Advantech

SNMP Subagent

User Guide

For Windows

Version <0.99>

Revision History

Date	Version	Description	Author
2018/05/02	0.99	Add log file descriptions	Zhirong.Hsu
2017/08/29	0.98	Update powerObj to add pwr-v1-low(3), pwr-v2-low(4) status.	Zhirong.Hsu
2016/10/05	0.97	Update Screenshot	Zhirong.Hsu
2016/02/16	0.96	Add powerObj to monitorGroup. Add trapPowerStatusChanged	Zhirong.Hsu
2015/12/23	0.95	Fix typo	Zhirong.Hsu
2015/12/21	0.94	Update monitorGroup to introduce the new thresholds and severity. Add memoryInfo, storageInfo, memory usage traps, and storage usage traps.	Zhirong.Hsu
2015/08/20	0.93	ManageEngine Free SNMP MIB Browser	Zhirong.Hsu
2015/04/01	0.92	Add Supported MIB Browser	Zhirong.Hsu
2014/12/12	0.91	Add Advantech SNMP Subagent Functions	Zhirong.Hsu
2014/10/23	0.90	Initial draft	Zhirong.Hsu

Copyright

Acknowledgements

Contents

User Guide

1. Introduction

1.1 Advantech SNMP Subagent

The Advantech SNMP Subagent allows you to communicate Simple Network Management Protocol (SNMP) with the common or platform Subagent on the managed system. With the Advantech SNMP Subagent, you can use SNMP SETs, GETs, and TRAPs to manage supported platforms.

1.2 Supported Advantech Platforms

The current version of Advantech SNMP Subagent supports the Advantech x86 hardware platform products. See the release notes to check the supported product list before using it.

1.3 Supported Operating Systems

The Advantech SNMP Subagent supports the following operating systems:

- Windows Embedded Standard 2009
- Windows Embedded Standard 7
- Windows Embedded 8 Standard
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10

1.4 System Requirements

1.4.1 SNMP Master Agent

The Advantech SNMP Subagent is based on the Windows SNMP service. You must install the Windows SNMP service on the supported operating systems. You can check the service snap-in. Please refer to Figure 1-1 (found under Administrative Tools in Windows Control Panel).

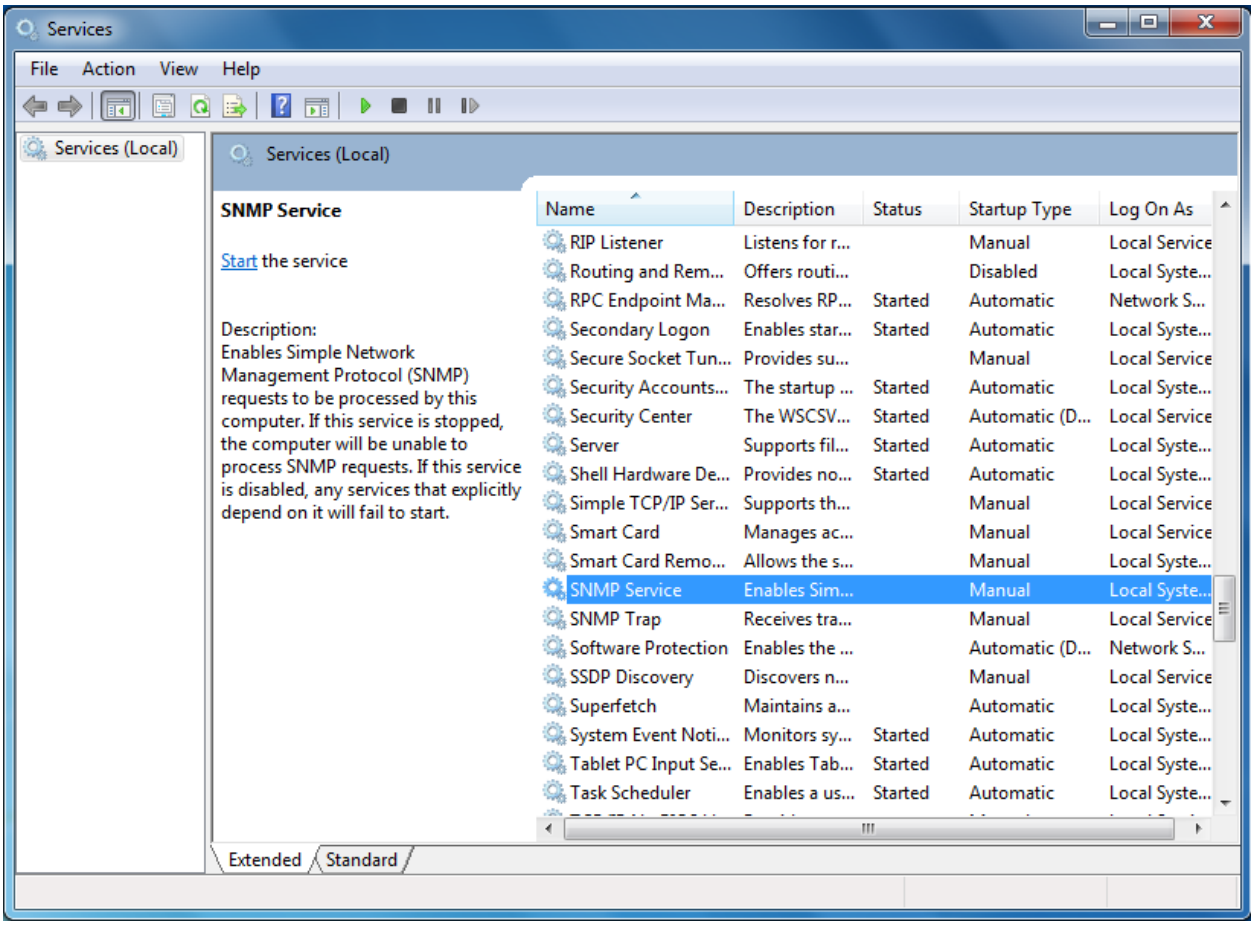

Figure 1-1 Windows Services

If the SNMP service does not exist, you can turn on the *Simple Network Management Protocol* by the following steps. Here is a Windows 7 example.

1. Go to **Control panel > Programs and Features**. (Figure 1-2)
2. Click **Turn Windows features on or off** on the left panel.
3. In **Windows Features** window, check the checkbox **Simple Network Management Protocol**. (Figure 1-3)
4. Click **OK**.

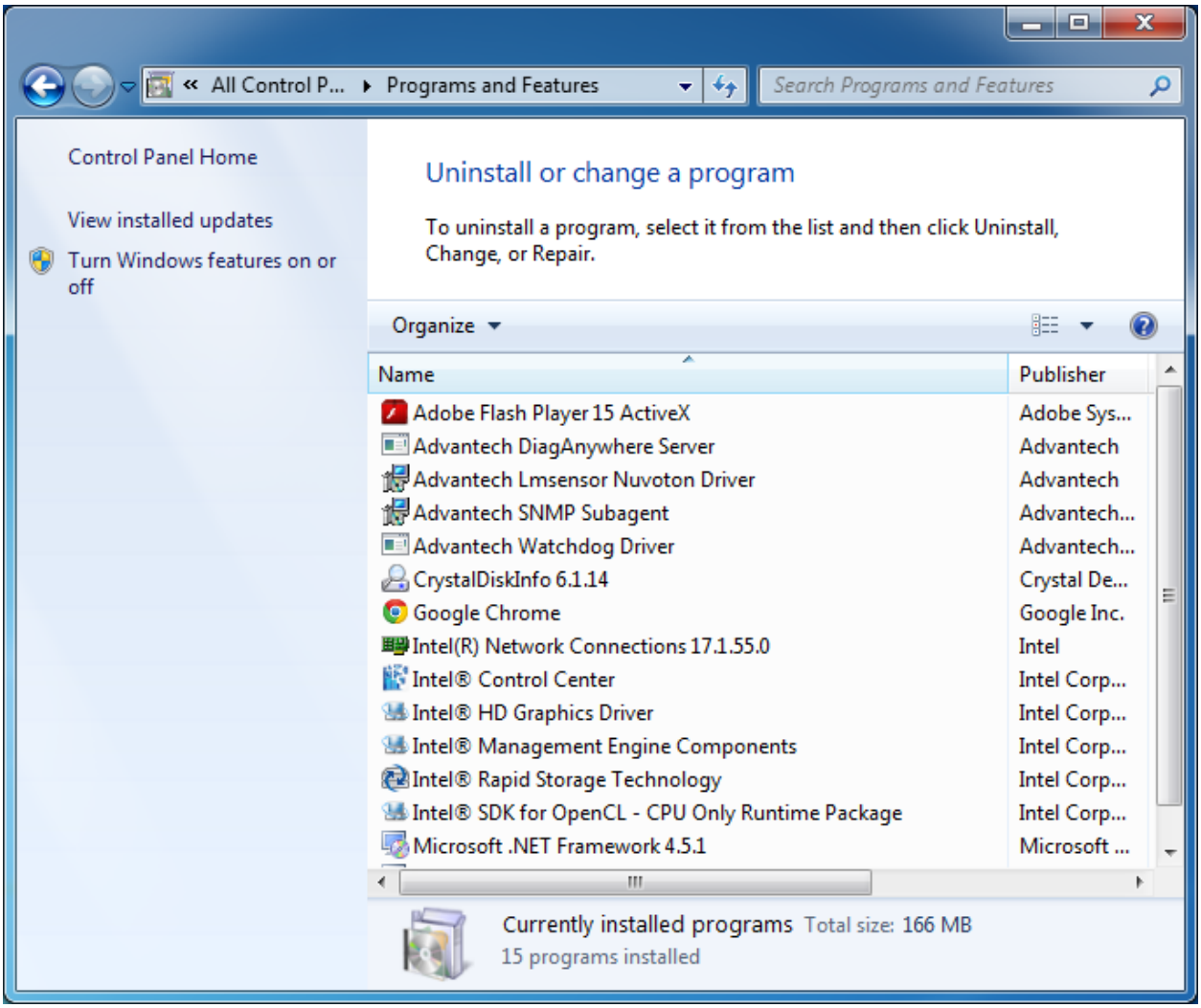

Figure 1-2 Programs and Features

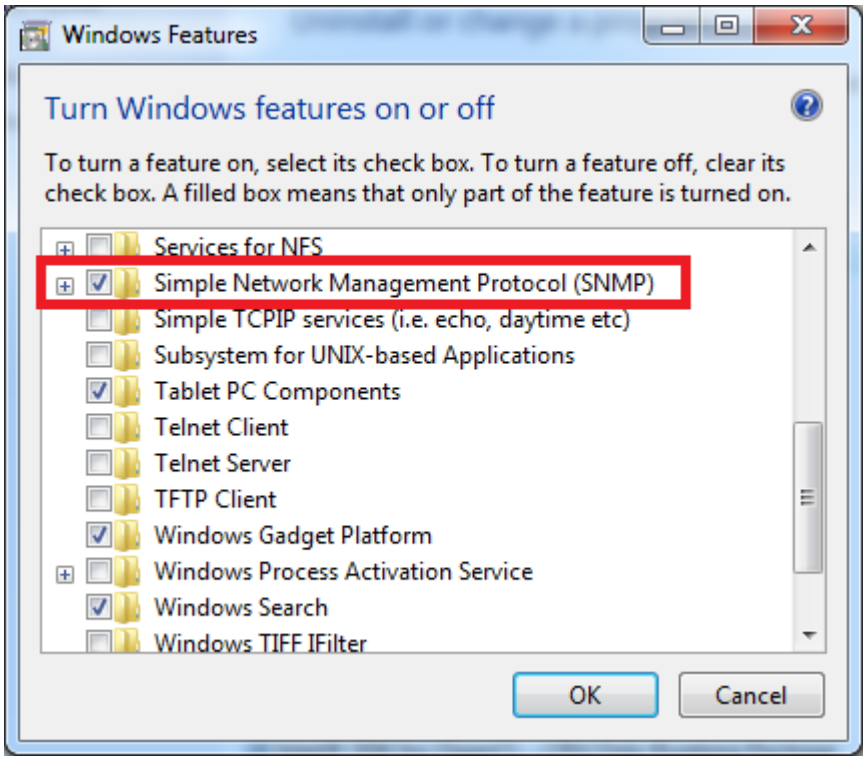

Figure 1-3 Windows Features

1.4.2 Latest Drivers

The Advantech SNMP Subagent requires the latest Advantech drivers including the following.

- Advantech Lmsensor Drivers
- Advantech Watchdog Drivers
- Advantech Multi-level Watchdog Drivers (If applicable)
- Advantech Brightness Drivers (If applicable)
- Advantech UNODIO Drivers for embedded IO (If applicable)

2. Advantech SNMP Subagents Overview

Advantech SNMP Subagents are SNMP extension agents that provide interfaces for retrieving Advantech x86 hardware and software information and monitoring the health status of the network using the SNMP protocol. Table 2-1 is the basic information of Advantech SNMP Subagents.

Table 2-1 Advantech SNMP Subagents

Name	**MIB file**	**Supported Region**
Advantech Common Agent	advantech-common-mib.mib	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).advantech(10297).advantechCommonMIB(100)
Advantech Platform Agent	ADVANTECH-PLATFORMS-MIB.mib	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).advantech(10297).advantechPlatformsMIB(200)

2.1 MIB and OID

SNMP works with basic components OIDs (Object Identifier) and MIBs (Management Information Base). The user gets information by querying “Objects”. A MIB (Management Information Base) is a database including many objects and it is a tree structure shown in Figure 2-1; each node is addressed through an object identifier (OID) and it maps to an entity in a communications network. OIDs are always written in a numerical form instead of a text one. Therefore, the top three object levels are written as “1.3.1” rather than “iso\org\dod” and the OIDs of Advantech is *1.3.6.1.4.1.10297*

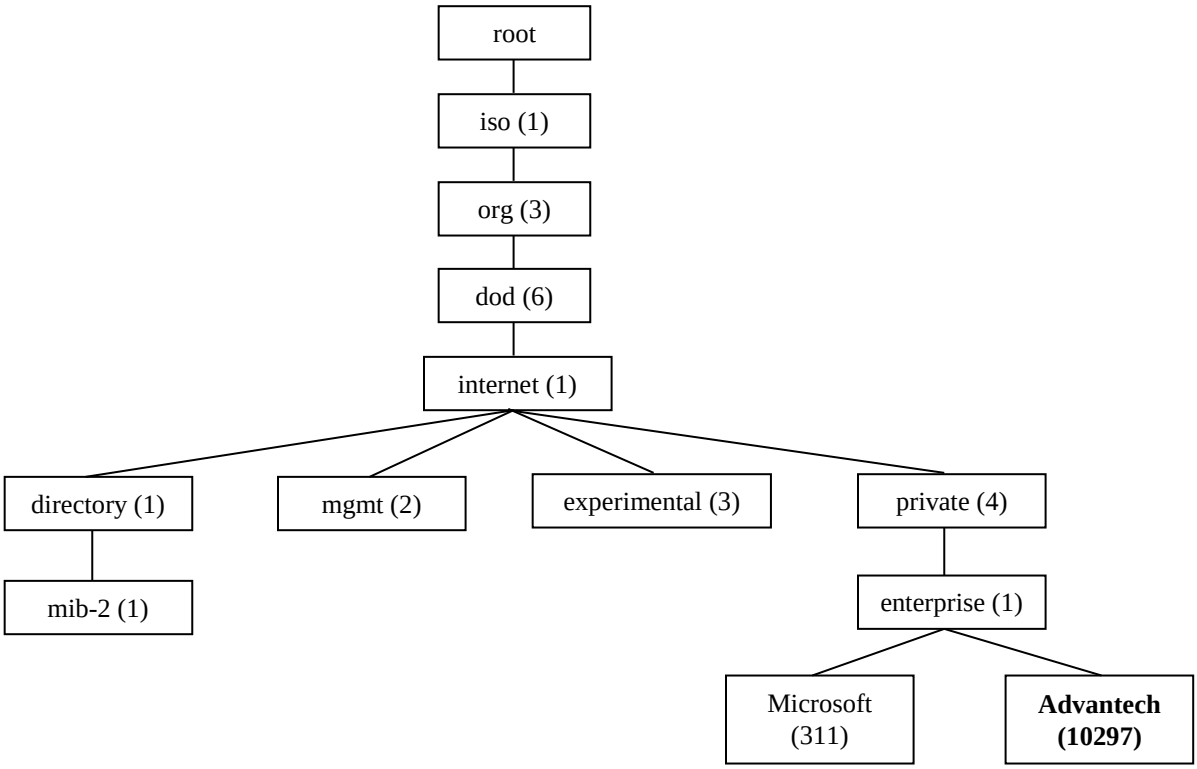

Figure 2-1 OIDs tree

2.2 Community Strings

Community Strings are similar to passwords. They are used to allow authorized you to access the SNMP agent on a device.

Community Strings can be configured as read-only (RO) or read-write (RW). As the name implies, read-only strings only allow information to be pulled from the agent. However, read-write strings are much more powerful and can allow reconfiguration of many device properties. In general, the default community strings are set to be “public” for read-only (RO), and “private” for read-write (RW).

2.3 Architecture

Network Management Station (NMS) can communicate with subagents by the OIDs defined in the MIB files.

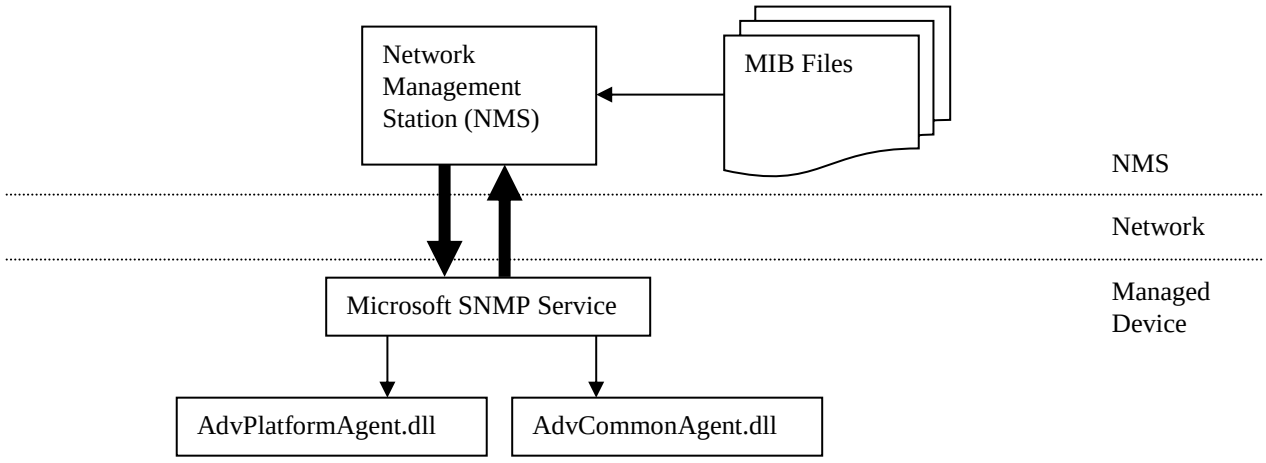

Figure 2-2 Architecture

2.4 Advantech SNMP Subagents

The Advantech SNMP Subagents provides the functions as shown in Figure 2-3.

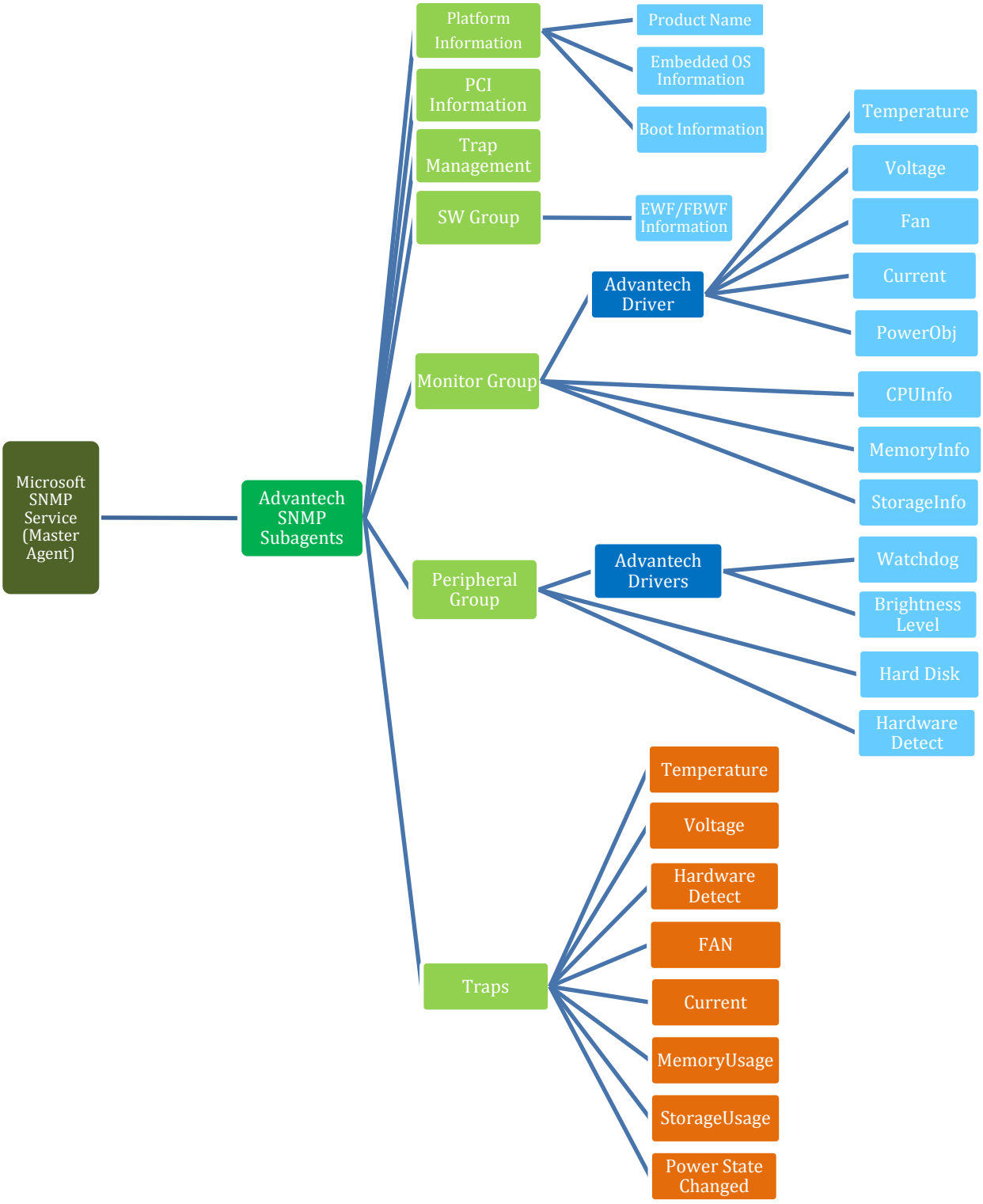

Figure 2-3 Advantech SNMP Subagent Functions

2.4.1 Platform Information

You can **get** the system information of the managed device, such as *model name*, *image version*, *image release date*, *system first boot time*, *system boot time*, and *boot count*.
If there are multiple identical devices, you can **set** an *alias name* or a *description* of each device.

