\input.xml |
| junk.txt |

| NON-Acceptable Forms |
|---|
| C:\winn\system32\notepad.exe |
| C:\winnt\system32\cmd /c test.cmd |
| \\computerA\c$\temp\run.exe |
| ..\..\test.cmd |

The process will be created with the user account that the SNMP service runs with, normally the SYSTEM account. If you wish to create the process a different account than what the SNMP Service is executed as, you can write a script which would run a tool like "su.exe" to execute as a different user.

By default, GUI application will not be displayed on the console window. If the GUI application must be shown, then you must enable "Allow service to interact with desktop". An administrator can do this by running the Windows Service Manager, double clicking on the SNMP Service entry, clicking on the "Log On" tab, and enabling the "Allow service to interact with desktop" checkbox, then clicking the "Okay" button, and restarting the SNMP service. Doing this will cause GUI applications started by the SNMP Informant Operating System agent to appear on the destination computer's console when executed.

### ossvcState (.1.3.6.1.4.1.9600.1.22.11.1.1.21.x)

The ossvcState OID allows a user to remotely start, stop, pause, or resume a Windows Service on the destination computer using SNMP SET. The .x at the end of the OID is the instance number of the service you wish to perform the action on. The OID must be set to an INTEGER value representing the final state you wish to put the service into. Below is a list of valid final states you can set the service to:

| Value | Meaning |
|---|---|
| 7 | Paused |
| 4 | Running (or resume) |
| 1 | Stopped |

For example, if the service is in the "stopped" state and you wish to start it, you would set the state to "running". If you would want to pause a service, you would set it to the "paused" state. If you wish to resume a service, you would set it to the "running" state.

Here's an example:

First, you need WALK the Service Caption OID (.1.3.6.1.4.1.9600.1.22.11.1.1.4) to identify the service you want to manipulate. There you will see a list of all the services identified by an instance number. Let's assume that ossvcCaption.71, or .1.3.6.1.4.1.9600.1.22.11.1.1.4.71 = Task Scheduler

Then navigate to the ossvcState OID (.1.3.6.1.4.1.9600.1.22.11.1.1.21). WALK this OID, and you will see the instance numbers again, and their current states. Find the instance number that matches the process you want to manipulate (as identified in the first step). In this example, .ossvcState.71 = running

SO … in order to stop the Task Scheduler service, you would send an SNMP SET to .1.3.6.1.4.1.9600.1.22.11.1.1.21.71 with a value of 1 (Stop).

## Using the MSCS Agent

The SNMP Informant Cluster Server Agent allows you to collect Microsoft Cluster Services information remotely using SNMP, by linking into the Cluster Services components (on your Windows 2000 or Windows 2003 cluster server, of course).

Cluster Services *must* be present on the server in order for the SNMP Informant Cluster Server Agent to install.

First, install the MSCS Informant agent on all the clustered computers. Then, when you want to collect cluster server information, query the *cluster name* rather than each computer individually. The information is redundant on all clustered computers, so by querying the cluster name, you will get the information from the active node.

Second, clustered resources are assigned to cluster groups. Whenever a cluster resource fails (e.g., a node failure or a SCSI interface failure), the entire group is moved to one of the other nodes in the cluster. Since SNMP Informant currently does not support any trap based notifications, the best way to monitor for a failure is to poll either mscsResGroupOwnerNode or mscsResourceOwnerNode. If the owner ever changes, it's usually because the owner node has shutdown/restarted, a hardware failure occurred, somebody manually moved the cluster resources through the Cluster Administrator interface, or a failback occurred. If a cluster resource has permanently failed (e.g., a permanent clustered disk failure), then you can monitor mscsResGroupState or mscsResourceState for this failure.

The "State" OIDs will not pick up transient changes (e.g., a resource group moving from one computer to another successfully) unless you poll at a fairly high frequency. You can also monitor mscsNodeState to see if a specific cluster node is up or down.

## Common SNMP Informant OIDs

The following table lists some common SNMP Informant OIDs which can be used to monitor different types of Windows Servers.

