ASUS System Management Application Notes

User Notice

No part of this product, including the product and software may be reproduced, transmitted, transmitted, transcribed, stored in s retrieval system, or translated into any language in any form by any means with the express written permission of ASUSTek COMPUTER INC. except documentation kept by the purchaser for backup purpose.

This manual introduces the fundamental Server Management knowledge, the hardware support in ASMM board . This note provides features and architecture of the ASMM product for the server and the console.

Table of Contents

1. Introduction ---------- 3

1.1 What is the ASUS System Management ---------- 3

1.2 ASMM Overview ---------- 3

1.3 ASMA Overview ---------- 4

1.4 SNMP Overview ---------- 8

1.5 Terminology ---------- 9

2. ASMA installation and configuration ---------- 10

2.1 Installation Tip ---------- 10

2.2 Configuration ---------- 10

2.3 Troubleshooting ---------- 15

3. NT Performance Monitor ---------- 17

4. NT Event Viewer ---------- 22

5. NT Web Admin ---------- 25

6. ASUS LDSM OEM Release ---------- 28

7. SNMP Management Station ---------- 45

7.1 HP Openview ---------- 45

7.2 Microsoft SMS ---------- 51

7.3 Solaris Solstice Site/SunNet/Domain Manager ---------- 58

7.4 CA-TNG ---------- 63

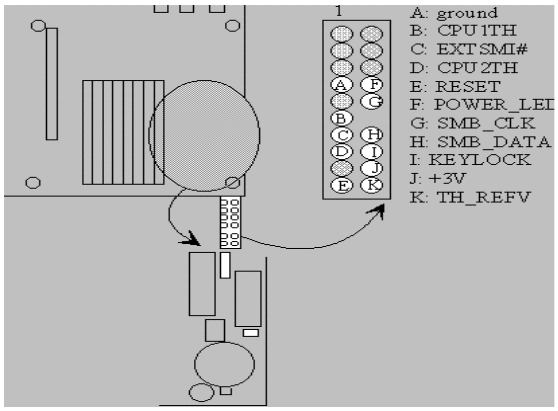
Chapter 1 Introduction

1. 1 What is the ASUS System Management

There are two components for ASUS System Management. One is ASMM – ASUS System Monitoring Module, the other one is ASMA – ASUS System Monitoring Agent. ASMM had been implemented on an ISA card and ASUSTek mainboards. This hardware module provides Fan speed, Voltage, Temperature and Chassis Intrusion information of system and Automatic Server Restart function. ASMA contains ASMM's driver and its SNMP agent. Through SNMP Agent, Network management software such as HP OpenView can monitor the system's fan speeds, working voltage and system temperature. SNMP Agent will report to Network Manager immediately to prevent problems from getting worse when the server's in an abnormal state.

1.2 ASMM Overview

ASUS System Monitoring Module, is a hardware portion of this management environment. There are two kinds of implementation for this part. One is ISA card implementation, the other one is mainboard implementation.
Basically the ASMM card is a 8 bit ISA Server Monitoring Card which includes a 20-pin external feature connector for ASUSTek SMH (Server Monitoring Header).



The connections are classified into 2 categories: Chassis Intrusion and Fan Monitor: Chassis Intrusion: Chassis Intrusion permits the activation of a user-installed alarm. One 3 wires cable supports the external customized chassis intrusion alarm. The pin definition are : RED (battery power), YELLOW (intrusion signal), and BLACK (ground). The external intrusion signal should be open-drained. Fan Monitor: The fan monitor provides

power for up to 3 fan while monitoring the connected fans' rotation through the specially designed tachomter. Three 3 wire cables are used to extend the length of each fan connection. The pin definitions are: YELLOW (tachometer signal), RED (+12V) , and BLACK (ground).

The system can be notified when the voltage/temperature/fan speed exceeds the predefined thresholds. The notification mechanism can be a simple as polling or through SMI#/IRQ service routine, depending on the programming of LM78. Five ISA IRQ can be selected (IRQ 3,4,5,6,7) through hardware jumper.