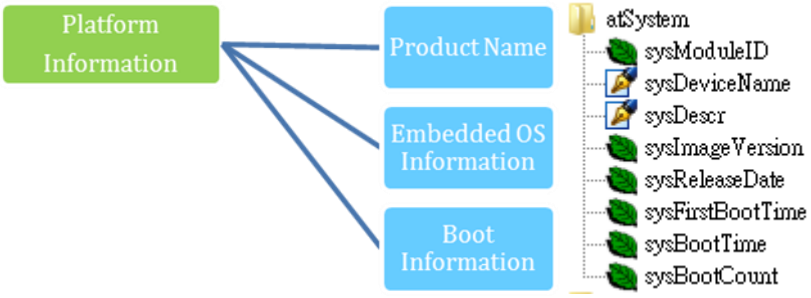

Figure 2-4 Platform Information

2.4.2 PCI Information

You **can** get the PCI information (table) of the managed device, such as *Vendor ID*, *Device ID*, *IRQ*, *Description*, *Base Address* … etc.

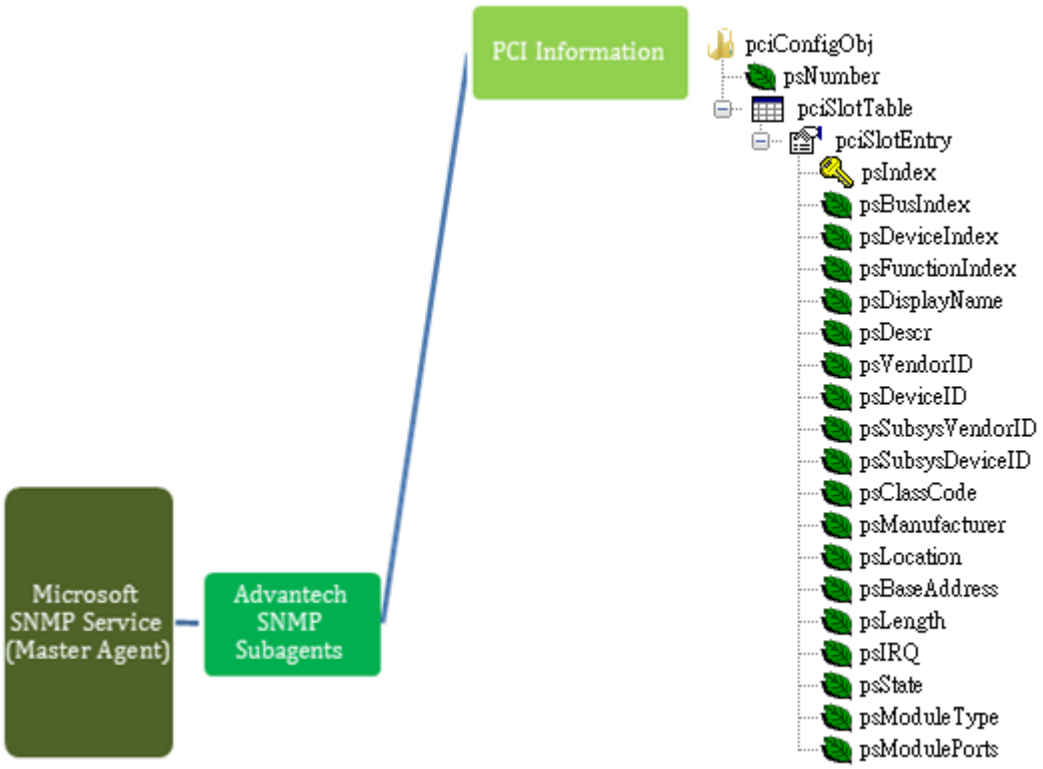

Figure 2-5 PCI Information

2.4.3 Trap Management

You can **set** the *destination IP* of NMS or trap management tool.

Figure 2-6 Trap Management

2.4.4 Software Group

You can **get** the *EWF (Enhanced Write Filter)* and *FBWF (File Based Write Filter)* current settings.

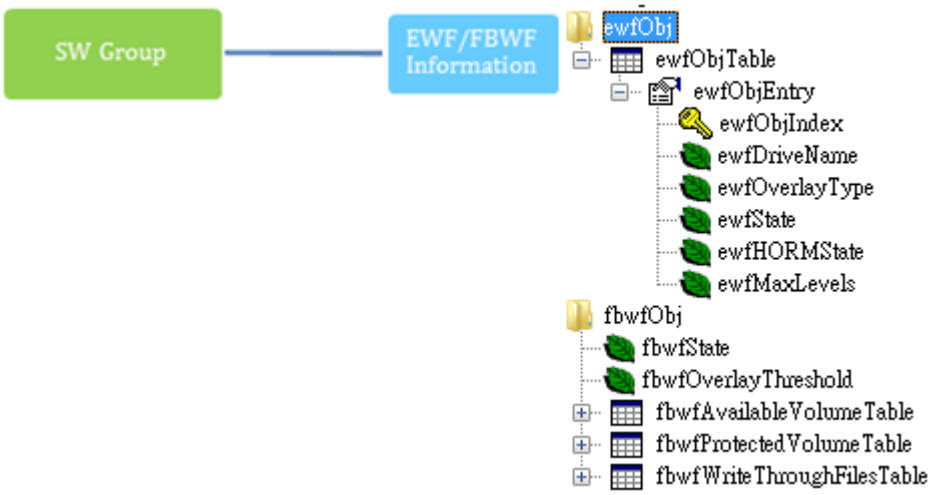

Figure 2-7 SW Group

2.4.5 Monitor Group

- You can **get** the *Temperature*, *Voltage*, *Fan,* and Current information which are handled by *Advantech Driver*.
- You can **set** *high*, *low, high-high, and low-low* threshold values of each Temperature, Voltage, Fan, and Current. You can also set a **null** value to disable the threshold.
  When the threshold has been set, the monitored *value* will be divided into **5** levels, cleared(1), critical-low (2), low (3), high (4), and critical-high (5).
  - If the *Value* is greater than the *high-high* threshold and *high-high* threshold is not disabled (null), the level is **critical-high** (5).
  - If the *Value* is greater than the *high* threshold and less than or equal to the *high-high* threshold and *high* threshold is not disabled (null), the level is **high** (4).
  - If the *Value* is greater than *low* threshold and less than or equal to the *high* threshold and *low* threshold is not disabled (null), the level is **low**(3).If the *Value* is less than the *low-low* threshold and the *low-low* threshold is not disabled (null), the level is **critical-low**(2).
  - Otherwise, the level is **cleared** (1).
- You can also enable monitoring state when the value is out of bound, it will send a trap to NMS.
- You can **get** the current *CPU Loading*, current *CPU Speed*, *CPU Maximum Speed*, *memory size*, *memory usage percentage,* and *storage usage percentage* of the managed device.
  There are **4** threshold values UsageTh1 ~ UsageTh4 which splits the usage into **5** severities, cleared(1), notice(2), warning(3), critical(4), and emergency(5) if the threshold value is not disabled (**-1**).
  - If the *usage* is greater than *UsageTh1* and *UsageTh1* is not disabled(-1), the severity is **notice**(2)
  - If the *usage* is greater than *UsageTh2* and less than or equal to *Usage Th1* and *UsageTh2* is not disabled(-1), the severity is **warning**(3)
  - If the *usage* is greater than *UsageTh3* and less than or equal to *Usage Th2* and *UsageTh3* is not disabled(-1), the severity is **critical**(4)
  - If the *usage* is greater than *UsageTh4* and *UsageTh4* is not disabled(-1), the severity is **emergency**(5)
  - Otherwise, the severity is **cleared**(1)
- You can **get** the power state **pwr-normal**(1), **pwr-redundancylost** (2), **pwr-v1-low** (3) or **pwr-v2-low** (4) and the power state severity including **cleared**(1), **notice**(2), **warning**(3), **critical**(4), and **emergency**(5) if the target platform support these features. You can also enable the power monitoring state when the power state changed, it will send a trap to the NMS.

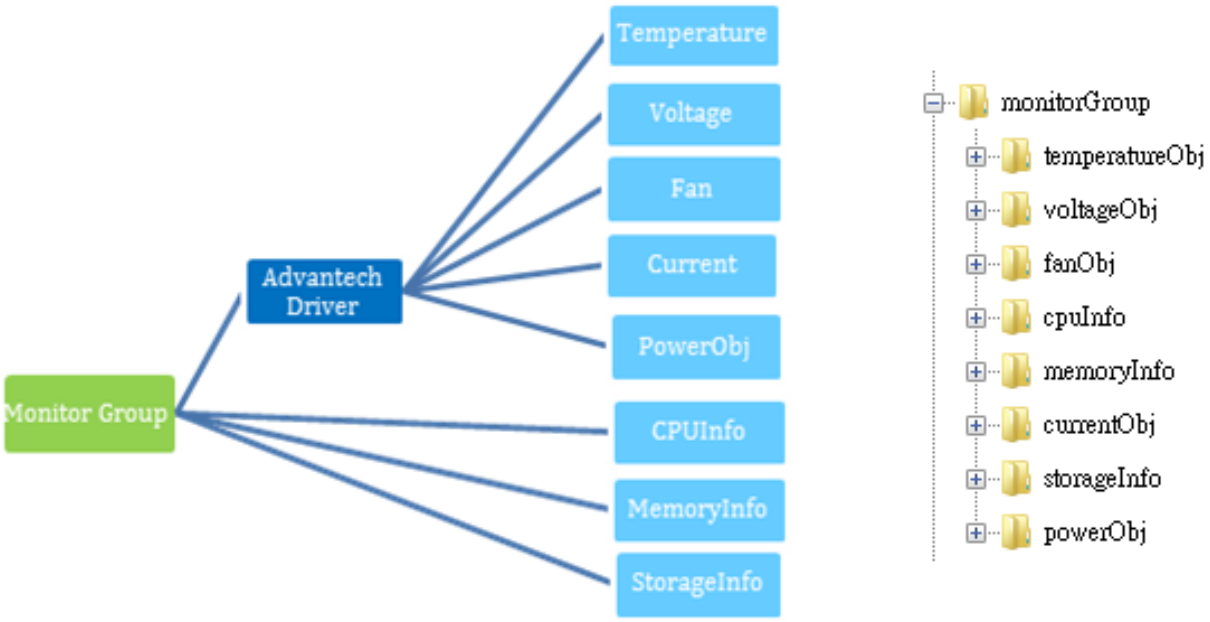

Figure 2-8 Monitor Group

2.4.6 Peripheral Group

You can **get** the current Watchdog/Multilevel Watchdog *configuration* and the current *state*. You can **get** the *current brightness level* of the HMI device. (If applicable)

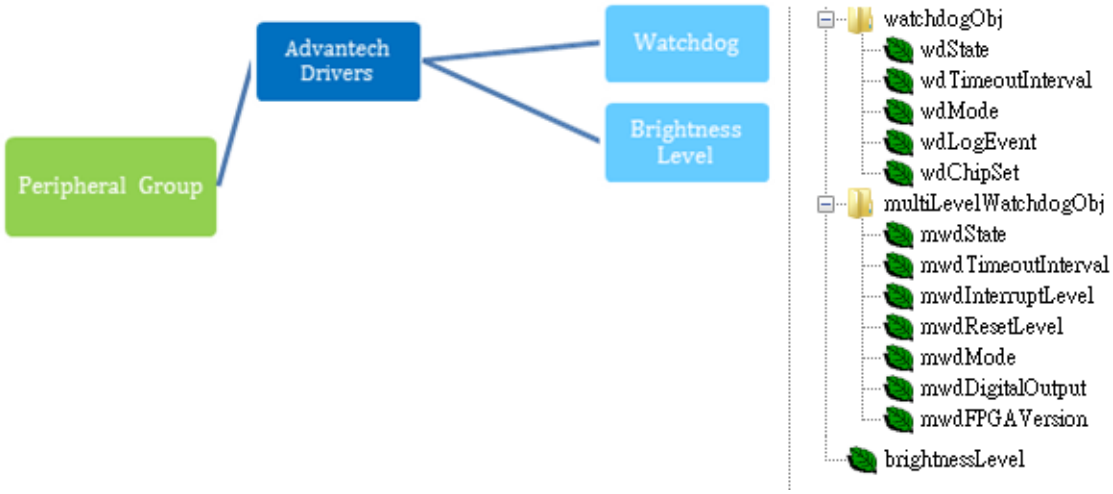

Figure 2-9 Peripheral Group

2.4.7 Peripheral Group – Hard Disk

You can **get** the *hard disk information* and the *S.M.A.R.T.* (Self-Monitoring, Analysis, and Reporting Technology) information of it.

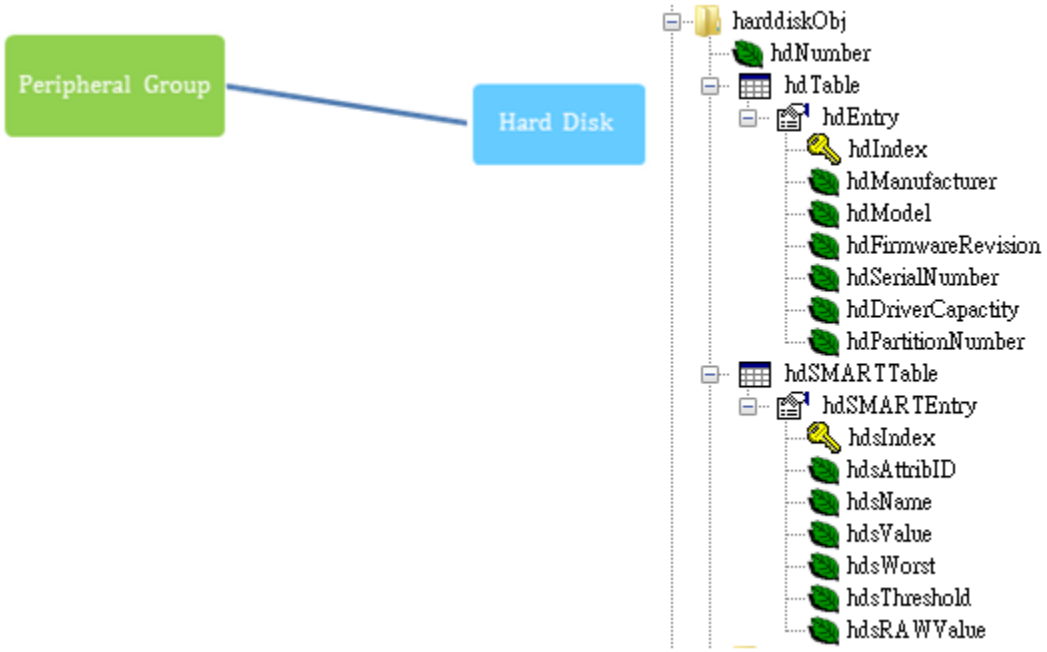

Figure 2-10 Peripheral Group – Hard Disk

2.4.8 Peripheral Group – Hardware Detection

If hardware is inserted or removed, the SNMP subagent will record the information. If the "hardware detect trap" is **enabled**, the SNMP subagent will also send a trap (alarm) to the NMS. The hardwareDetectObj supports the below types of hardware with related hwdClassGUID

- USBRawDevice : {a5dcbf10-6530-11d2-901f-00c04fb951ed}
- DiskDevice : {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- NetworkCard : {ad498944-762f-11d0-8dcb-00c04fc3358c}
- HumanInterfaceDevice (HID) :{4d1e55b2-f16f-11cf-88cb-001111000030}

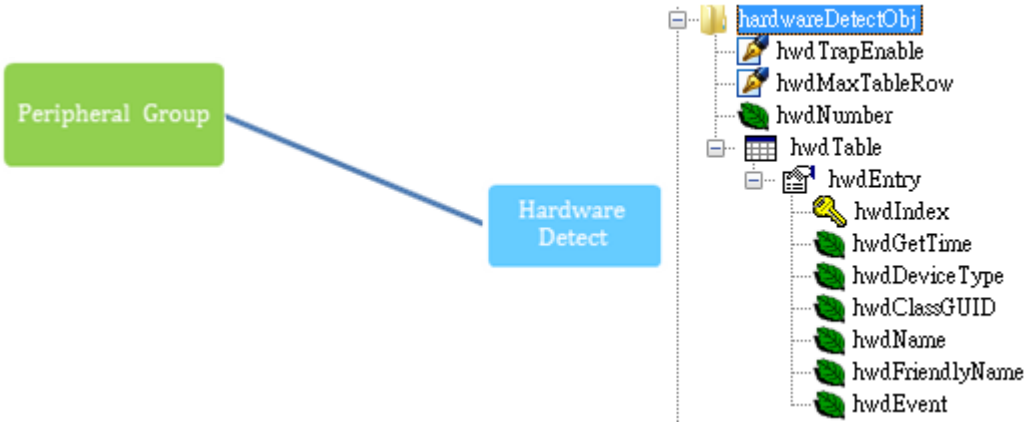

Figure 2-11 Peripheral Group – Hardware Detection

2.4.9 Trap

The *Advantech SNMP Subagents* currently support 13 types of Traps.

- Temperature is out of range
- Temperature becomes normal
- Voltage is out of range
- Voltage becomes normal
- Hardware insertion and removal
- Fan Speed is out of range
- Fan Speed becomes normal
- Current is out of range
- Current becomes normal
- Memory Usage exceeds the threshold value
- Memory Usage becomes normal
- Storage Usage exceeds the threshold value
- Storage Usage becomes normal
- Power State is changed

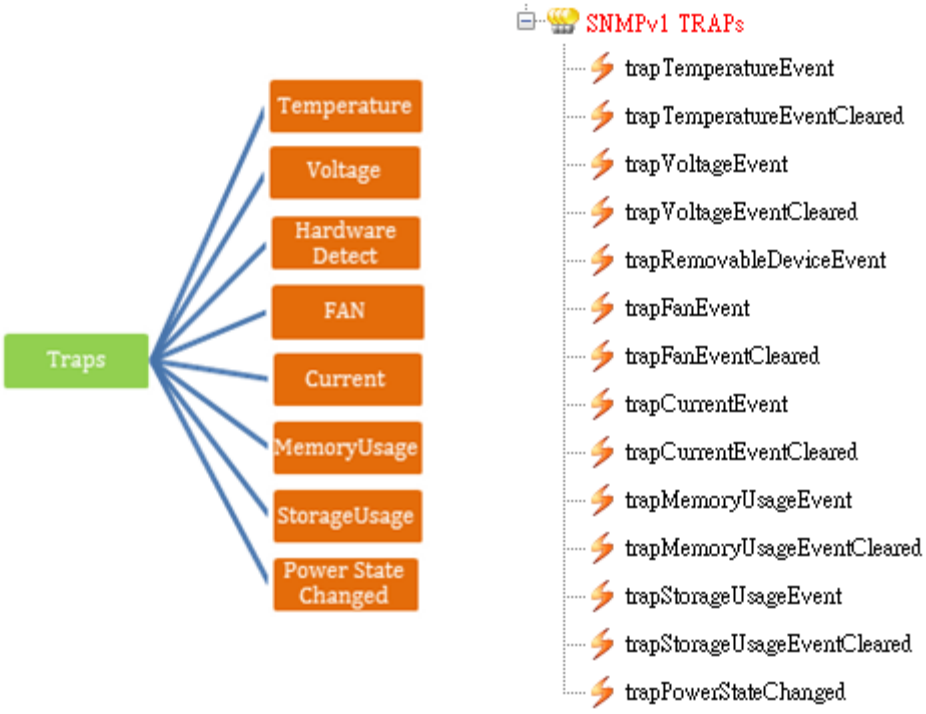

Figure 2-12 Traps

2.4.10 Log files

There are log files for *Advantech SNMP Subagents* to keep track of important events. The subagent defines the following commonly used *severity levels*: **none** = 0, **fatal** = 1, **error** = 2, **warning** = 3, **info** = 4, **debug** = 5, **verbose** = 6 and the default level is ***error***.

These log files can be found in the C:\Windows\System32 (32-bit Windows) or C:\Windows\SysWOW64 (64-bit Windows) folder and the file names are **AdvCommonAgent.log** for *Advantech Common Agent* and **AdvPlatformAgent.log** for *Advantech Platform Agent*.

The subagent supports **Log Rotation,** and the log file is rolled over after a specified size **MaxLogFileSize** (in bytes) has been reached.
For example, if logging to a file named file.log, when the file size reaches the specified size limit, the contents are archived in a file named file.1.log and file.log is truncated. When the size limit is reached the second time, file.1.log is renamed to file.2.log; contents from file.log are archived to file.1.log and file.log is truncated.

This continues until the maximum backup index **MaxLogFileCount** is reached, after which the oldest log file is deleted on each rollover.

You can set **LogSeverity** (default is 2), **MaxLogFileSize** (default is 1048576 bytes) and **MaxLogFileCount** (default is 5) in the registry.
32-bit Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Advantech Corp.\SNMP
64-bit Windows:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Advantech Corp.\SNMP

Table 2-2 Log Parameters

Entry name	Data type	Values
LogSeverity	REG_DWORD	none = 0, fatal = 1, error = 2 (default), warning = 3, info = 4, debug = 5, verbose = 6
MaxLogFileSize	REG_DWORD	Maximum allowed file size (in bytes) before rolling over; the lowest MaxLogFileSize is 1000 bytes. Default is 1048576 bytes (1 MB)
MaxLogFileCount	REG_DWORD	A number of log files to keep. Default is 5

3. Installation and Uninstallation

3.1 Installation

3.1.1 Launch installation package

Launch the *Advantech SNMP Subagent Installation Package* and you can see the following wizard. Click *Next* to start the installation.