| Category | Performance Counter | SNMP Informant Agent Required | SNMP Informant OID (with comments where applicable) |
|---|---|---|---|
| **Exchange Server** | SMTP Server\Categorizer Queue Length | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**70**.6.95.84.111.116.97.108 (_Total) |
| | SMTP Server\Local Queue Length | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**81**.6.95.84.111.116.97.108 (_Total) |
| | SMTP Server\Remote Queue Length | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**110**.6.95.84.111.116.97.108 (_Total) |
| (see SMTP Notes below) | SMTP Server\Messages Delivered/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**93**.6.95.84.111.116.97.108 (_Total) |
| | SMTP Server\Messages Received/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**96**.6.95.84.111.116.97.108 (_Total) |
| | SMTP Server\Messages Sent/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.76.1.**101**.6.95.84.111.116.97.108 (_Total) |
| | | | |
| | MSExchangeIS Mailbox\Receive Queue Length | Exchange Server Application Plus Pack | |
| | MSExchangeIS Mailbox\Send Queue Length | Exchange Server Application Plus Pack | |
| | MSExchangeIS Mailbox\Folder Opens/sec | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.15.1.**6**.6.95.84.111.116.97.108 (_Total) |
| | MSExchangeIS Mailbox\Message Opens/sec | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.15.1.**18**.6.95.84.111.116.97.108 (_Total) |
| | MSExchangeIS Mailbox\Local Delivery Rate | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.15.1.**16**.6.95.84.111.116.97.108 (_Total) |
| | MSExchangeIS Public\Receive Queue Size | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.16.1.**27**.6.95.84.111.116.97.108 (_Total) |
| | MSExchangeIS Public\Send Queue Size | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.16.1.**45**.6.95.84.111.116.97.108 (_Total) |
| | MSExchangeIS\RPC Operations/sec | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.14.68.0 |
| (see Exchange Notes below) | MSExchangeIS\RPC Requests | Exchange Server Application Plus Pack | .1.3.6.1.4.1.9600.1.5.14.70.0 |
| | | | |
| **SQL Server** | SQLServer:Buffer Manager\Buffer cache hit ratio | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.22.1.6.**x** (where x increments per SQL instance) |
| | SQLServer:Buffer Manager\Page reads/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.22.1.14.**x** (where x increments per SQL instance) |
| (see SQL Notes below) | SQLServer:Buffer Manager\Page writes/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.22.1.15.**x** (where x increments per SQL instance) |
| | SQLServer:Cache Manager\Cache Hit Ratio | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.24.1.2.1.6.95.84.111.116.97.108 (_Total) |
| | SQLServer:Databases\Active Transactions | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.27.1.2.1.6.95.84.111.116.97.108 (_Total) |
| | SQLServer:Databases\Transactions/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.27.1.32.1.6.95.84.111.116.97.108 (_Total) |
| | SQLServer:General Statistics\User Connections | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.29.1.17.**x** (where x increments per SQL instance) |
| | SQLServer:General Statistics\Logins/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.29.1.4.**x** (where x increments per SQL instance) |
| | SQLServer:General Statistics\Logouts/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.29.1.5. **x** (where x increments per SQL instance) |
| | SQLServer:Memory Manager\Total Server Memory (KB) | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.32.1.13. **x** (where x increments per SQL instance) |
| | SQLServer:Memory Manager\SQL Cache Memory (KB) | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.32.1.12. **x** (where x increments per SQL instance) |
| | SQLServer:Locks\Lock Requests/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.31.1.1.1.6.95.84.111.116.97.108 (_Total) |
| | SQLServer:Locks\Average Wait Time(ms) | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.31.1.2.1.6.95.84.111.116.97.108 (_Total) |
| | SQLServer:SQL Statistics\Batch Requests/sec | SQL Server Application Plus Pack | .1.3.6.1.4.1.9600.1.3.39.1.2. **x** (where x increments per SQL instance) |

| Category | Performance Counter | SNMP Informant Agent Required | SNMP Informant OID (with comments where applicable) |
|---|---|---|---|
| **Active Directory** | NTDS\DS Threads in Use | Advanced Agent | .1.3.6.1.4.1.9600.1.2.55.88.0 |
| | NTDS\LDAP Client Sessions | Advanced Agent | .1.3.6.1.4.1.9600.1.2.55.94.0 |
| | NTDS\LDAP Searches/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.55.95.0 |
| | NTDS\DRA Inbound Bytes Total/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.55.22.0 |
| | NTDS\DRA Outbound Bytes Total/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.55.40.0 |
| | | | |
| **IIS Web**<br>(see IIS Notes below) | Web Service\Connection Attempts/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.86.1.**7**.6.95.84.111.116.97.108 (_Total) |
| | Web Service\Current Connections | Advanced Agent | .1.3.6.1.4.1.9600.1.2.86.1.**14**.6.95.84.111.116.97.108 (_Total) |
| | Web Service\Logon Attempts/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.86.1.**27**.6.95.84.111.116.97.108 (_Total) |
| | Web Service\Bytes Received/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.86.1.**3**.6.95.84.111.116.97.108 (_Total) |
| | Web Service\Bytes Sent/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.86.1.**4**.6.95.84.111.116.97.108 (_Total) |
| | | | |
| **IIS FTP**<br>(see IIS Notes below) | FTP Service\Bytes Sent/sec | Advanced Agent | .1.3.6.1.4.1.9600.1.2.23.1.**3**.6.95.84.111.116.97.108 (_Total) |
| | FTP Service\Current Connections | Advanced Agent | .1.3.6.1.4.1.9600.1.2.23.1.**6**.6.95.84.111.116.97.108 (_Total) |
| | FTP Service\Total Logon Attempts | Advanced Agent | .1.3.6.1.4.1.9600.1.2.23.1.**17**.6.95.84.111.116.97.108 (_Total) |
| | | | |