If your motherboard has equipped with LM78 chipset, system will report an warning message as both LM78s (The on board and the one on ASMM) use the same I/O address which is necessary for LDSM software that LM78 is located at I/O address of 0x295. The basic idea for testing the LM78 function of ASMM is to disable the on-board LM78. The ASR related function gets no influence of LM78 and need to do nothing for disable any function. Currently, the BIOS cannot auto-detect the on-board LM78 and LM78 on ASMM such that a hardware conflict occurs and results in a system warning. Future BIOS will automatically disable the onboard LM78 if the ASMM is detected. There is a chip on the motherboard at the rear edge about in the middle of the plug in slots called and LM78. It's a chip made by National Instruments and it's the LM78 that provides the circuitry for monitoring the motherboard hardware such as fan RPM's and Temp. There are several features:

Fan Status Monitoring and Alarm: To prevent system overheat and system damage, the CPU fan and system fans are monitored for failure. Each fan can be set for its alarm thresholds.

Voltage Monitoring and Alert: System voltage levels are monitored to ensure stable current to critical motherboard components. Voltage specifications are more critical for future processors, so monitoring is necessary to ensure proper system configuration and management.

System Resources Alert: Today's operation systems, such as Windows 95, Windows NT and OS/2, require much more memory and hard drive space to present enormous user interfaces and run large applications. The system resource monitor will warm the user before the system resources are used up to prevent possible application crashes.

If you want to maintain mainboard, you must use jumper to disable Photo Sensor Chassis Intrusion. If you do not disable Photo Sensor Chassis Intrusion, the capacity of battery will be lost when you maintain mainboard.

1.3 ASMA Overview

ASUS System Monitoring Agent is a SNMP agent. This software enable the computer to be managed by Network Management Station (NMSs) through Internet. ASUS System Monitoring Agent can report the computer fan speeds, working voltage, system temperature and chassis intrusion to NMS. ASUS System Monitoring Module can enable or disable Automatic Server Restart (ASR) function from NMS through the Internet. ASR is a function that can reboot the computer system automatically when the computer system is hang. ASR and Chassis Intrusion functions must have ASMM card or its hardware circuit/components installed on the computer system. However, the P2B-DS motherboard already included ASR and Chassis Intrusion There are several manageable environments for ASMA:

NT Performance Monitor - is a graphical tool for measuring the performance of your own computer or other computers on a network. On each computer, you can view the behavior of objects, such as processors, memory, cache, threads, and processes. Each of these objects has an associated set of counters that provide information about device usage, queue lengths, delays, and information used to measure throughput and internal congestion. It provides charting, alerting, and reporting capabilities that reflect both current activity and ongoing logging. You can open, browse, and chart log files later as if they reflected current activity.

NT Event Viewer - is the tool you can use to monitor events in your system. You can use Event Viewer to view and manage System, Security, and Application event logs. You can also archive event logs. The event-logging service starts automatically when you run Windows NT. You can stop event logging with the Services tool in Control Panel.

NT Web Administration - for Microsoft Windows NT Server enables you to remotely administer Microsoft Windows NT Server using existing HTML browsers. Web Administration is not designed to replace existing administrative tools for Windows NT servers; instead, it is to enable you to perform limited administrative tasks when you are roaming, away from your usual workstation.

LANDesk Server Manager - provides network administrators with a proactive management solution and emergency management recovery Tools to help maximize business-critical server uptime. From a centralized console, LANDesk Server Manager monitors critical parameters on either Microsoft NT or Novell Netware servers. Through enhanced alerting features and server health monitoring, LANDesk Server Manager products notify the LAN administrator when a server reaches a predefined threshold.

SNMP Management Stations – there are several management programs in the market. One of the SNMP programs from HP is Openview, which is to control basic network devices and critical systems and applications. Microsoft System Management Server (SMS) is a solution for centralized management of Windows-based environment. SMS offers features that can help administrators streamline their work and increase user productivity.

Table of ASMA function for ASMM card and ASUS mainboard

Model / Function	P2B-LS Rev. 1.03 P2B-S Rev 1.03	P2B-D2 Rev 1.02	P2B-DS Rev. 1.03	CUV4X	CUR-DLS	CUR-DLSR
Chassis Fan 1	X	X	X	X	X	X
Chassis Fan 2					X	X
CPU 1 Fan Speed	X	X	X	X	X	X
CPU 2 / Power Fan Speed	X (Power Fan)	X (CPU 2 Fan)	X (CPU 2 Fan)	X (Power Fan)	X	X
Chassis Fan Control				X	X	X
CPU1 Fan Control				X	X	X
CPU2/Power Fan Control				X (Power)	X	X
CPU 1 Vcore	X	X	X	X	X	X
CPU 2 Vcore		X	X		X	X
+3.3V	X	X	X	X	X	X
+5V	X	X	X	X	X	X
+12V	X	X	X	X	X	X
+1.5V				X	X	X
+2.5V				X	X	X
+3VSB				X	X	X
+5VSB				X	X	X
CMOS Battery				X	X	X
NVRAM Battery				X	X	X