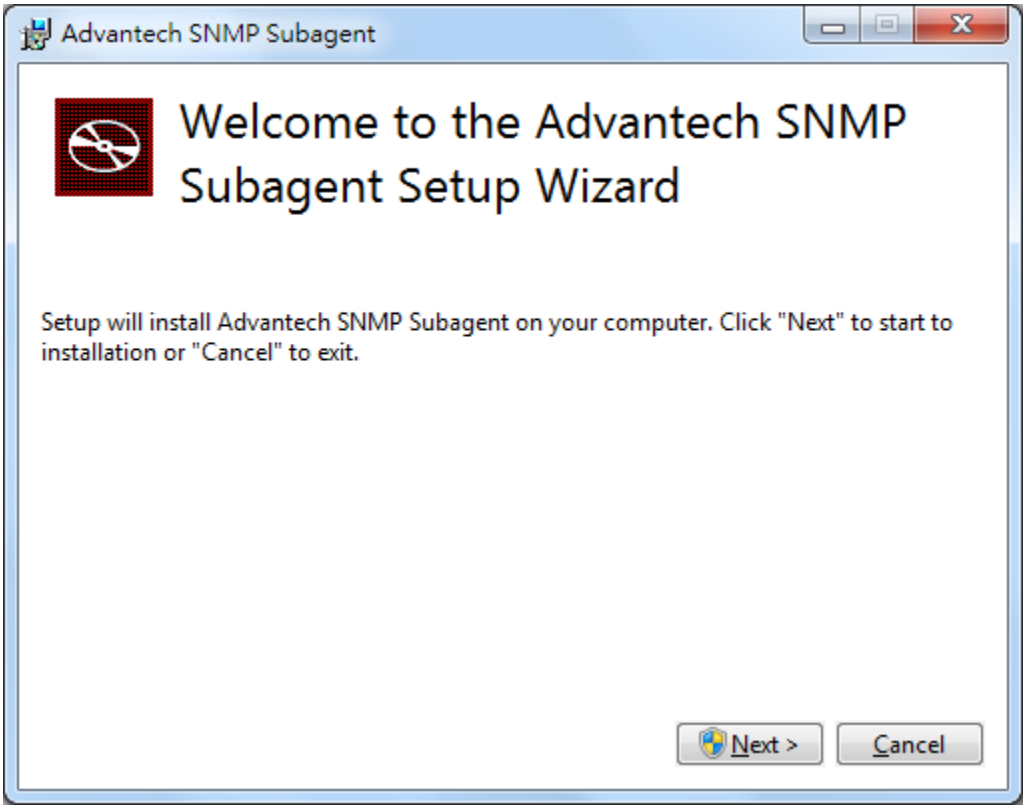

Figure 3-1 Advantech SNMP Subagent Installation Package

You may see an error message below if the target platform has not installed *SNMP service* before.

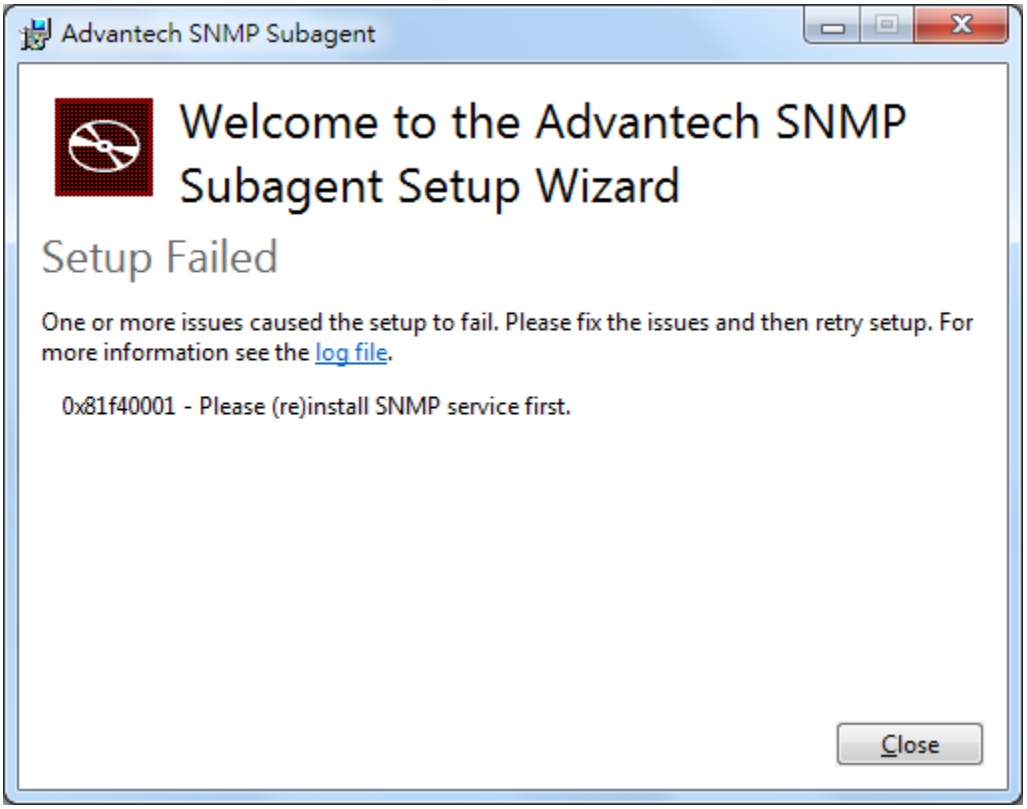

Figure 3-2 Please install SNMP service

3.1.2 Install Advantech Kernel Driver

The installation package will install the *Advantech Kernel Driver* which is needed by *Advantech SNMP Subagent*.

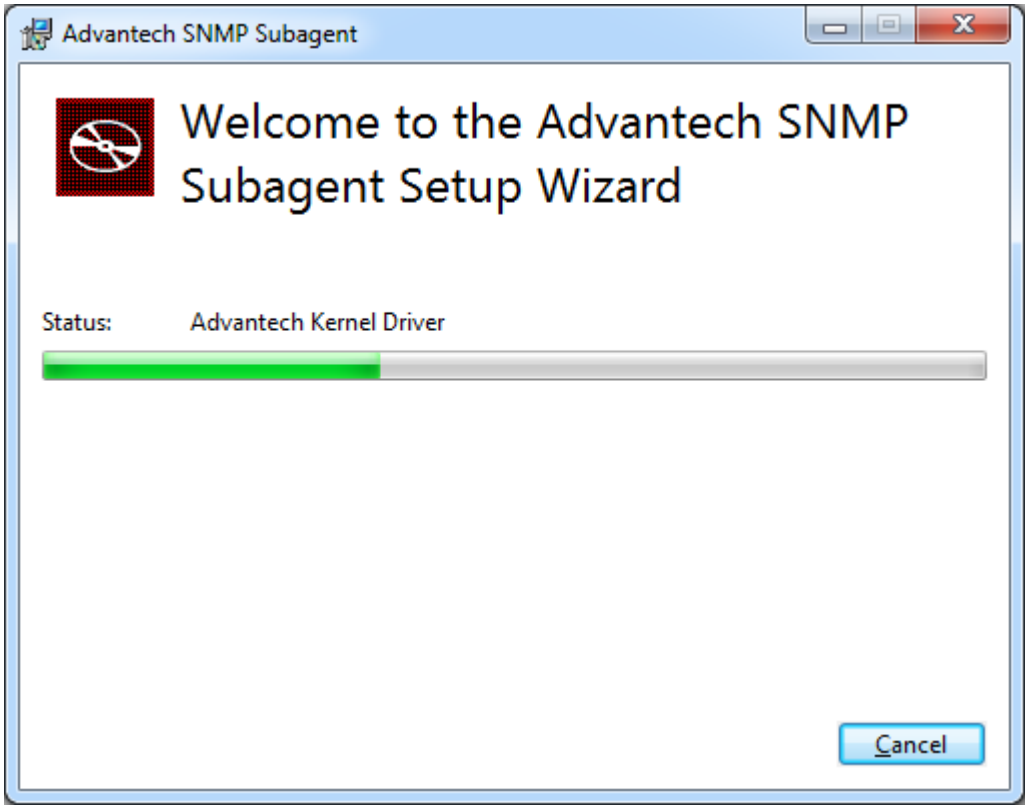

Figure 3-3 Advantech Kernel Driver

The Installation may display the following message, check ***Always trust software from "Advantech Co., Ltd."*** *and* click **Install** to complete the driver installation.

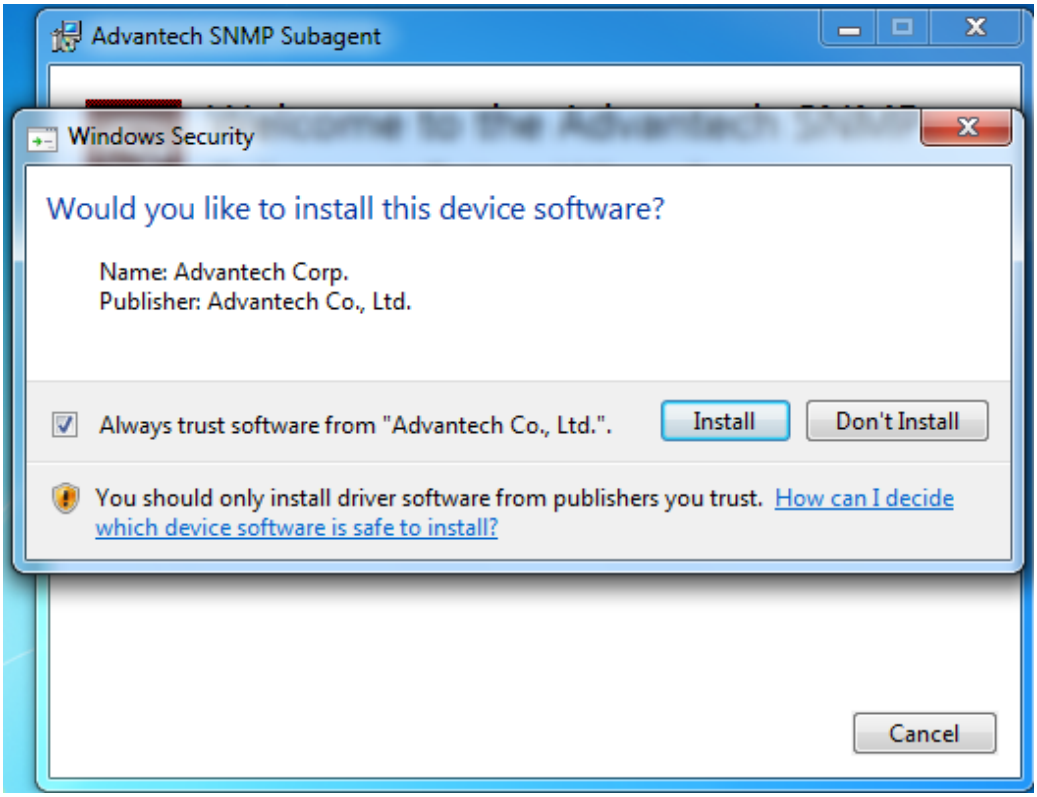

Figure 3-4 Windows Security of Driver

3.1.3 Install Advantech SNMP Subagent

To install the *Advantech SNMP Subagent*, the installation Wizard will display another installation wizard as shown in Figure 3-6.

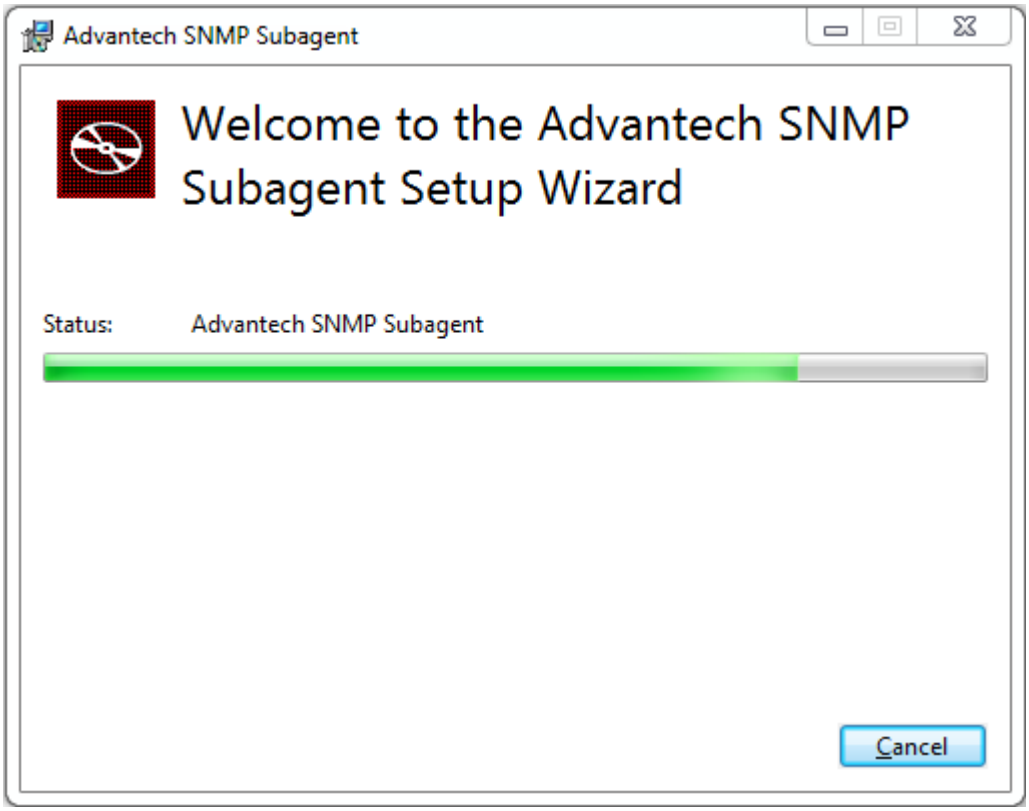

Figure 3-5 Advantech SNMP Subagent

Click **Next** to start the installation and you will see an *SNMP configuration* page as shown in Figure 3-7.

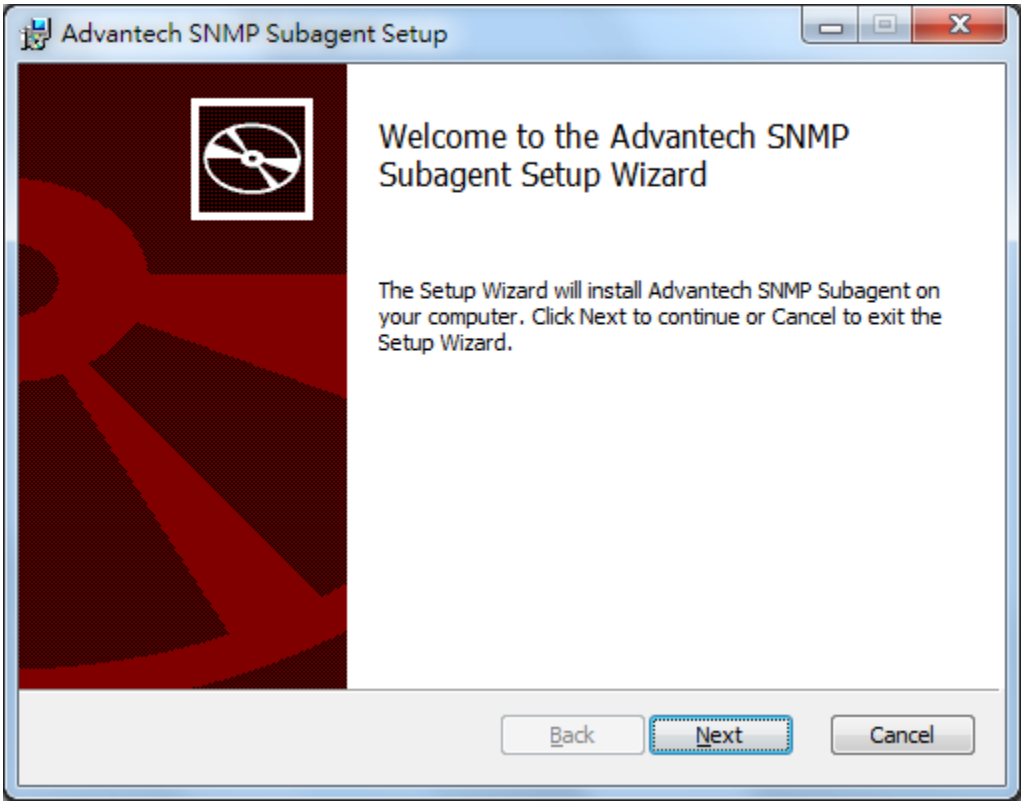

Figure 3-6 Advantech SNMP Subagent Setup Wizard

3.1.4 SNMP Configuration

You can enter the *Read-Only*, *Read-Write*, and *Trap Community* which will be applied to the SNMP service. If you input an incorrect Community String, the installation wizard will show an error message as shown in Figure 3-8.

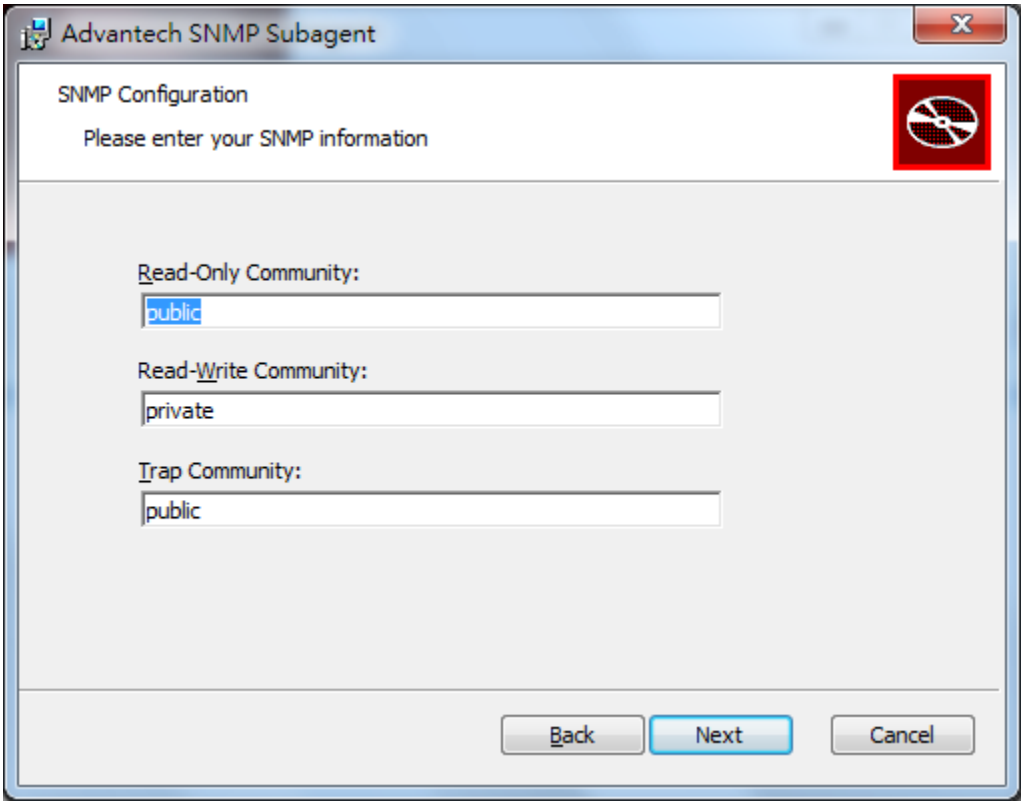

Figure 3-7 SNMP Configuration

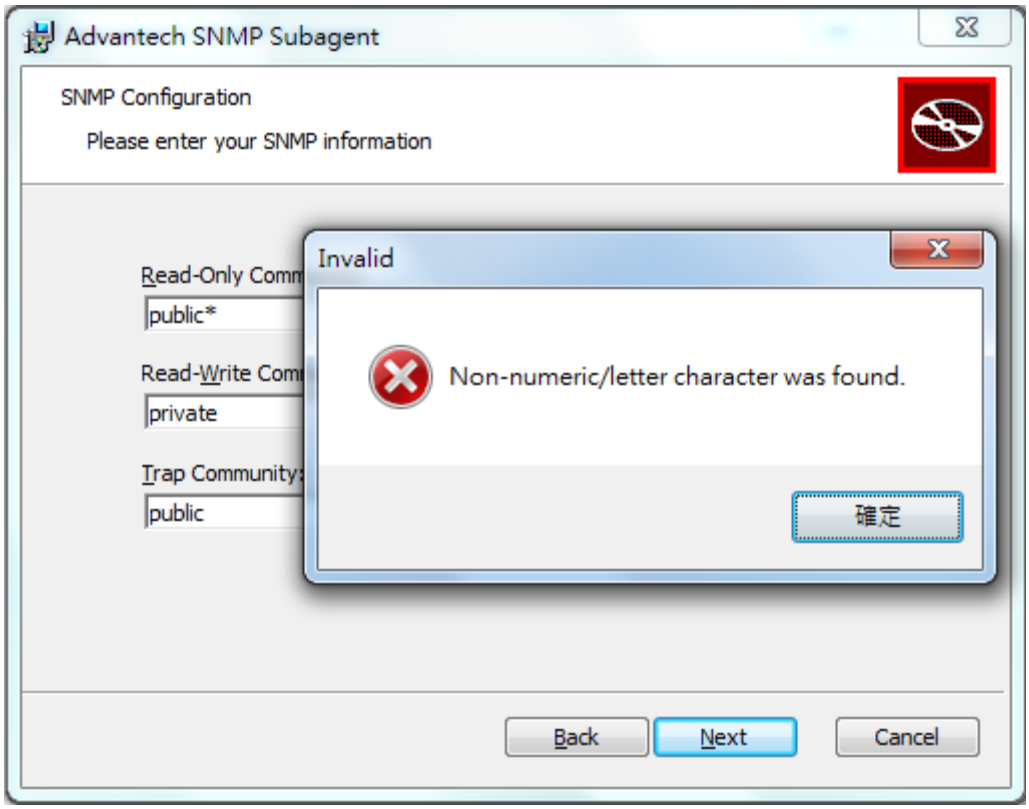

Figure 3-8 Incorrect Community String

After installation, the Read-Only and Read-Write community will be applied to the *Security tab* of SNMP Service Properties as shown in Figure 3-9.