**SMTP Service Notes:** SMTP service counters support all named SMTP server instances as created. The first number after the bolded number indicates the number of characters in the named instance, and the remaining numbers are ASCII representations of the characters in the name. For example, .6.95.84.111.116.97.108 means that **6 numbers follow**, and that they (in ASCII) spell out **_Total**. To find out the instance name and the numbers that follow the bolded number, walk OID .1.3.6.1.4.1.9600.1.2.76.1.1.

**Exchange Notes:** Exchange counters support all named Storage Group names as created. The first number after the bolded number indicates the number of characters in the Storage Group Name, and the remaining numbers are ASCII representations of the characters in the name. For example, .6.95.84.111.116.97.108 means that **6 numbers follow**, and that they (in ASCII) spell out **_Total**. To find out the Storage Group name, and the numbers that follow the bolded number, walk OID .1.3.6.1.4.1.9600.1.5.15.1.1.

**SQL Notes:** Walk OID .1.3.6.1.4.1.9600.1.3.16.1.2 to determine what instance number (**x**) matches what database instance number.

**IIS Notes:** IIS Web and FTP counters support all named Web and FTP instances as created. The first number after the bolded number indicates the number of characters in the named instance, and the remaining numbers are ASCII representations of the characters in the name. For example, .6.95.84.111.116.97.108 means that **6 numbers follow**, and that they (in ASCII) spell out **_Total**.

# 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.<br>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<br>• http://www.wtcs.org/informant/support.htm<br>Check the Microsoft Windows support website for related information<br>• 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<br>• 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<br>• http://www.wtcs.org/informant/support.htm<br>Check the Microsoft Windows support website for related information<br>• 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<br>• http://www.wtcs.org/informant/support.htm<br>Check the Microsoft Windows support website for related information<br>• http://support.microsoft.com |

## Troubleshooting PDH agents

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.

## Troubleshooting WMI agents

As in the Performance Counters, what WMI classes you can access also depends on the OS/product version where SNMP Informant is installed. For example, Windows 2003 may have WMI classes and objects that do not exist on Windows 2000, so SNMP GET requests to OIDs that map to Windows 2003 WMI classes will fail on Windows 2000 systems. The same applies to the WMI-HW and WMI-Exchange agents.

In order to install successfully, all SNMP Informant WMI Agents requires that the Windows WMI Service is properly installed and configured. A default installation of the Windows WMI service is usually sufficient for SNMP Informant WMI agents to install successfully.

The general "can I access the <insert name here> WMI class?" test is this:

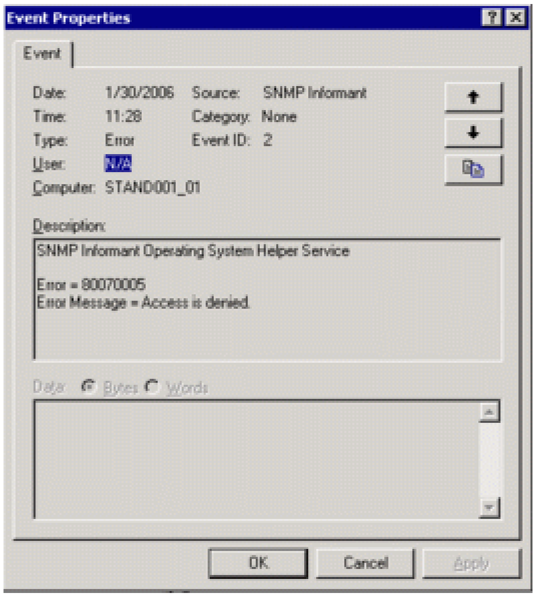
Check to see if the WMI class and object is available using a tool such as the **WMI Object Browser**. You can get this tool as part of the free "WMI Tools" download from Microsoft at: https://www.ms2.cn/downloads/details.aspx?FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314&DisplayLang=en

If you see the WMI classes and objects 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 WMI classes and objects, then you will NOT be able to get that data using SNMP Informant.