System Temperature	X	X	X	X	X	X
CPU 1 Temperature	X	X	X	X	X	X
CPU 2 / Regulator Temperature	X (Regulator Temp.)	X (CPU 2 Temp.)	X (CPU 2 Temp.)		X (CPU 2 Temp.)	X (CPU 2 Temp.)
ASR	X	X	X	X	X	X
Chassis Intrusion	X	X	X	X	X	X
Remote Reboot Management	X	X	X	X	X	X
Event Action	X	X	X	X	X	X
SCSI Backplane			X		X	X

Table of ASMA function for ASMM card and ASUS mainboard (continue)

Model / Function	CUV-LSV
Chassis Fan 1	X
Chassis Fan 2	
CPU 1 Fan Speed	X
CPU 2 / Power Fan Speed	
Chassis Fan Control	X
CPU1 Fan Control	X
CPU2/Power Fan Control	
CPU 1 Vcore	X
CPU 2 Vcore	
+3.3V	X
+5V	X
+12V	X
+1.5V	X
+2.5V	X
+3VSB	X
+5VSB	X
CMOS Battery	X
NVRAM Battery	X
System Temperature	X

CPU 1 Temperature	X
CPU 2 / Regulator Temperature	)
ASR	X
Chassis Intrusion	X
Remote Reboot Management	X
Event Action	X
SCSI Backplane	

(Notes: **X** is mean its VALUE is VALID in this mainboard)

ASMA can monitor the BackPlane's DriveBay status, the power system of DriveBay is good or bad, the cooling fan status of the BackPlane and the temperature of the BackPlane. When these BackPlane objects are not at normal status, the ASMA will send snmp trap to SNMP NMS. It can also automatic adjust cooling fan speed depend on the temperature of the BackPlane.

ASMA function on different BackPlane board

Function	DA-BP5 (Rev 1.03)	DA-BP5E	DA-BP4E	DA-BP3E
Temperature	X	X	X	X
Cooling Fan1 status	X	X	X	X
Cooling Fan2 status	X	X	X	X
Cooling Fan1 Speed (RPM)		X	X	X
Cooling Fan2 Speed (RPM)		X	X	X
+5V (mV)		X	X	X
+12V (mV)		X	X	X
LED/Fan Module status	X	X		
Drive(1~5) Plugin status	X	X	X	X
Drive(1~5) Power status	X	X	X	X
Cooling Fan Speed control	X			
Automatic Cooling Fan Speed Adjust	X			
Cooling Fan Enable/Disable	X	X	X	X

Backplane Configuration Remap	X	X	X	X
Drive Power off	X	X	X	X

(Notice: the "X" means the function is supported in the BackPlane.)

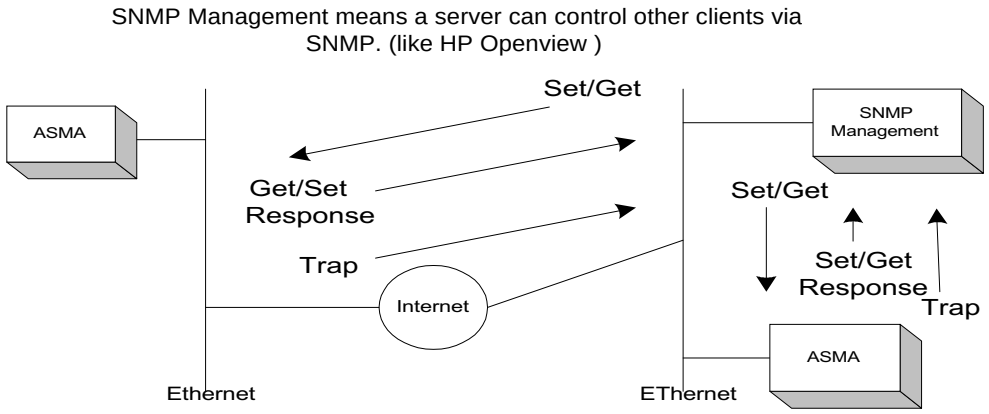
ASMA can light the LED of BackPlane when RaidCard is rebuilding the Raid Drive. ASMA 2.0 can let user to know hard drive status (rebuild, spare, and Failure) by using light the LEDs of BackPlane. User need to install RAID driver and GUI RAID Manager for Windows NT for this feature.