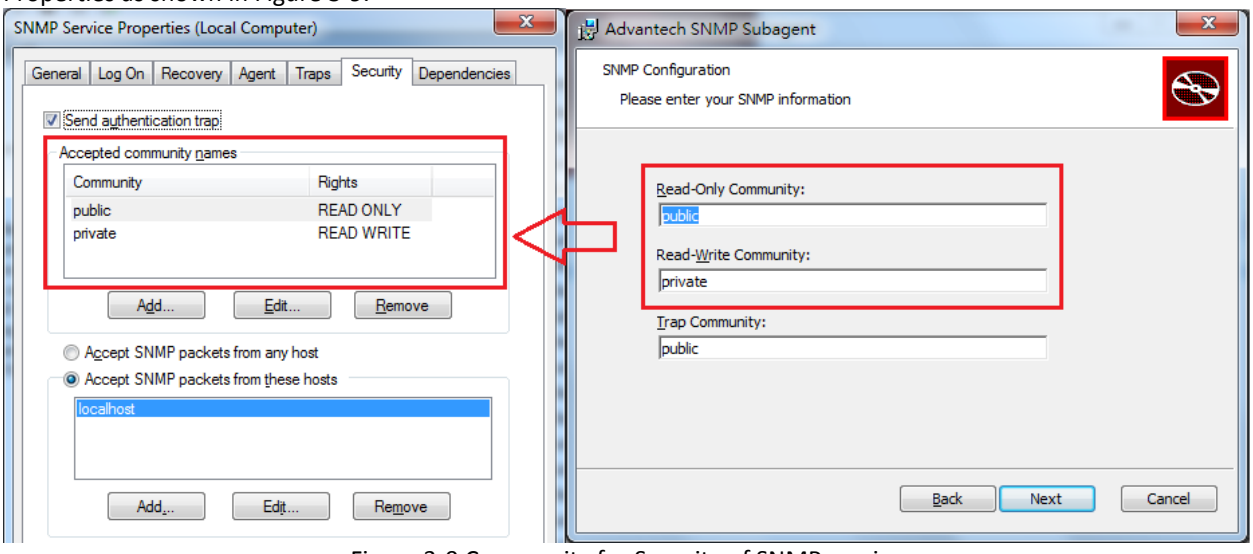

Figure 3-9 Community for Security of SNMP service

The *Trap Community* will be applied to the *Traps* tab of *SNMP Service Properties* as shown in Figure 3-10. You can add more *Trap destinations* in the *Traps* tab of *SNMP Service Properties* if need.

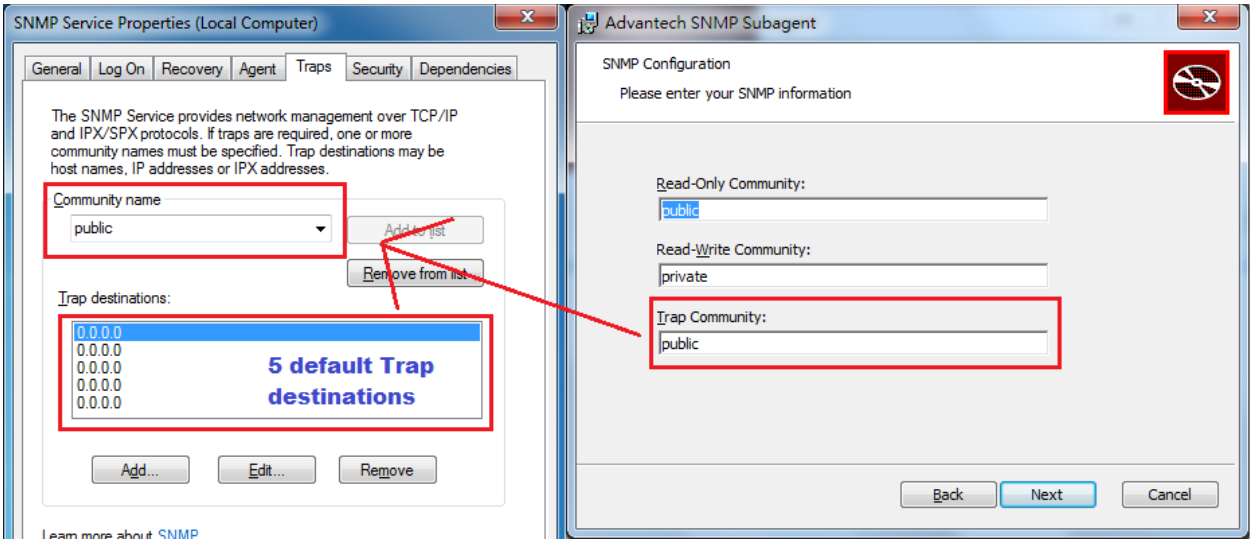

Figure 3-10 Community for Traps of SNMP service

3.1.5 Install the SNMP Subagent

After finishing SNMP configuration, you can continue to install SNMP subagent. During installation, it will install subagents to the system and restart the SNMP service as shown in Figure 3-12.

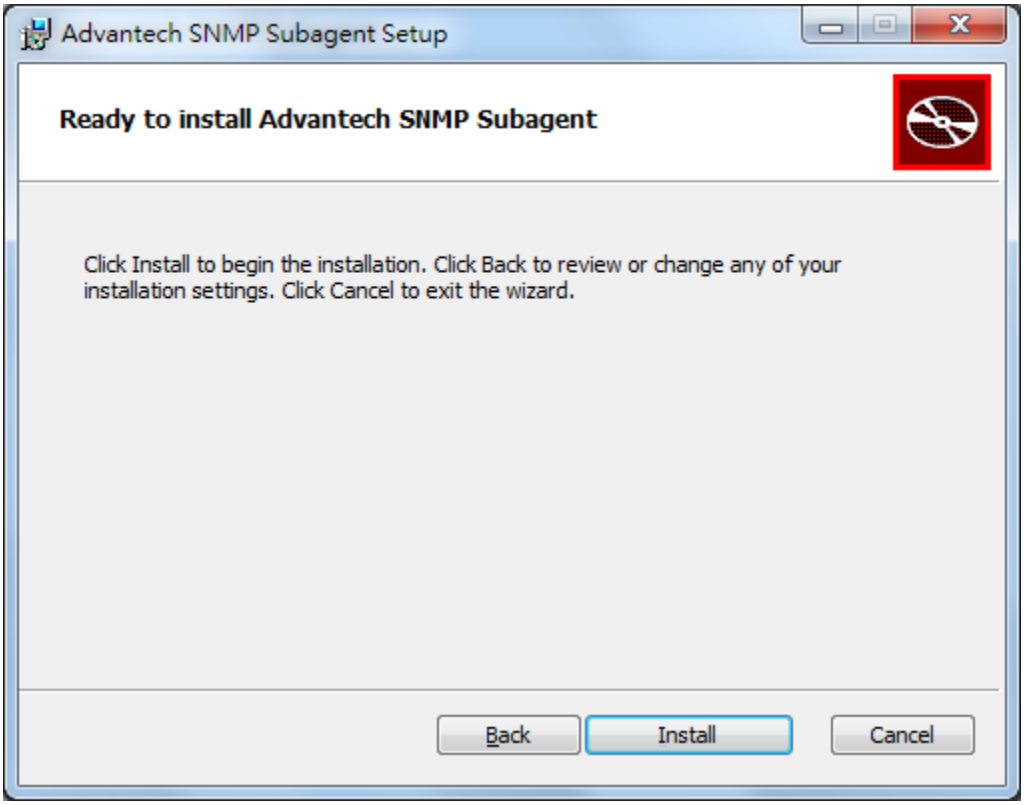

Figure 3-11 Ready to Install SNMP Subagent

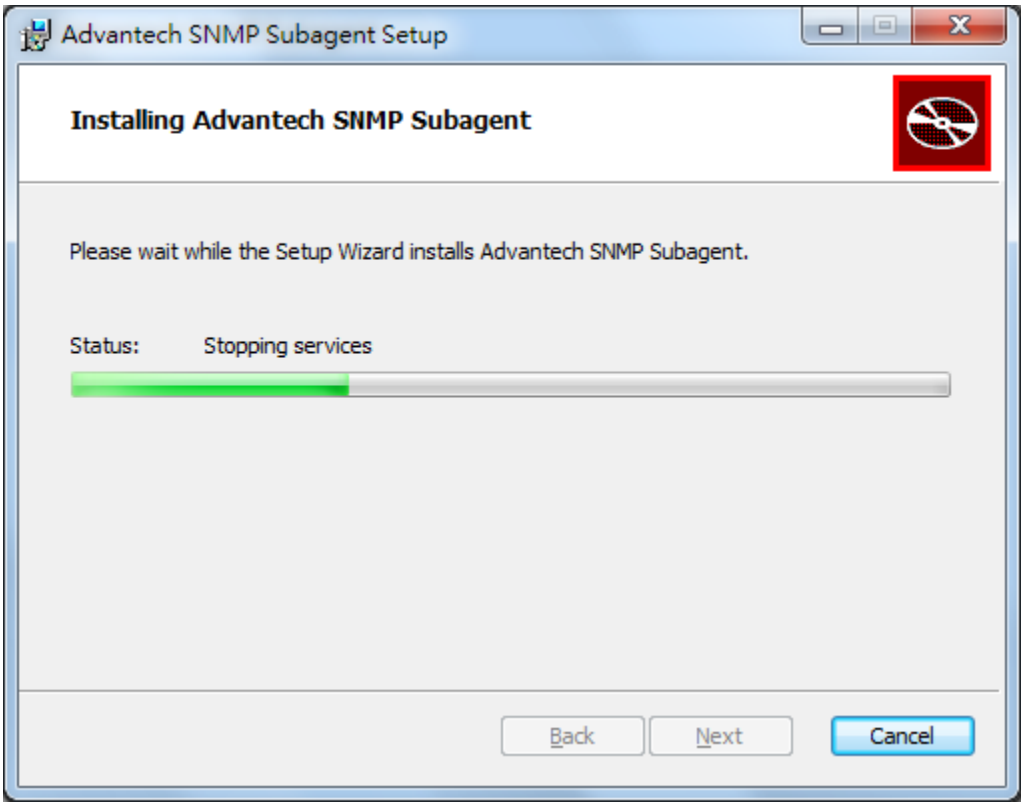

Figure 3-12 Stop/Start Service

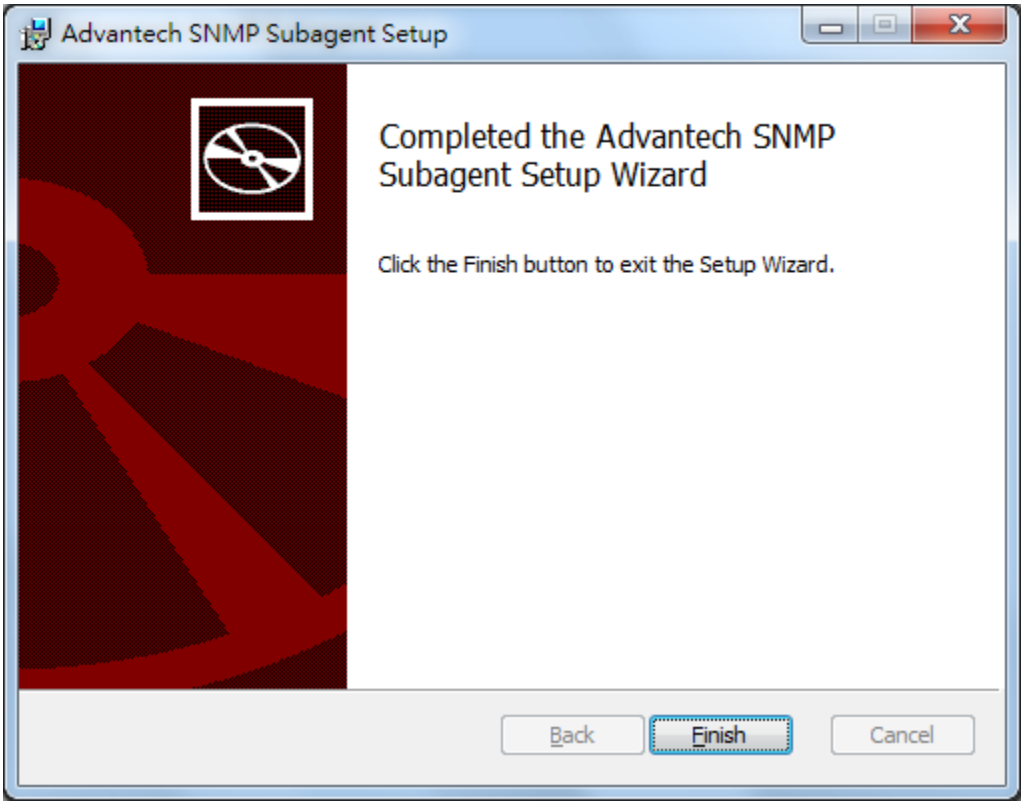

Figure 3-13 Installation Completed

3.1.6 Restart Computer

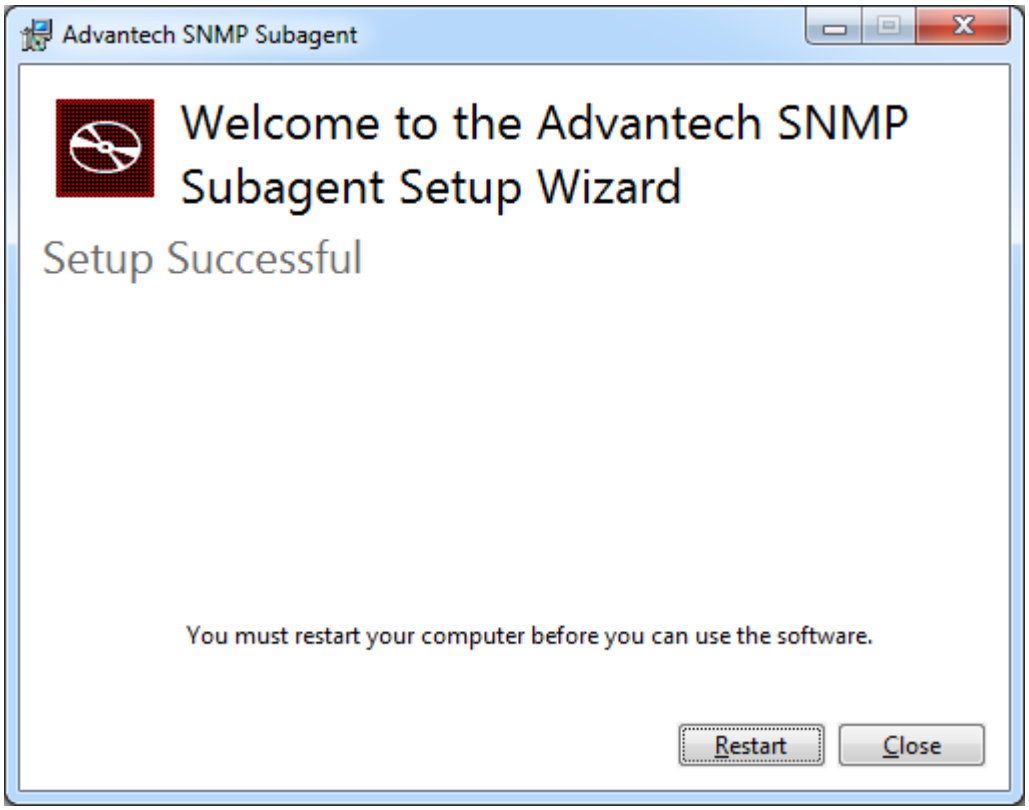

Figure 3-14 Restart Required

3.1.7 Security Settings

In order to communicate with Network Management Station (NMS), you need to add the NMS IP address to the Security tab of SNMP service properties as shown in Figure 3-15

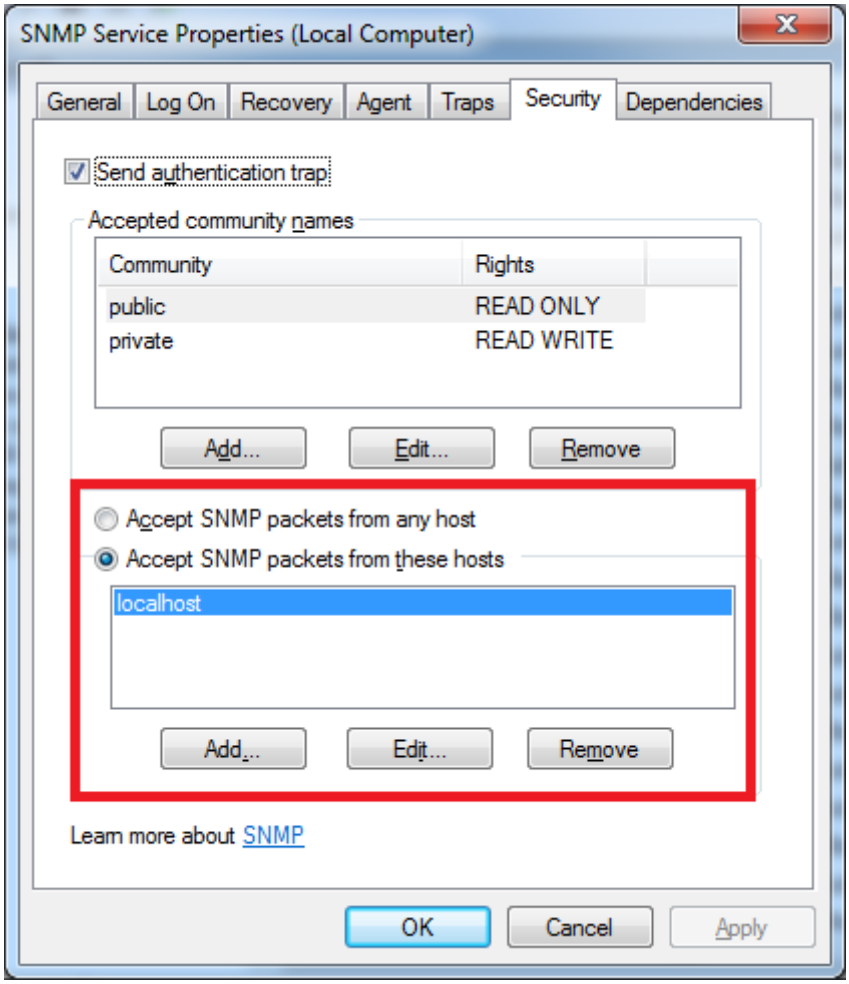

Figure 3-15 Add NMS IP address

3.1.8 Get MIB files

After the installation finished, you can find the MIB Files from **Start menu** > **All Programs** > **Advantech** > **SNMP Subagent** > **SNMP Subagent MIB Files** as shown in Figure 3-16 or from the installation folder of *Advantech SNMP Subagent* as shown in Figure 3-17.

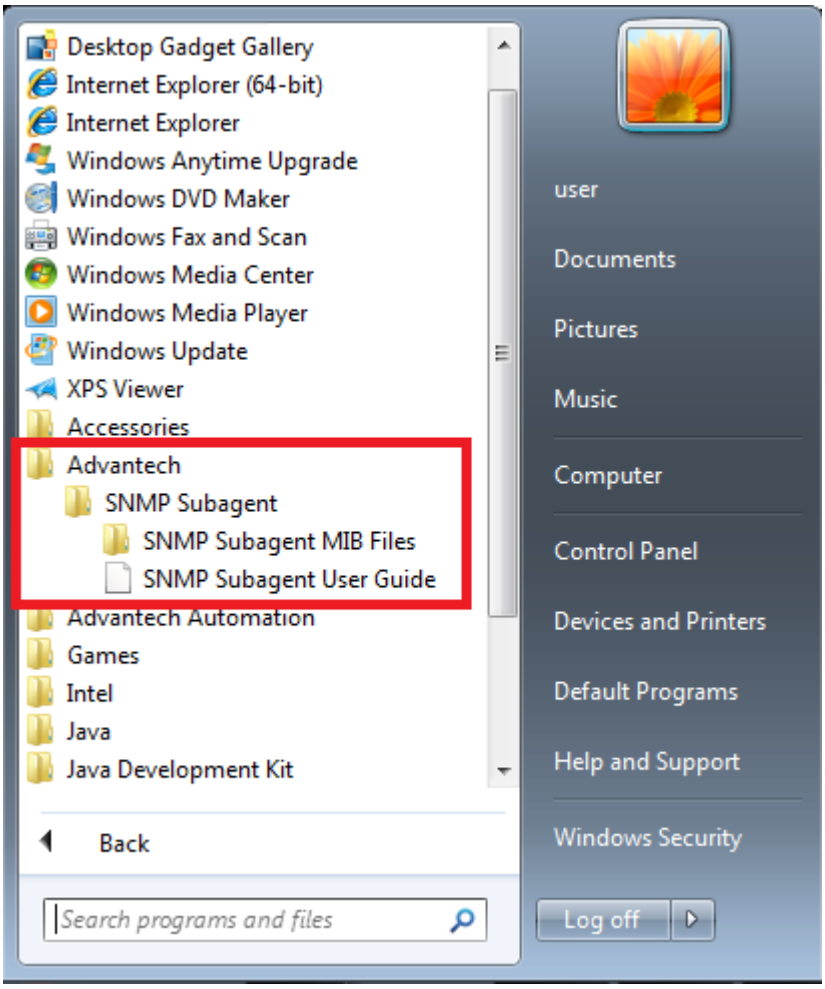

Figure 3-16 MIB Files

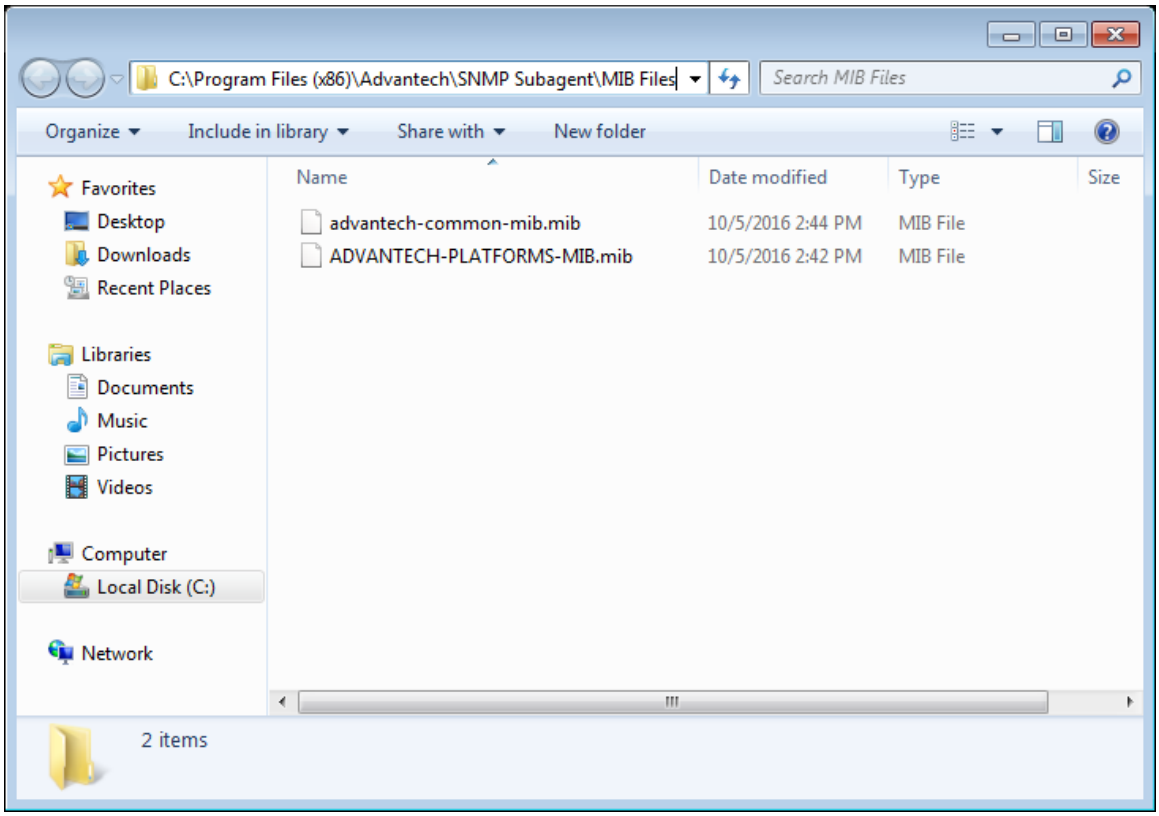

Figure 3-17 MIB Files Location

3.2 Uninstallation

To uninstall the Advantech SNMP Subagent, you can follow the following steps.