### A note about the "No endpoint mapper available" message in the Application Event Log:

The SNMP Informant WMI-OS, and WMI-Exchange agents install a separate SNMP Informant "helper" service to connect to the WMI subsystem using RPC/DCOM. Sometimes this connection cannot be completed, and the error log might get filled with messages like:

```
SNMP Informant Operating System Helper Service
Error = 80070005
Error Message = Access is denied
```



Date: 1/30/2006 Source: SNMP Informant
Time: 11:28 Category: None
Type: Error Event ID: 2
User: N/A
Computer: STAND001_01

Description:

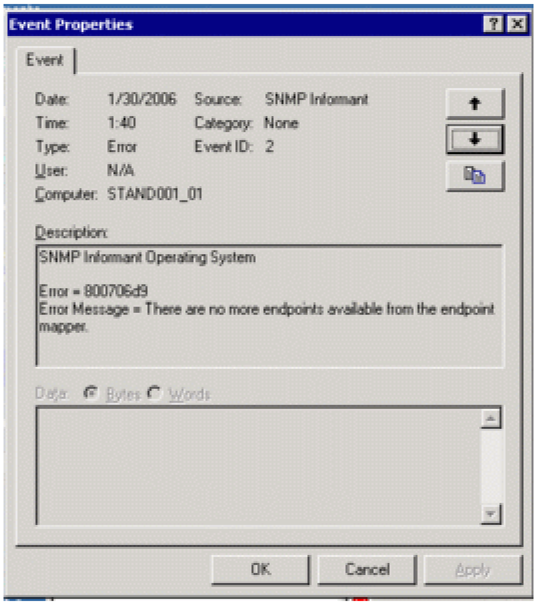
SNMP Informant Operating System Helper Service

Error = 80070005
Error Message = Access is denied.

Data: ● Bytes ○ Words

and this ...

**SNMP Informant Operating System**
**Error = 800706d9**
**Error Message = There are no more endpoints available from the endpoint mapper.**



Date: 1/30/2006 Source: SNMP Informant
Time: 1:40 Category: None
Type: Error Event ID: 2
User: N/A
Computer: STAND001_01

Description:

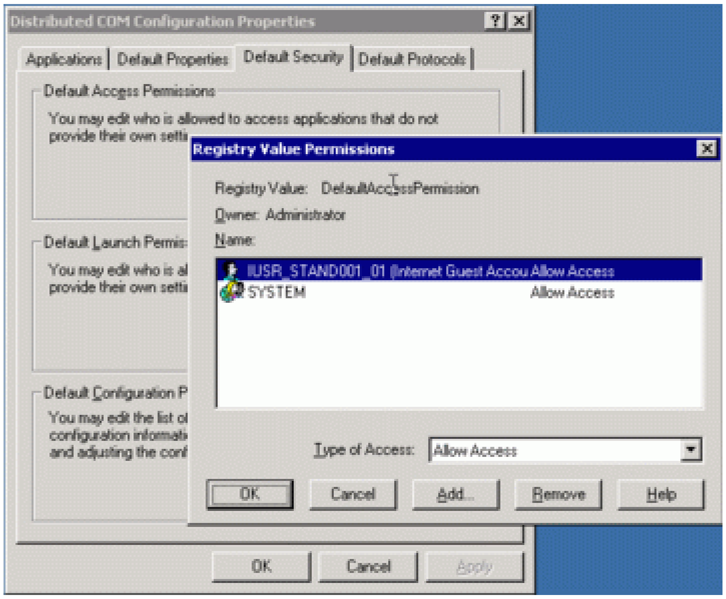
SNMP Informant Operating System

Error = 800706d9
Error Message = There are no more endpoints available from the endpoint mapper.

Data: ● Bytes ○ Words

If you are getting these error messages from SNMP Informant, check your event logs to see if you are getting 80070005 messages from *other* services as well, as DCOM security permissions affect more than just SNMP Informant (i.e. .Net runtime). Check MS KB 839880 at http://support.microsoft.com/kb/839880 for more information about troubleshooting RPC endpoint mapper problems.

To resolve this (for SNMP Informant at least), start the DCOM Configuration program (start/run/dcomcnfg), and add the SYSTEM account to the Default Access Permissions group.



You may edit who is allowed to access applications that do not provide their own setti

You may edit who is al provide their own setti

You may edit the list o configuration informati and adjusting the conf

Registry Value: DefaultAccessPermission

Owner: Administrator

| | |
|---|---|
| IUSR_STAND001_01 (Internet Guest Accou | Allow Access |
| SYSTEM | Allow Access |

Type of Access: Allow Access

You should also check the Default Launch Permissions group to ensure the SYSTEM account is also there.

More information about setting DCOM access permissions can be found here:

http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/set_specacc_dcom.htm

**End of Document**