ASMA can monitor the CPU1/CPU2/System temperature over the fatal high threshold value, then the event action will occur. The event action have reboot the system, power off the system and shutdown the system.

1.4 SNMP Overview

Simple Network Management Protocol (SNMP) is the most popular network management protocol in the TCP/IP protocol suite. SNMP lets TCP/IP-based network management clients exchange information about the configuration and status of nodes on a TCP/IP-based Internet. The information available is defined by a set of managed objects referred to as the SNMP.

The example of SNMP in a network environment is illustrated as follows.



As mentioned above, we will introduce several terminology of SNMP.

Management Information Base (MIB). The subset of managed objects comprising the TCP/IP portion of the MIB is maintained by each TCP/IP node. SNMP also generates trap messages used to report significant TCP/IP events asynchronously to interested clients.

SNMP Get – let SNMP NMS get the value of attribute of managed system, such as fan speed, working voltage and system temperature.

SNMP GetNext – allows the NMS to retrieve the next object instances from a table with an agent.

SNMP Set – set the value of attribute of managed system, such as fan speed threshold, working voltage threshold and system temperature threshold from SNMP NMS.

SNMP Response – be responsible for the response of SNMP GET, SNMP GETNext and SNMP Set.

SNMP Trap – managed computer system can inform the NMS of some event (when the interested attributes, such as fan/voltage/temperature, over or lower the thresholds) asynchronously.

1. 5 Terminology

The following table lists common terms for ASMM and LDSM

Term	Definition
ASMM	ASUS System Monitoring Module
LDSM	LANDesk Server Manager
LM78	H/W Monitor, which is for system temperature, fan status, CPU voltage and alert.
AMS2	A new version of Alert Management System
DMI	Desktop Management Interface, an industry standard management specification
MIB	Management Information Format, used by SNMP for describing component instrumentation
SNMP	Simple Network Management Protocol, a stand network protocol for management information
ASR	Automatic Server Restart, is a function that can reboot the computer system automatically when the computer system is hang
NMS	Network Management Station, such as LANDesk Server Manager, HP Openview , SUN Net Manager, Tivoli Netview and CA-Unicenter TNG.

Chapter 2 ASMA Installation and Configuration

2.1 Installation tip:

ASUS System Monitoring Agent defines ASUS Private Enterprise MIB that is about the computer system fan speed, working voltage and system temperature information. It has the thresholds MIBs for fan, voltage and temperature MIBs also. ASUS System Monitoring Agent can send SNMP Trap to NMS to inform user that computer system have an abnormal condition occur when ASUS System Monitoring Agent detect the computer system temperature/fan/ voltage over the temperature/fan/voltage threshold.

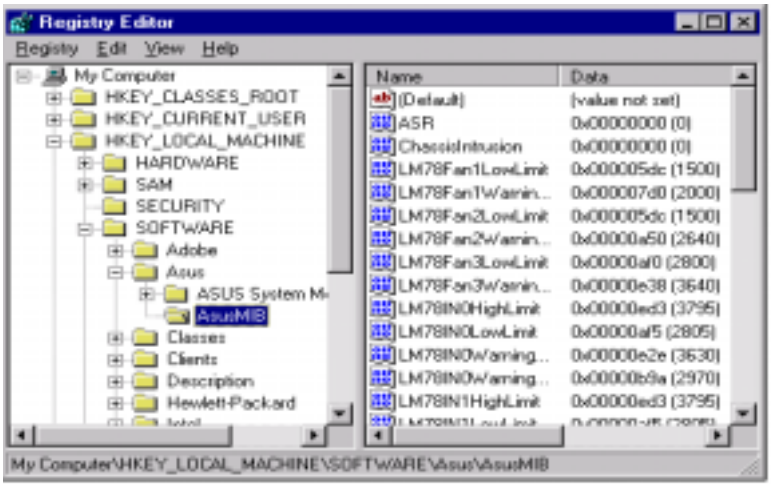
You must start the services to be monitored before configuring and starting the SNMP service on ASMA software. Once the SNMP service has been started on both remote and local side, you can use SNMP tools to monitor the running services.

NT SNMP Service Installing:

1. From the Windows NT **Control Panel**, double-click Network icon.
2. Click the **Services** tab.
3. Click the **Add** button.
4. Double-click **SNMP** Service.
5. Specify a location for the Windows NT install files and click the Continue button.