3.2.1 Launch uninstallation wizard

Go to **Control panel > Programs and Features** and select the **Advantech SNMP Subagent**. Click **Uninstall** to launch uninstallation wizard as shown in Figure 3-19.

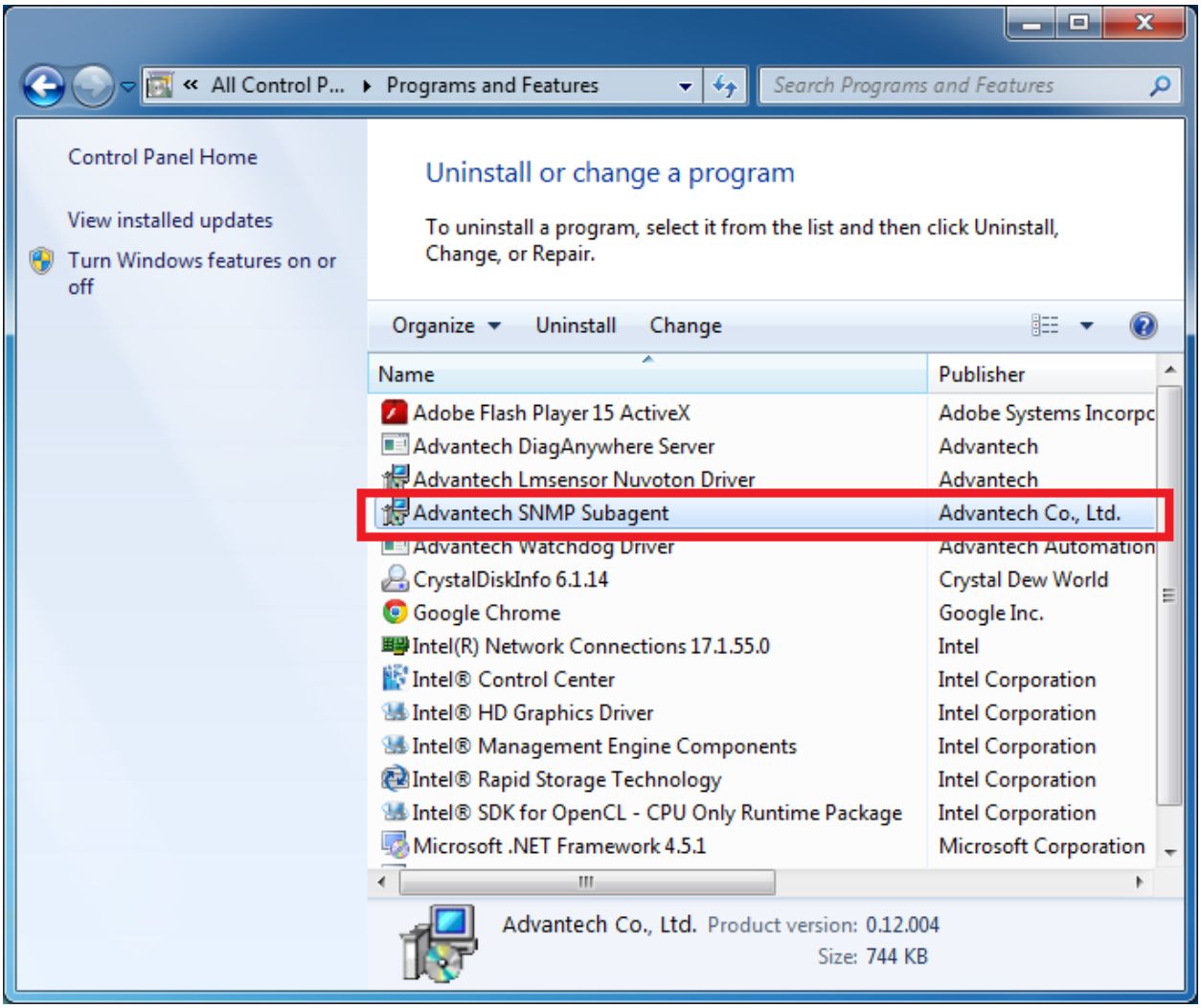

Figure 3-18 Uninstall or change a program

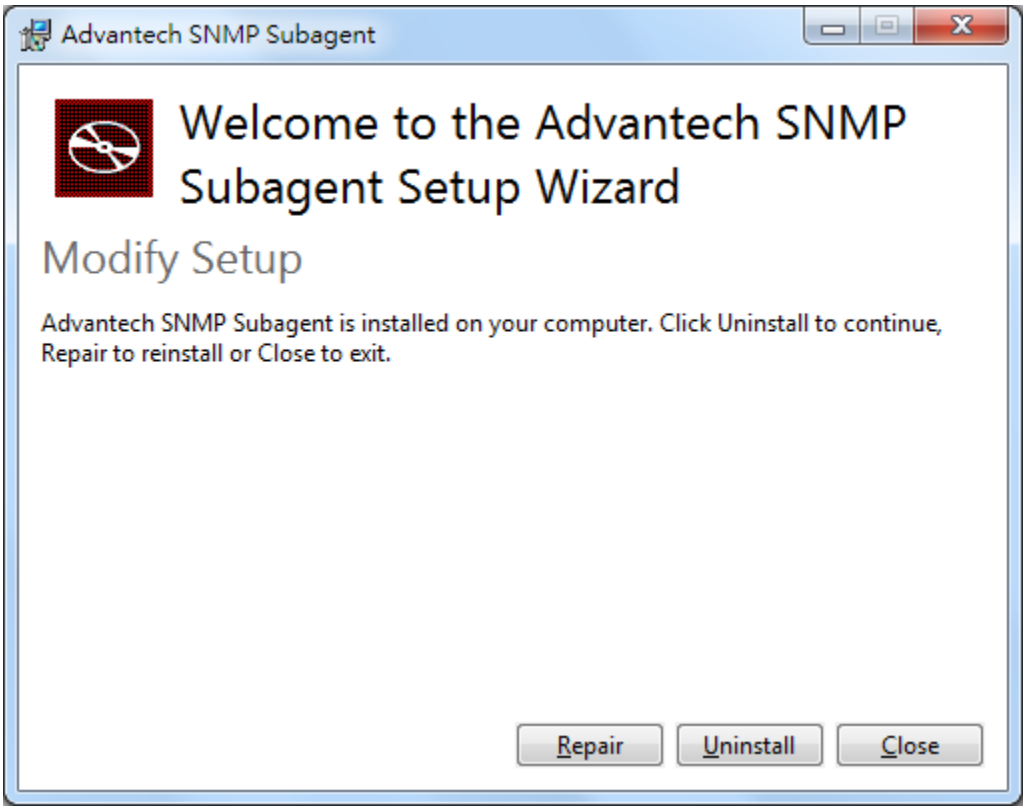

Figure 3-19 Uninstallation Wizard

3.2.2 Uninstall the Advantech SNMP Subagent

Click **Uninstall** to continue the uninstallation process and wait the subagent has been uninstalled as shown in Figure 3-21.

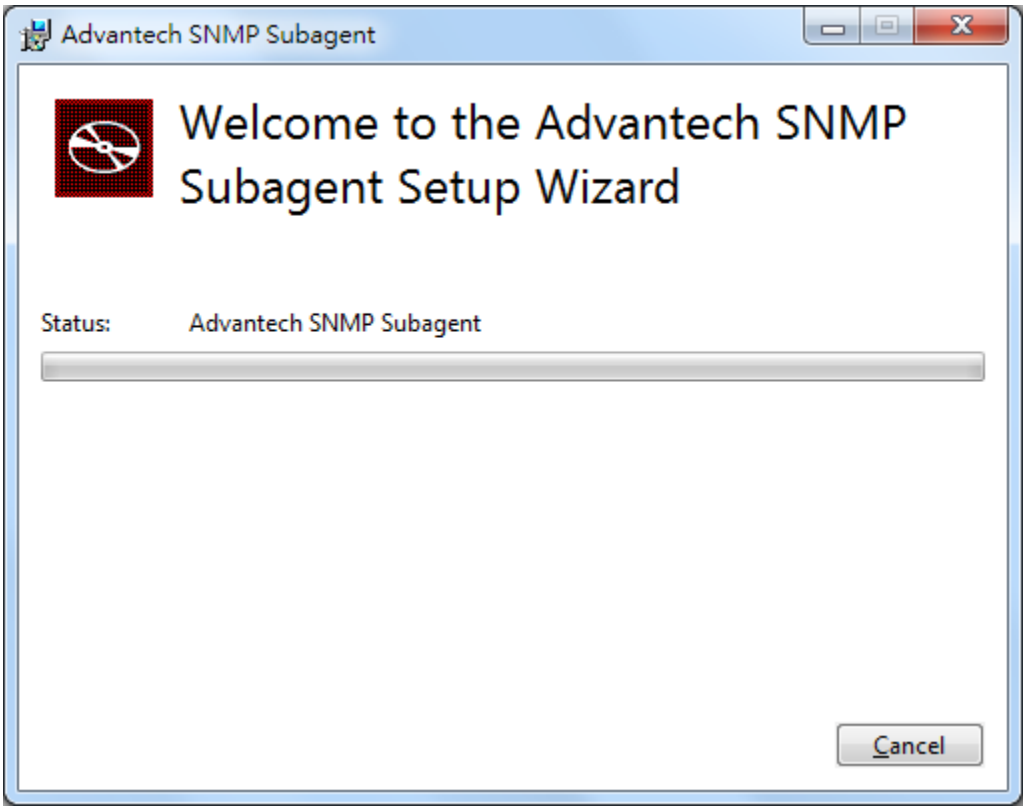

Figure 3-20 Uninstall Advantech SNMP Subagent

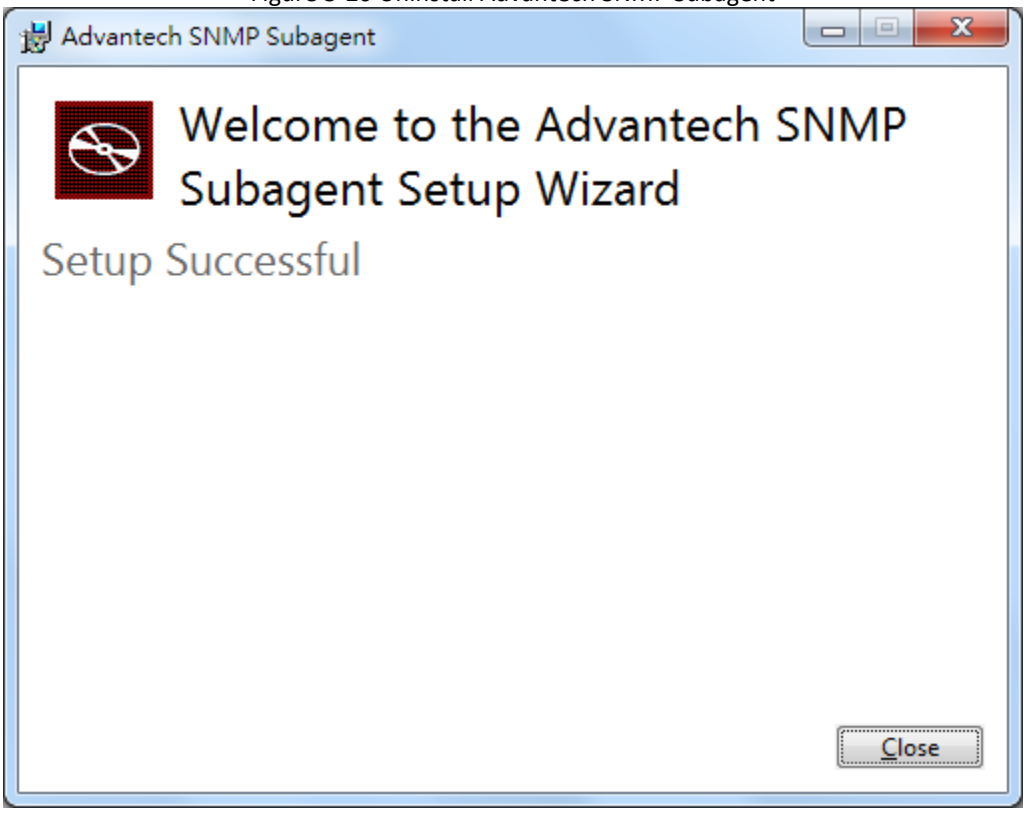

Figure 3-21 Uninstall Successful

4. Appendix

4.1 Third-Party MIB Browser

The Advantech SNMP Subagent has been tested with the following MIB Browser.

- iReasoning MIB browser
  http://ireasoning.com
- ManageEngine Free SNMP MIB Browser
  https://www.manageengine.com/products/mibbrowser-free-tool/

4.1.1 iReasoning MIB browser

Download Link: http://ireasoning.com/mibbrowser.shtml

1. Once running iReasoning MIB browser in the *client platform*, please load MIB files first.

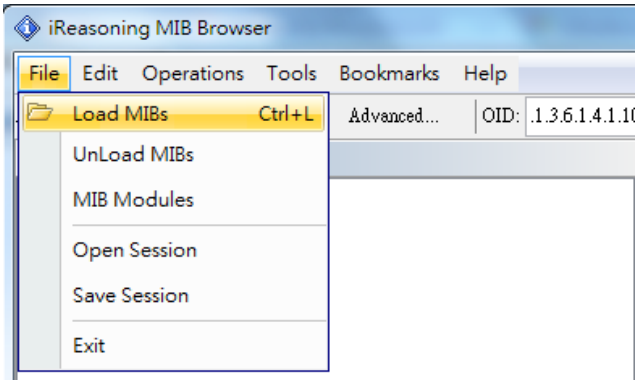

Figure 4-1 Load MIBs

2. Load *ADVANTECH-PLATFORMS-MIB.mib* and *advantech-common-mib.mib.* They are available after you installed the *Advantech SNMP Subagent*. (e.g., C:\program files\Advantech\AdvSNMPAgent\Mib). Copy these two files to your *client platform* in advance.

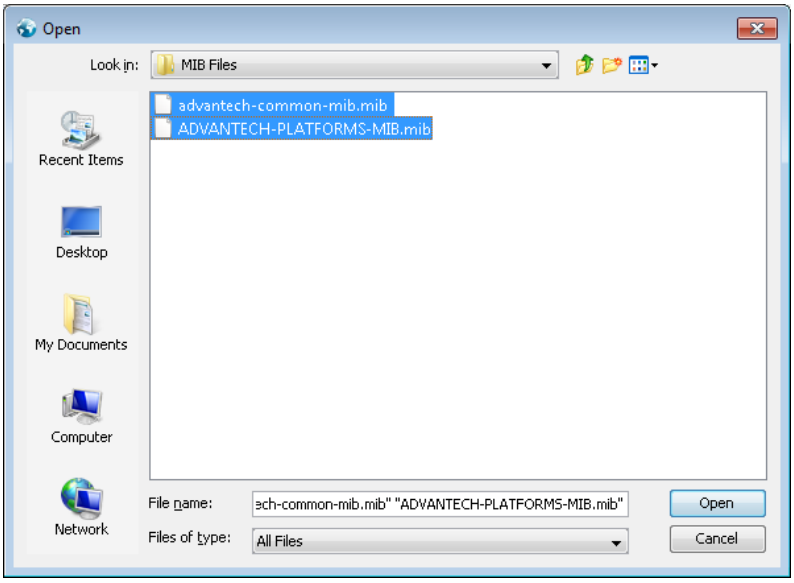

Figure 4-2 Advantech MIBs

3. Enter the IP address of the *target platform* where *Advantech SNMP Subagent* was installed.

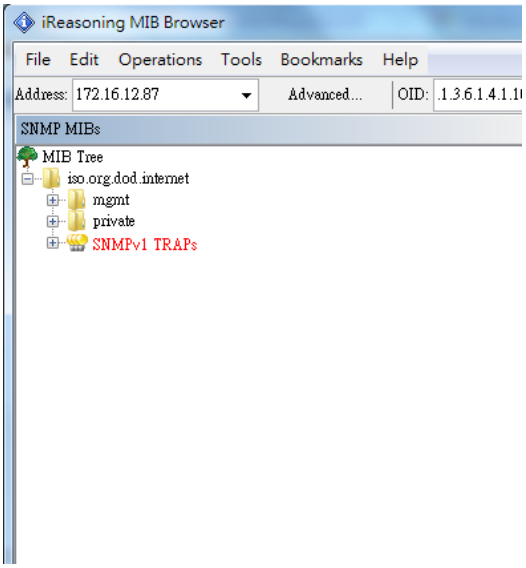

Figure 4-3 Enter IP address

4. For example, you can find **sysModuleID** as following Figure 4-4, and there is also a description at the bottom of the window.

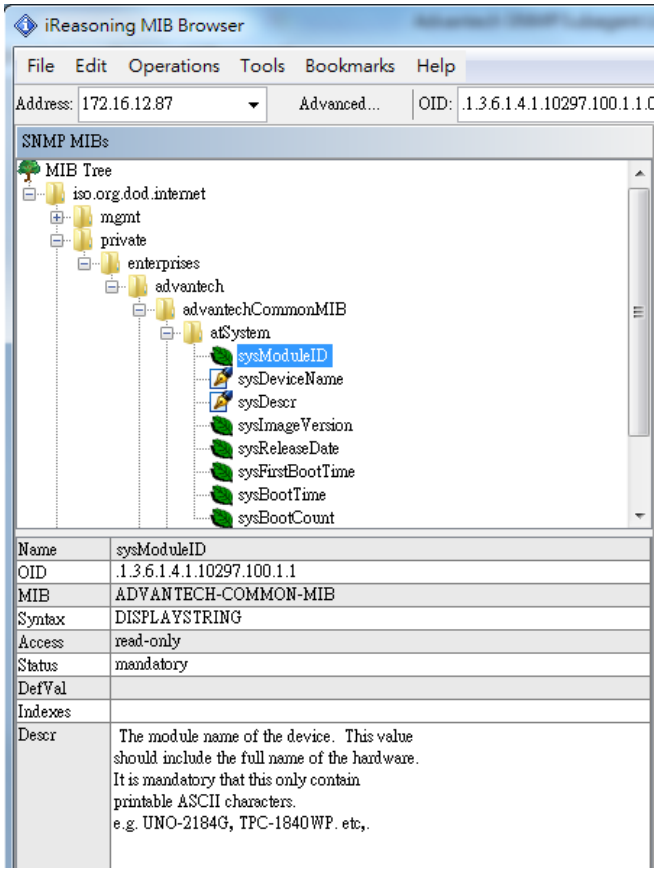

Figure 4-5 sysModuleID

5. Double click on sysModuleID. *Target platform* will reply the module/product name message at the right side of the window.

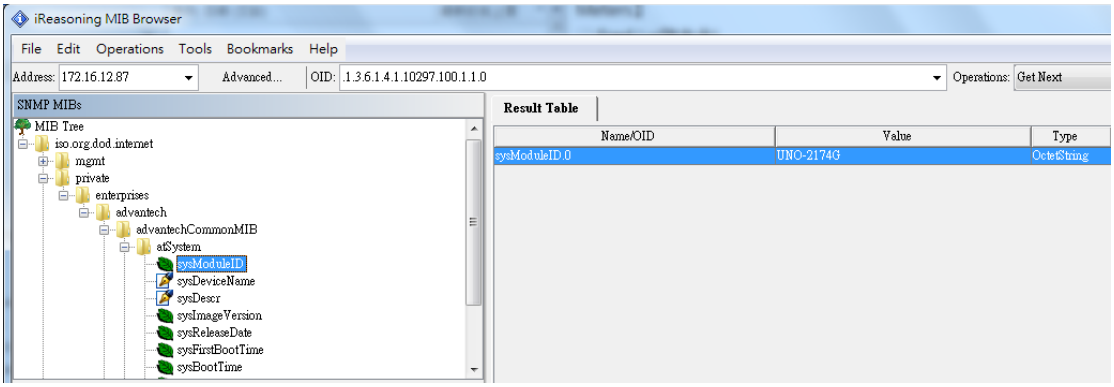

Figure 4-6 SNMP GET sysModuleID

6. You can also double click on **sysBootCount** to get reboot counter value from the *target platform,* for example.

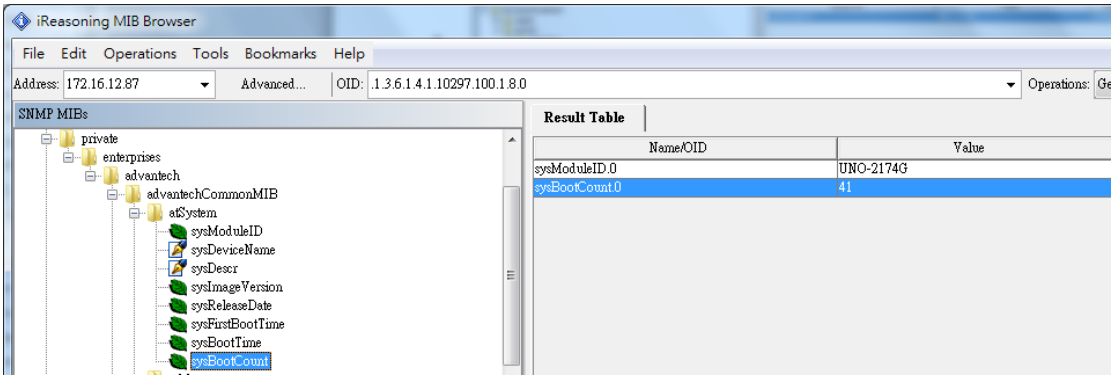

Figure 4-7 sysBootCount

7. *Advantech SNMP Subagent* also provides TRAP functions which will notify the *client platform* if alarm events happened on the *target platform*. For example, if the voltage is abnormal, SNMP will automatically send a trap to notify the user. Before the start, click the **Advanced** button and enter 'private' in the "Write Community" field.

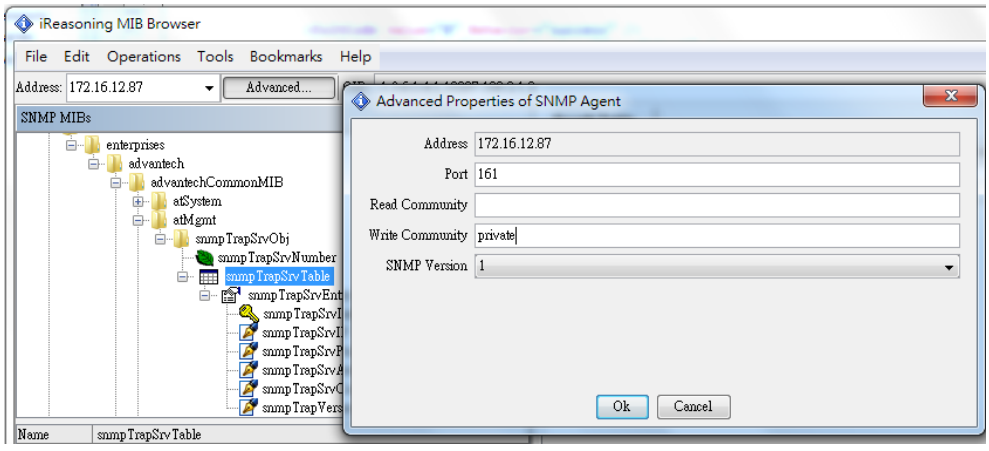

Figure 4-8 Write Community

8. Find **snmpTrapSrvTable**, right-click on it then click **Table View**.

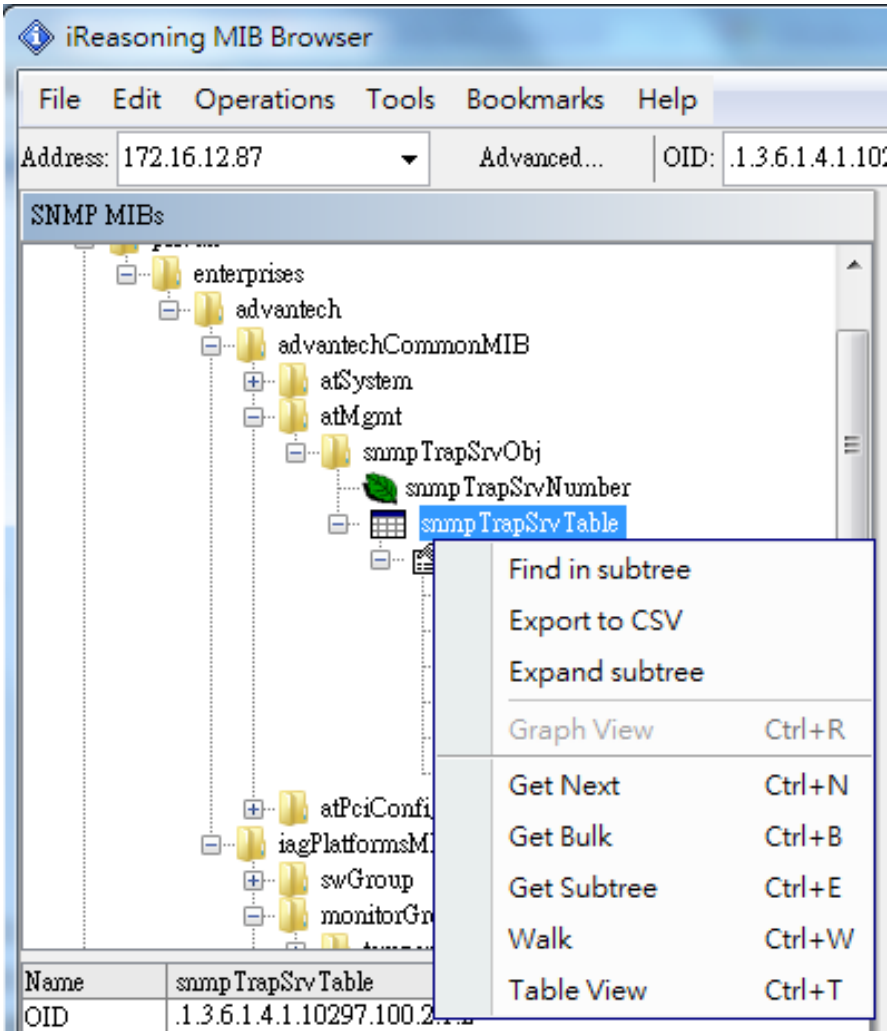

Figure 4-9 snmpTrapSrvTable

9. The Trap Server Table will show up at the right side of the window. There are **five** empty IP addresses **0.0.0.0** by default. You can update them with your *client platforms or NMS* IP addresses by *SNMP SET* command. You can also add/edit the snmpTrapSrvIP in the *Traps* tab of *SNMP Service Properties* as shown in Figure 3-10.

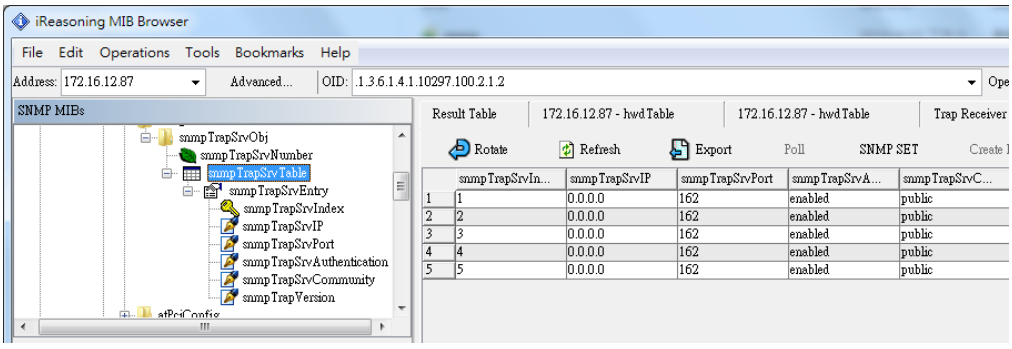

Figure 4-10 snmpTrapSrvTable with default IP addresses

10. First, click one text field of **snmpTrapSrvIP**, and click "**SNMP SET**"

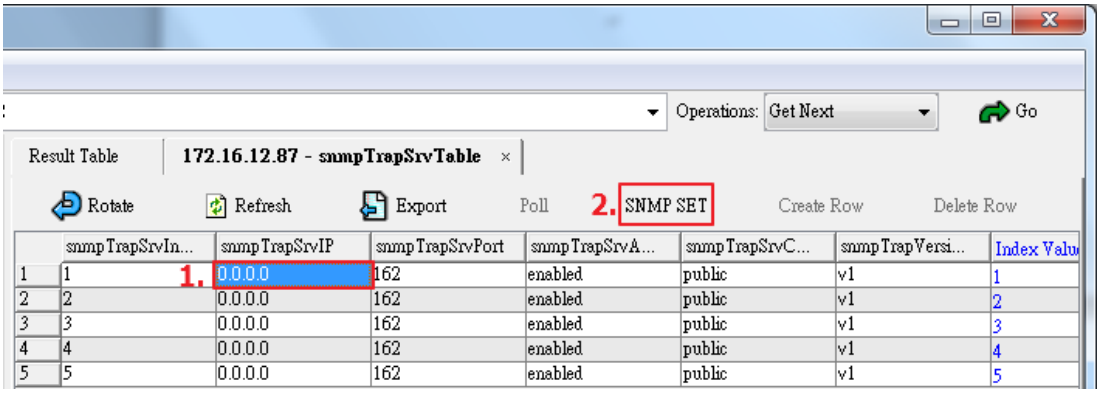

Figure 4-11 snmpTrapSrvIP and SNMP SET

11. Enter the IP address of the *client platform or NMS* in the **Value** field.

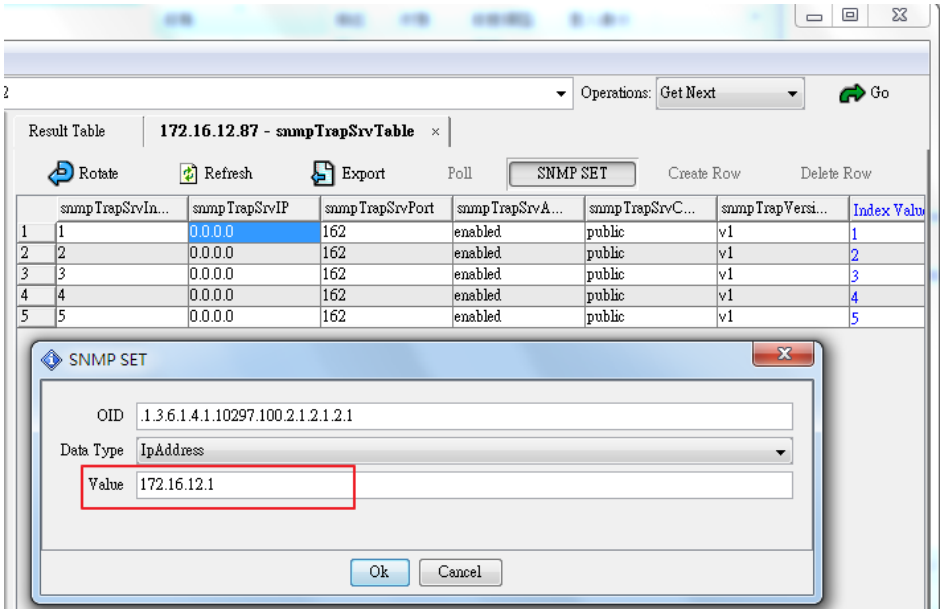

Figure 4-12 SNMP SET snmpTrapSrvIP

12. This message box "SET succeeded" is supposed to be showing up.

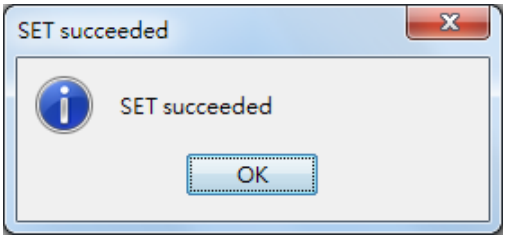

Figure 4-13 SET succeeded

13. Tools → Trap Receiver.

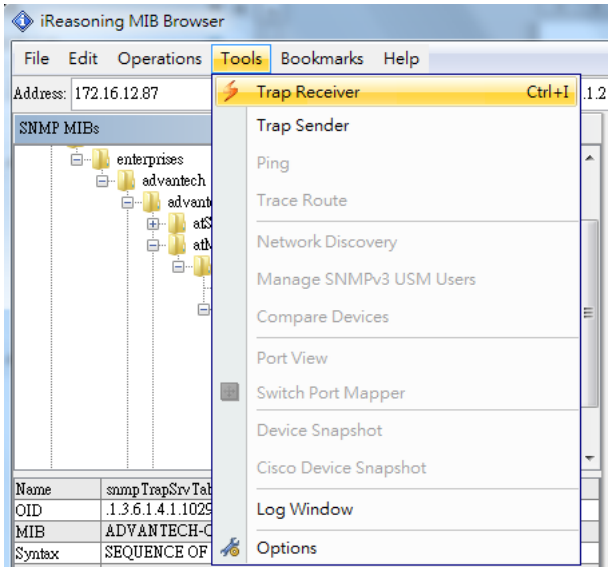

Figure 4-14 Trap Receiver

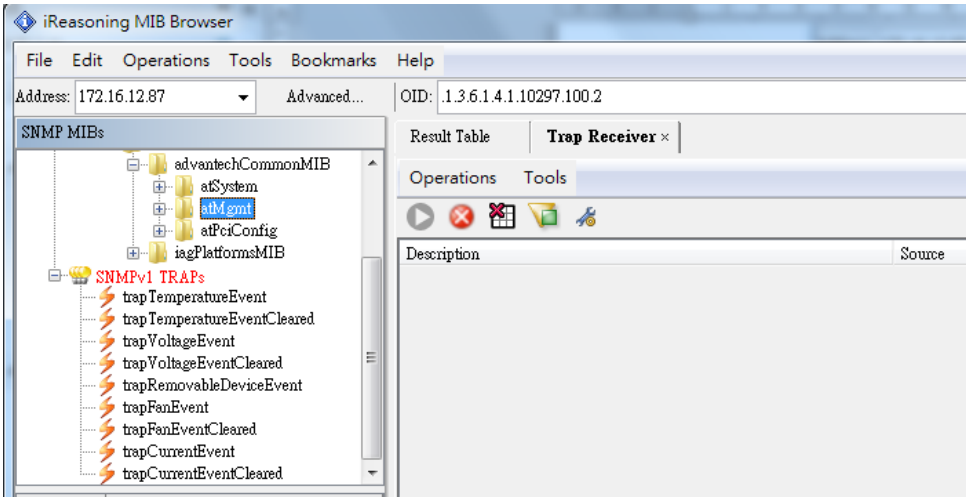

Figure 4-15 Trap Receiver Window

- Now *client platform* can receive Traps/Notifications if any device was changed on *target platform*. Please plug/remove a USB hard drive from SNMP server to verify if it works.

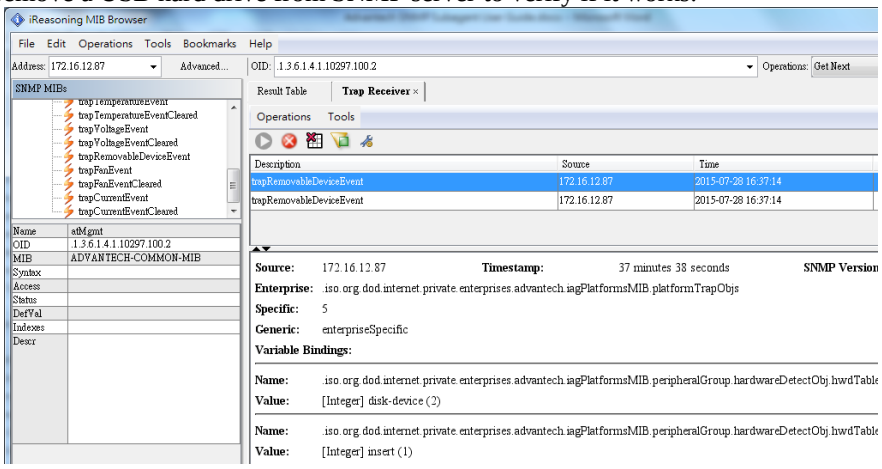

Figure 4-16 Receive Traps

14. In the example of the temperature trap, set **tpMax** to **20** and set **tpState** to be **enabled**.

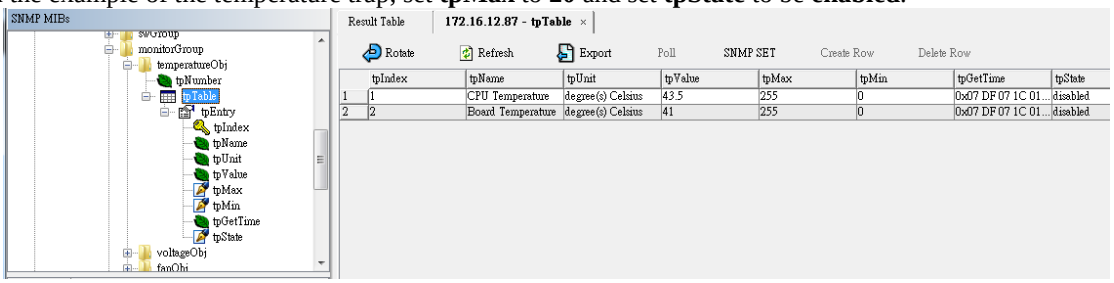

Figure 4-17 Set tpMax and tpState

(Zoom In)

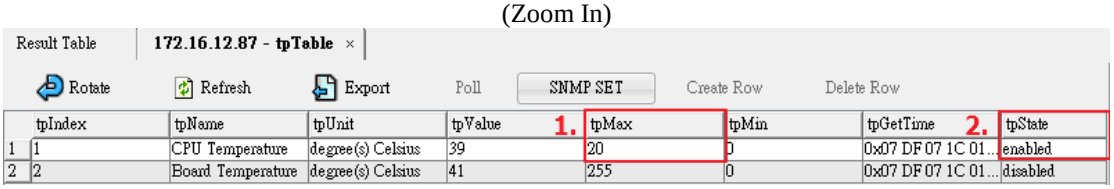

Figure 4-18 Set tpMax and tpState (Zoom In)

15. Now you will receive a trap which notifies you that the temperature is abnormal.

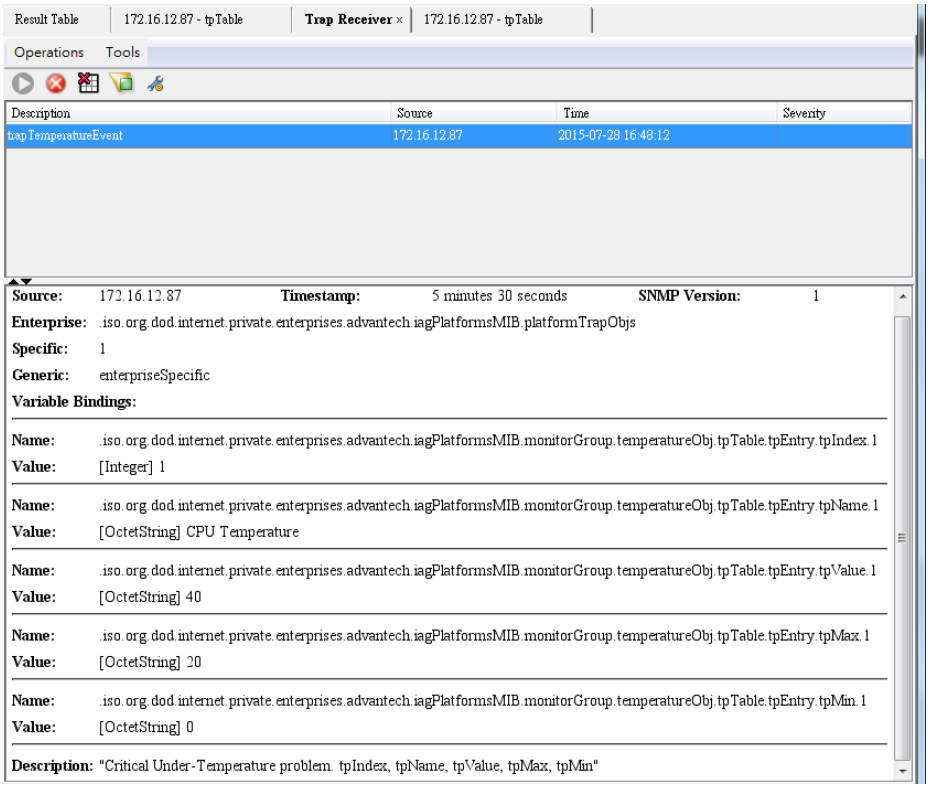

Figure 4-19 trapTemperatureEvent

4.1.2 ManageEngine Free SNMP MIB Browser

Download Link: https://www.manageengine.com/products/mibbrowser-free-tool/download.html

1. Once running ManageEngine Free SNMP MIB Browser in the client platform, please load MIB files first.

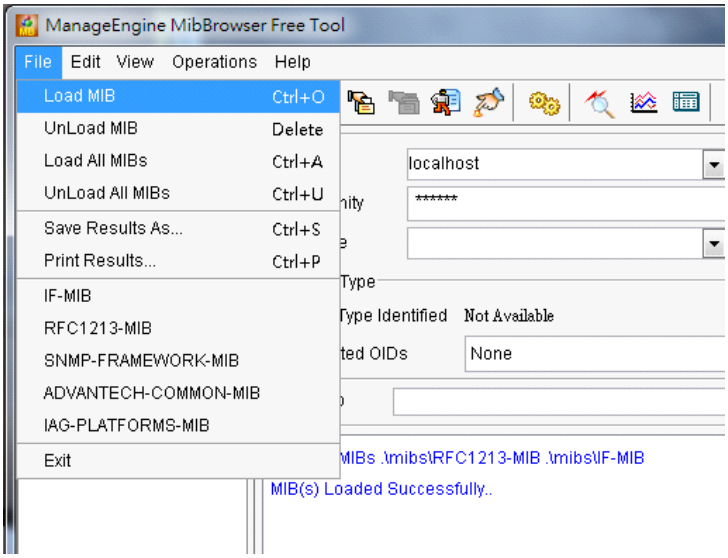

Figure 4-20 Free SNMP MIB Browser Load MIB

2. Load the *SNMP-FRAMEWORK-MIB* file from the MIB folder of the ManageEngine Free SNMP MIB Browser installation path. (e.g., C:\Program Files\ManageEngine\MibBrowser Free Tool\mibs)

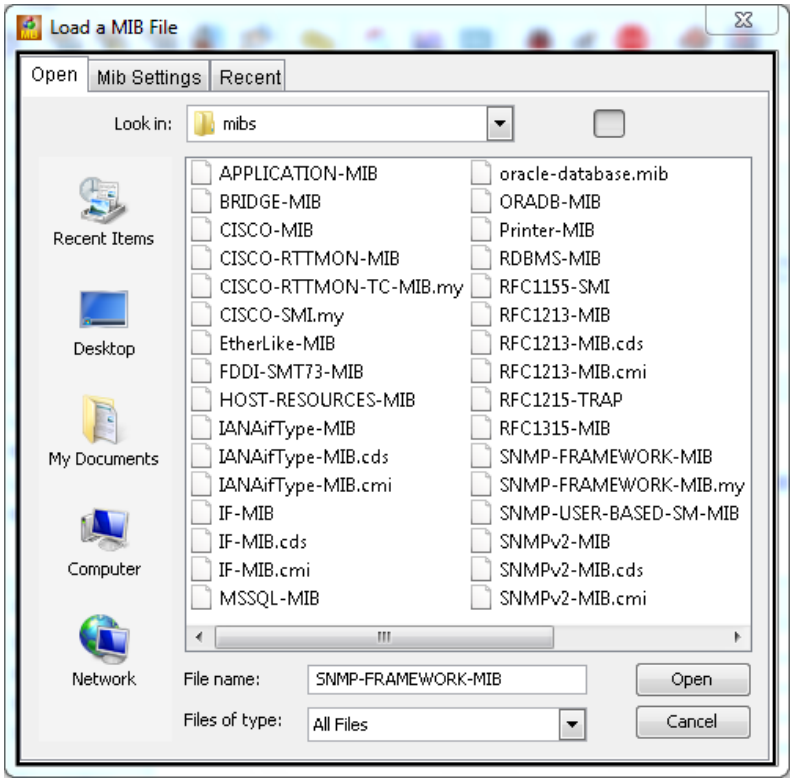

Figure 4-21 SNMP-FRAMEWORK-MIB

3. Load *ADVANTECH-PLATFORMS-MIB.mib* and *advantech-common-mib.mib*. They are available after you installed the *Advantech SNMP Subagent*. (e.g., C:\program files\Advantech\AdvSNMPAgent\Mib). Copy these two files to your *client platform* in advance.

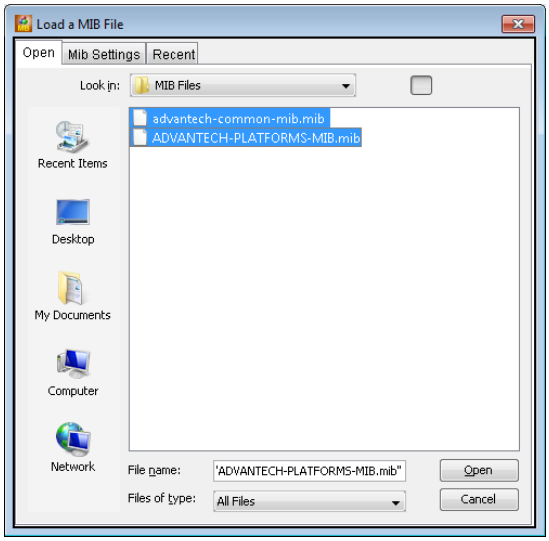

Figure 4-22 Advantech MIBs

4. Enter the IP address of the *target platform* where *Advantech SNMP Subagent* was installed in the **Host** field. Enter 'public' in the **Community** field and 'private' in the **Write Community** field.

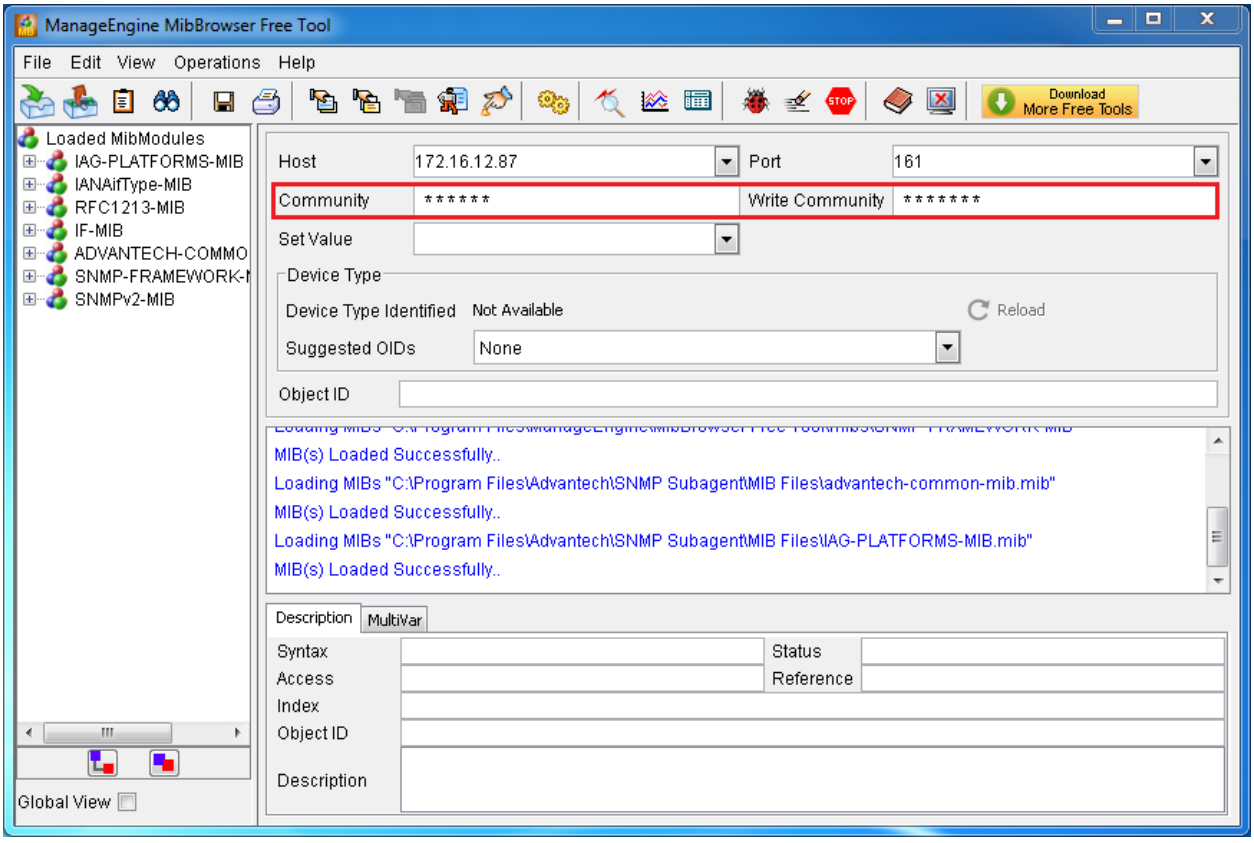

Figure 4-23 Community and Write Community

5. For example, you can find **sysModuleID** as the following Figure 4-24. Find **sysModuleID**, right-click on it then click **GET**

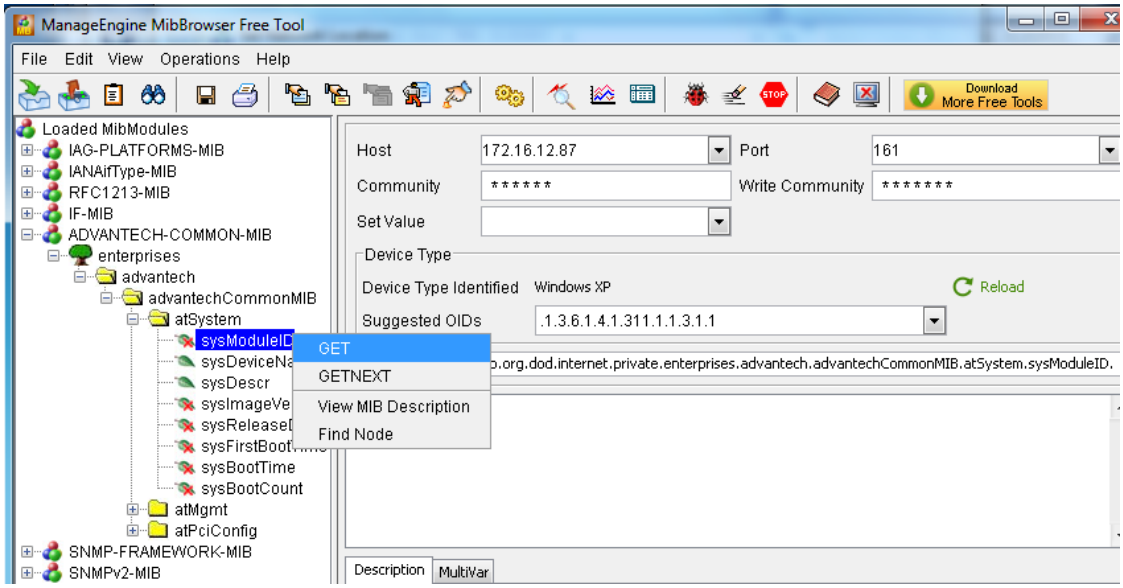

Figure 4-25 GET sysModuleID

6. The *target platform* will reply the module/product name message at the result window.

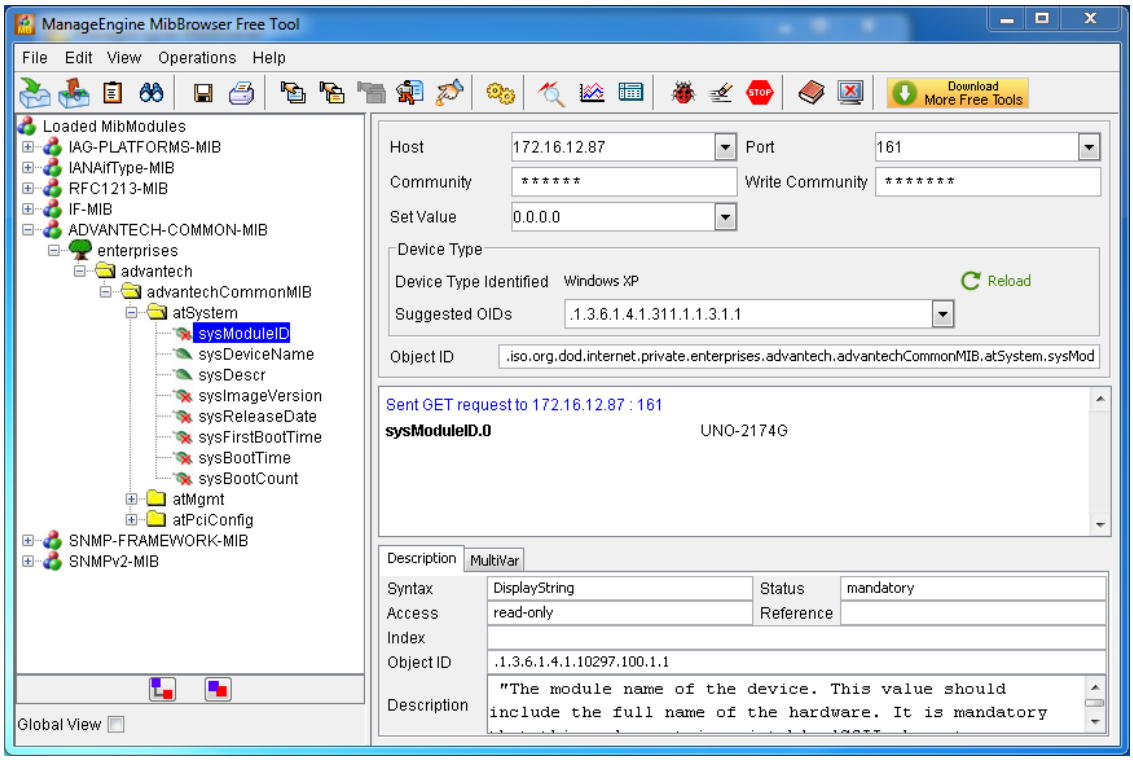

Figure 4-26 sysModuleID.0

7. You can also right-click on **sysBootCount**, and then click **GET** to get reboot counter value from *target platform*, for example.

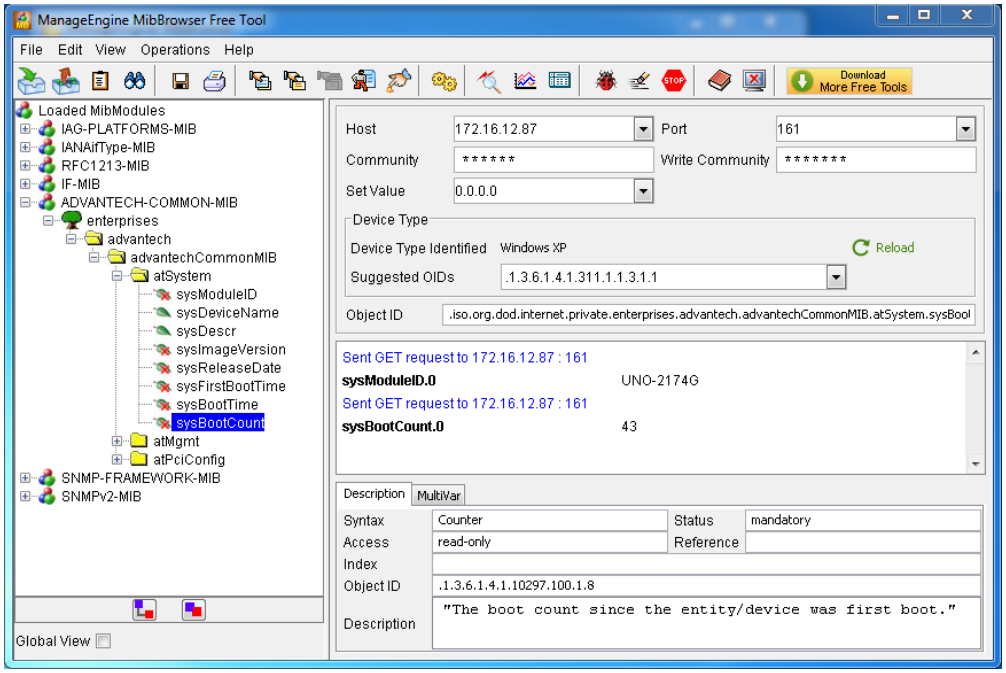

Figure 4-27 sysBootCount.0

8. *Advantech SNMP Subagent* also has TRAP functions which will notify the *client platform* if alarm events occurred on the *target platform*. For example, if the voltage is abnormal, SNMP will automatically send a trap to notify the user. Find **snmpTrapSrvTable**, click **View SNMP Data Table** on the toolbar.

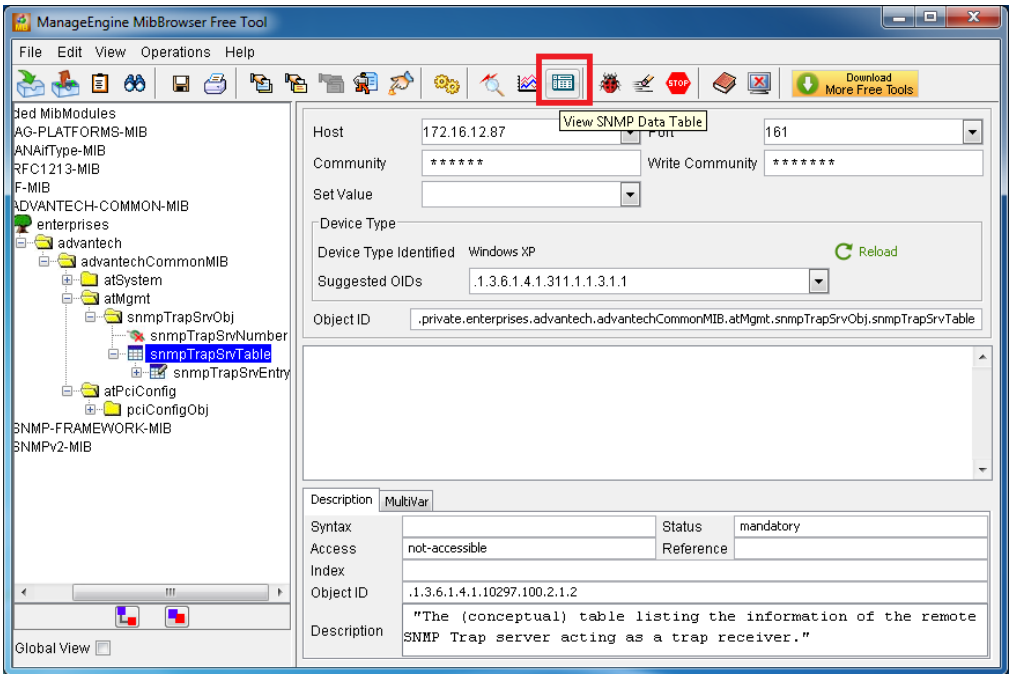

Figure 4-28 View SNMP Data Table

9. It will display an *SNMP Table* as below and then click **Start** to get the data.

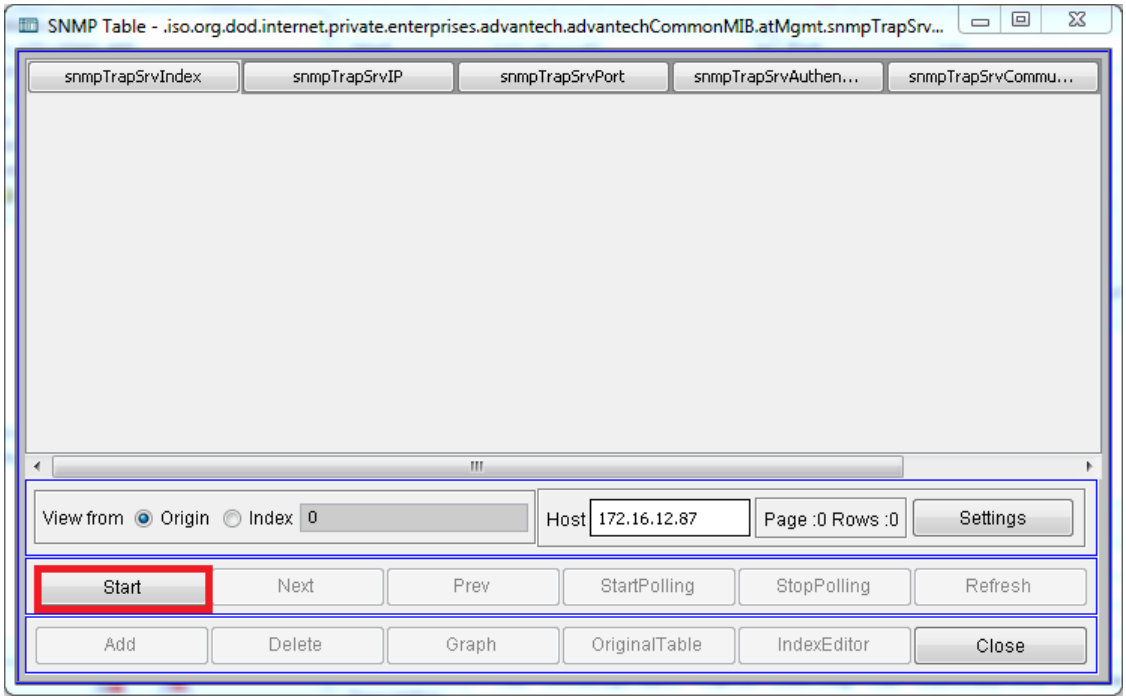

Figure 4-29 SNMP Table

10. The snmpTrapSrvTable will show up as below figure. There are **five** empty IP addresses **0.0.0.0** by default. You can update it with your *client platform or NMS* IP address by *SNMP SET* command. You can also add/edit the snmpTrapSrvIP in the *Traps* tab of *SNMP Service Properties* as shown in Figure 3-10.

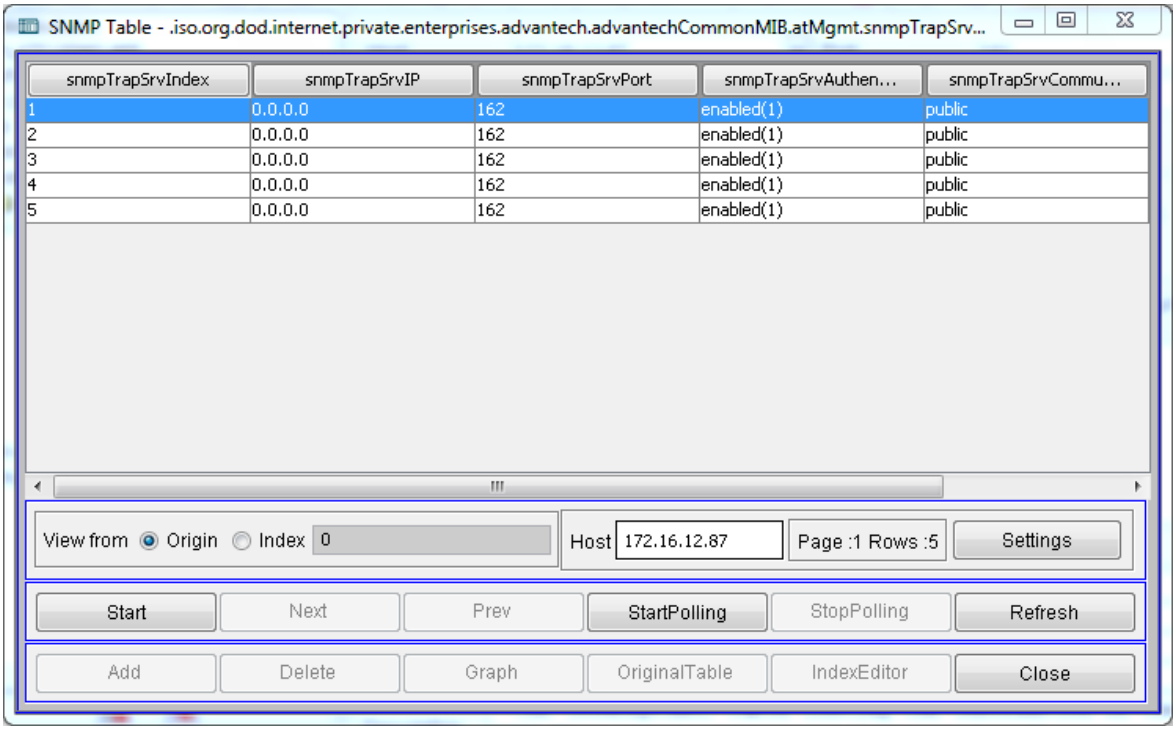

Figure 4-30 snmpTrapSrvTable data

11. Click on the each snmpTrapSrvIP text field and enter the IP address of the *client platform or NMS* and then click the **Refresh** button to make sure the IP address has been updated.

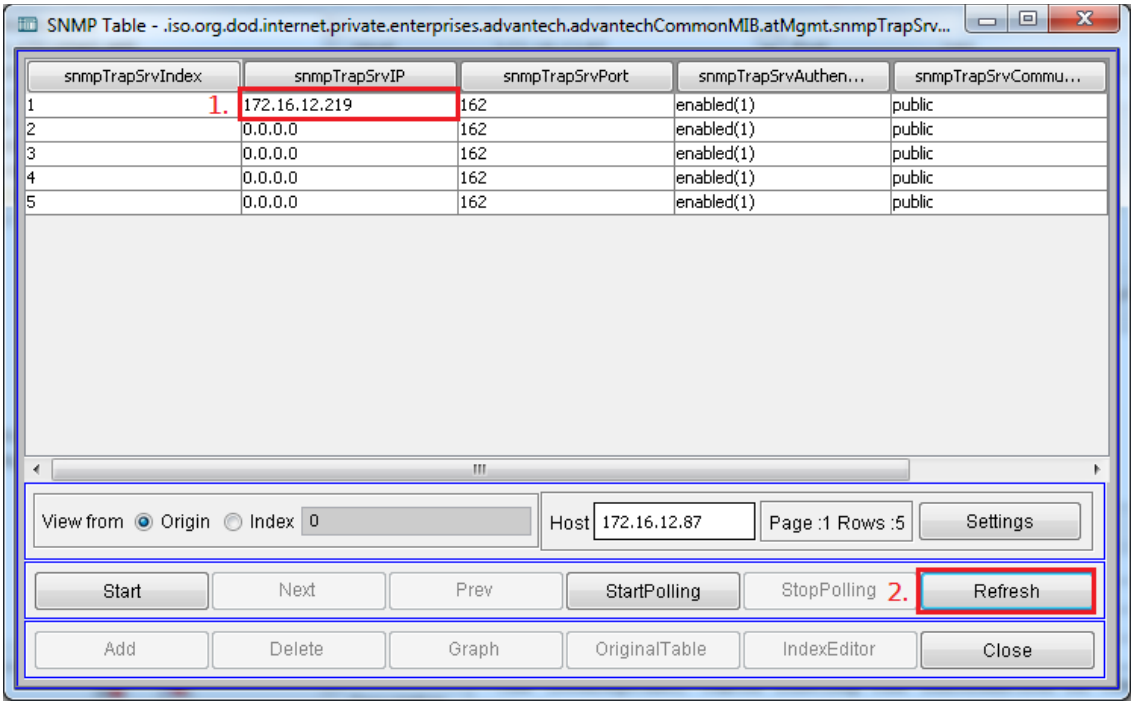

Figure 4-31 Set snmpTrapsrvIP

12. Click **Trap Viewer UI** icon on the toolbar.

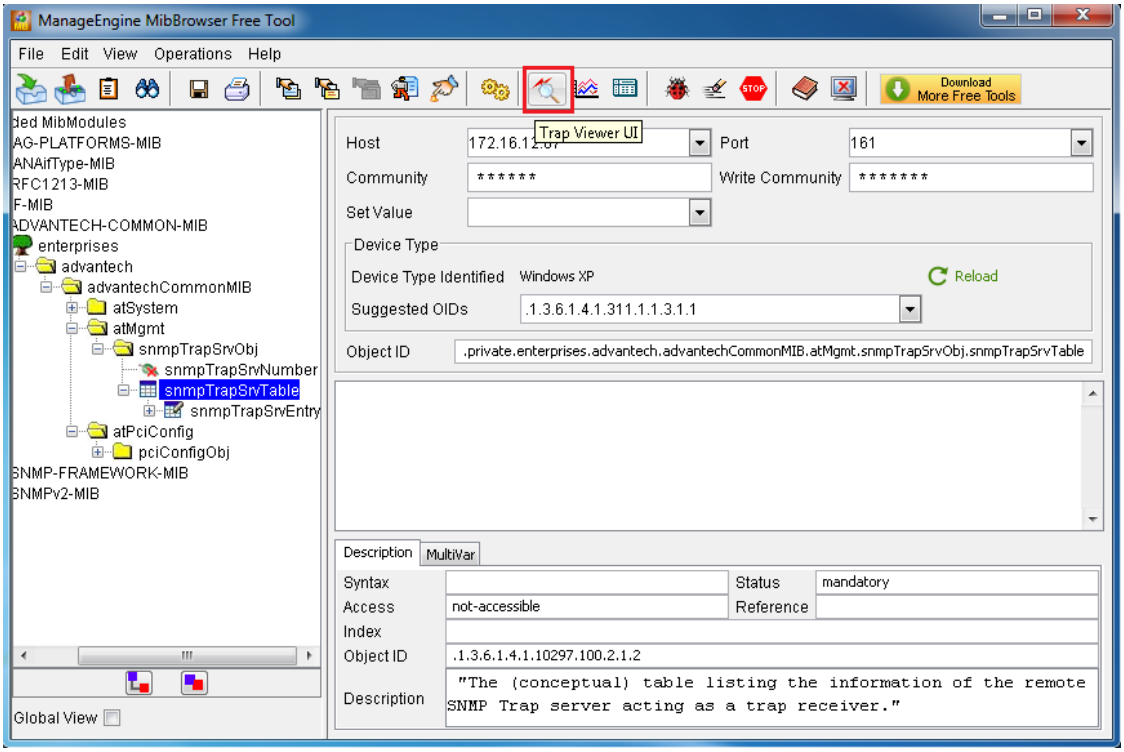

Figure 4-32 Click Trap Viewer UI

13. Now *client platform* can receive Traps/Notifications if any device was changed on the *target platform*. Click Start to listen for Traps.

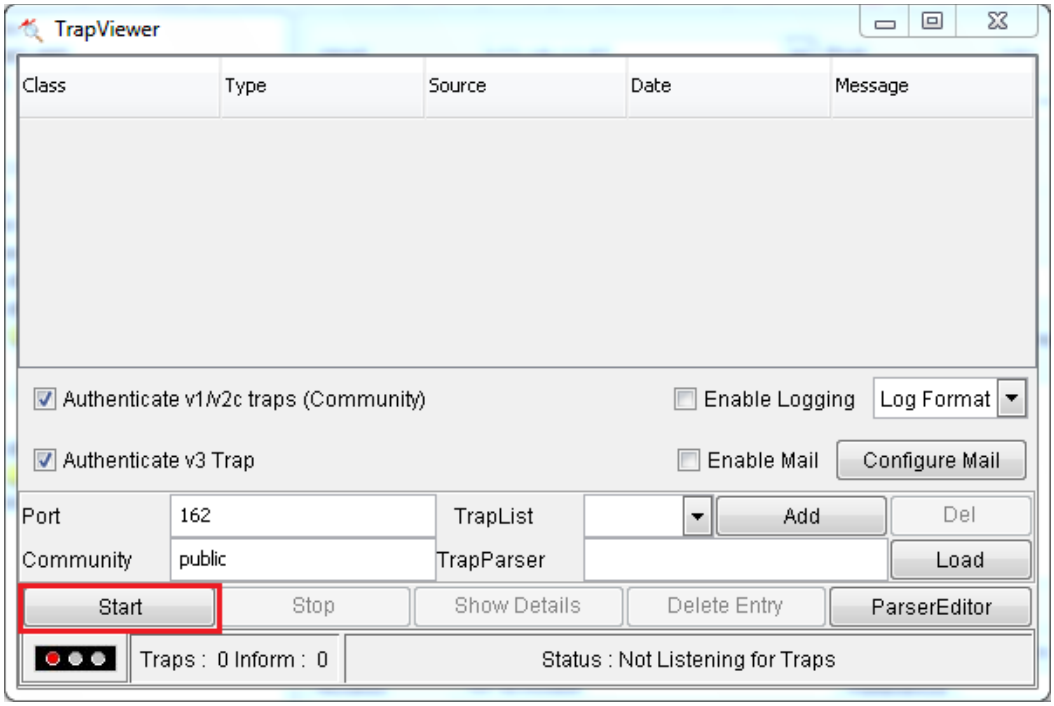

Figure 4-33 TrapViewer

14. Please plug/remove a USB hard drive from SNMP server to verify if it works. Click **Show Details**

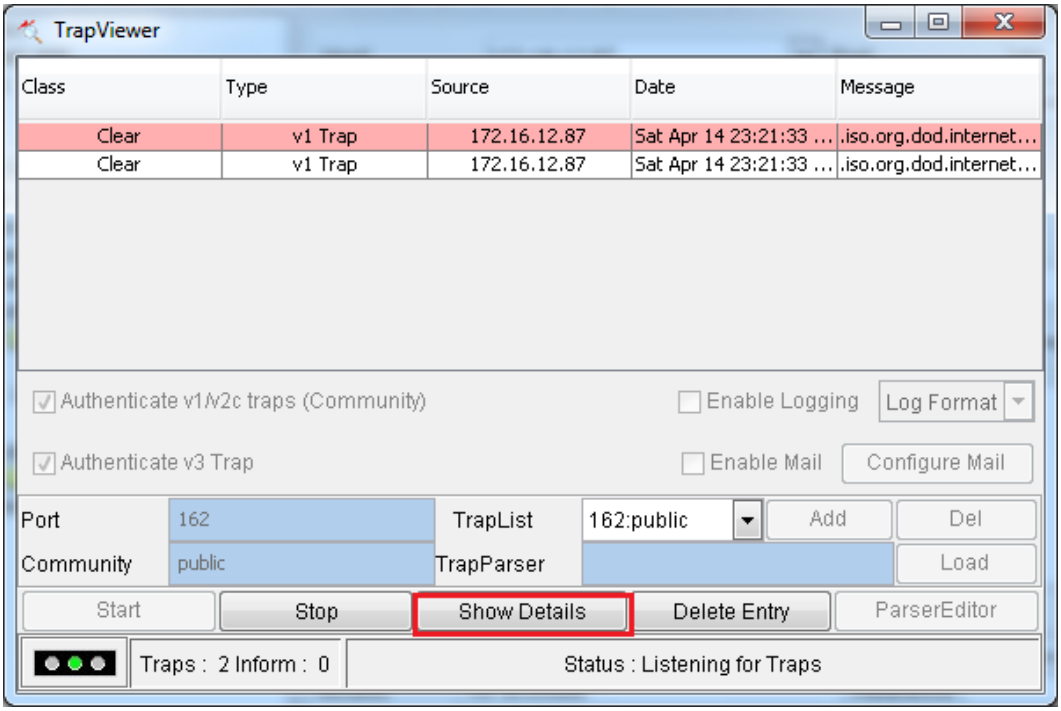

Figure 4-34 USB hard driver removed

15. It will display a Trap Details window as Figure 4-35.

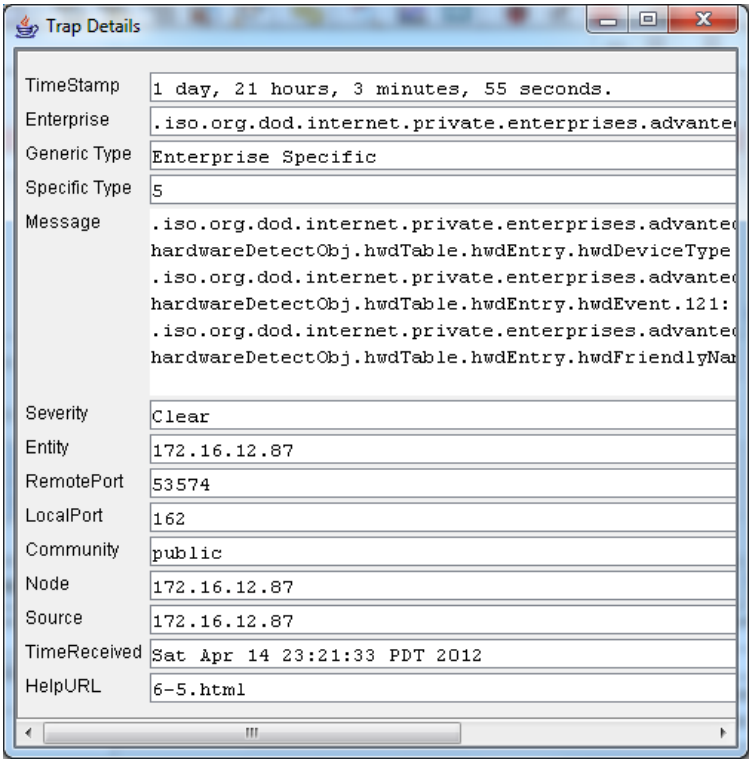

Figure 4-36 Trap Details

16. In the example of the temperature trap. Find **tpTable**, click **View SNMP Data Table** on the toolbar. In the SNMP Table set **tpMax** to **20** and set **tpState** to be **enabled**.

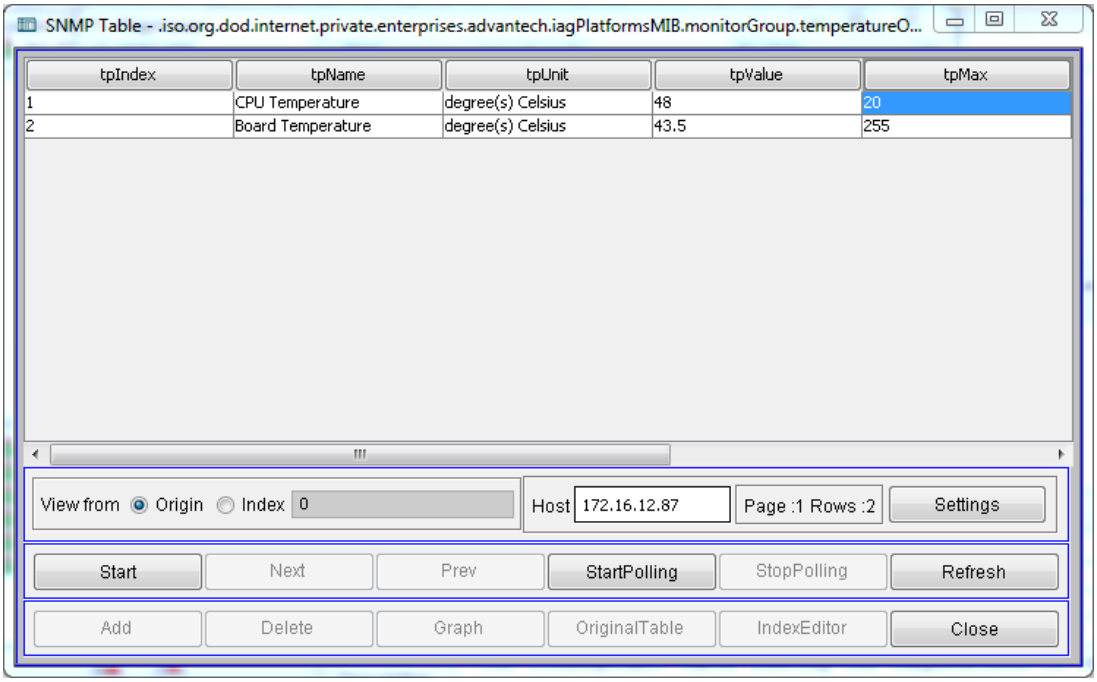

Figure 4-37 Set tpMax

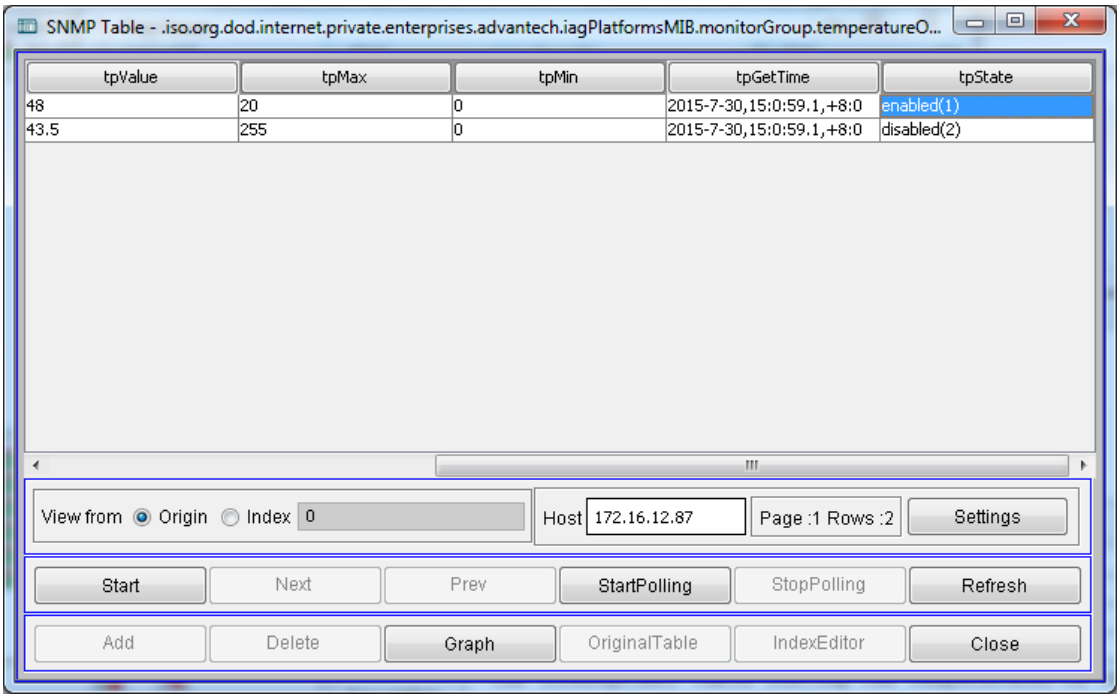

Figure 4-38 Set tpState

17. In the TrapViewer window, you can see a trap, click **Show Details** to get more information.

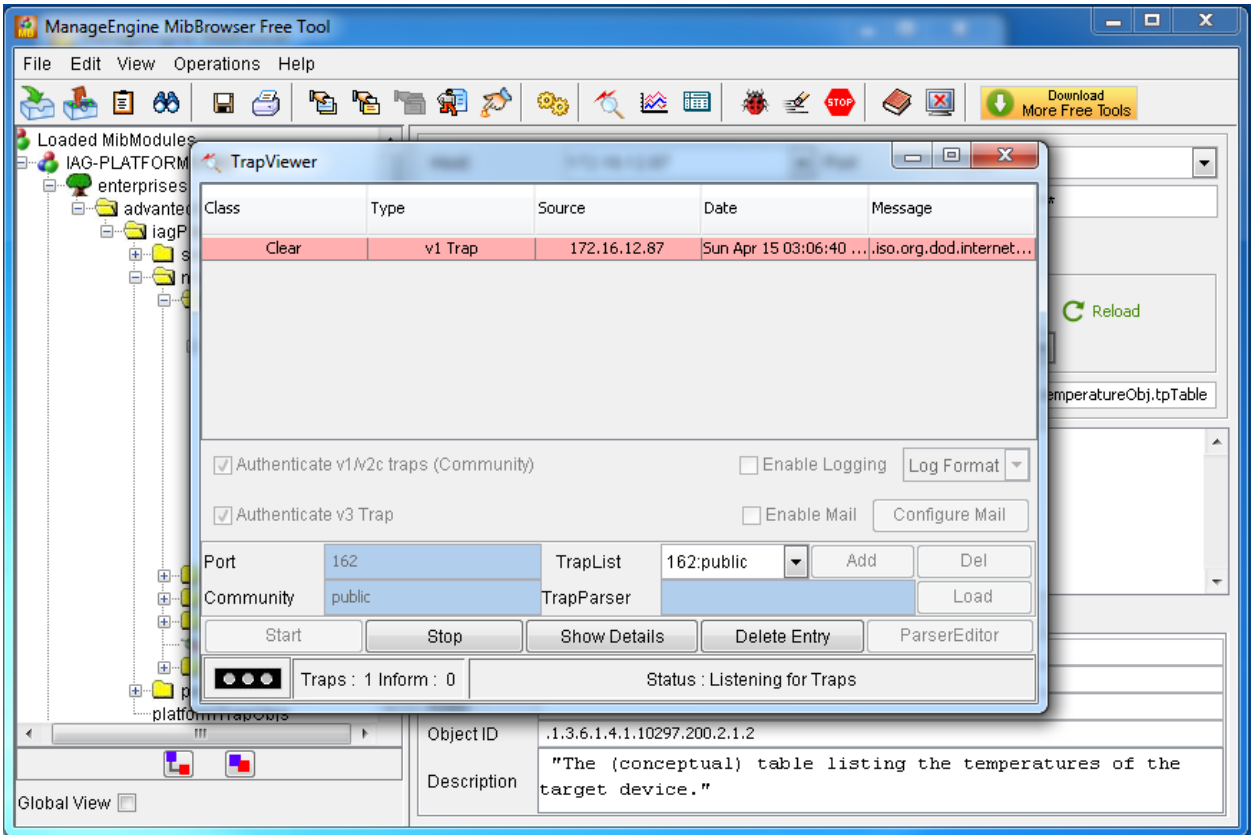

Figure 4-39 TrapViewer

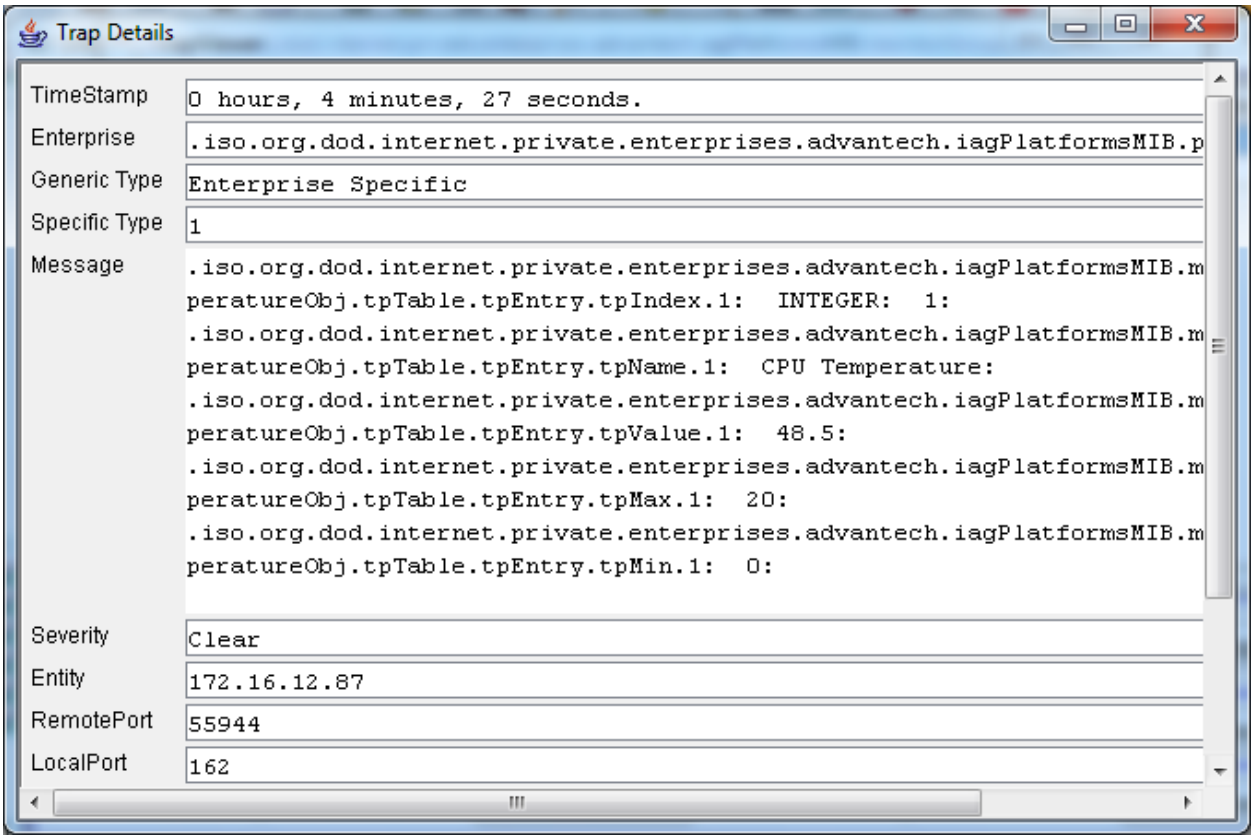

Figure 4-40 Trap Details