User may get this MIB file from ASUS subdirectory under Program File directory in local drive. User can use MIB Compiler to compile this file, then user adds the compiled ASUS MIB file module to NMS to manage and operate the ASUS private Enterprise MIB with the computer system has installed ASUS System Monitoring Agent .

You may verify this MIB file in REGEDIT program as following screen:



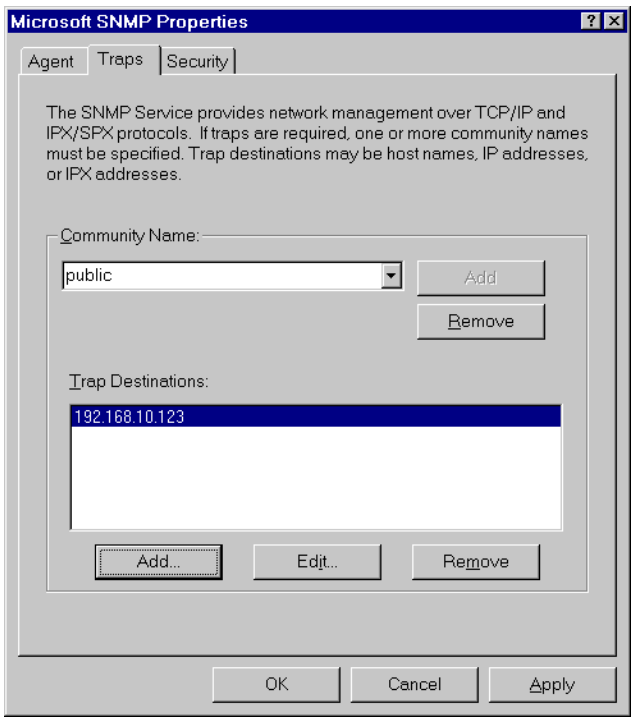
REGEDIT Program in NT server

2.2 Configuration

If you monitor your PC or network by using Simple Network Management Protocol (SNMP), you can use the SNMP Management Information Bases (MIBs) provided by ASMA software program. You will need to compile the MIB files using the MIB compiler that comes with your SNMP software.

Configuring SNMP Service on NT Server

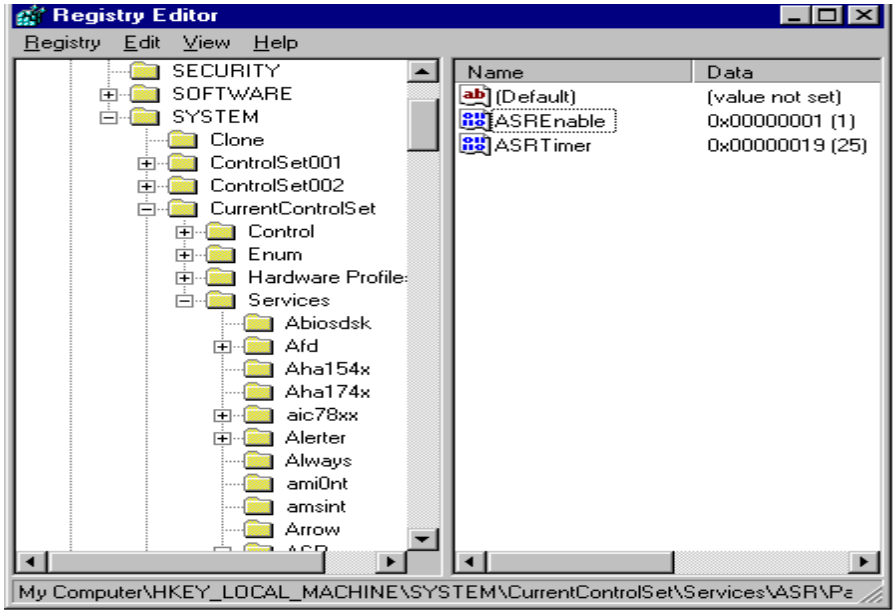
1.At the Microsoft SNMP Properties dialog, click the **Traps** tab.
2.In the **Community Name** box, type a name for the SNMP community, such as public.
3.Click the **Add** button.
4.Below the **Trap Destinations** box, click the Add button.
5.Type the **IP address** or **computer name** of your network's SNMP management station.
6.Click the **Add** button.
7.Click the **OK** button.
8.Click the **Close** button.
9.When prompted , click the **Yes** button to restart your computer.



To turn ON/OFF the Automatic Server Restart:

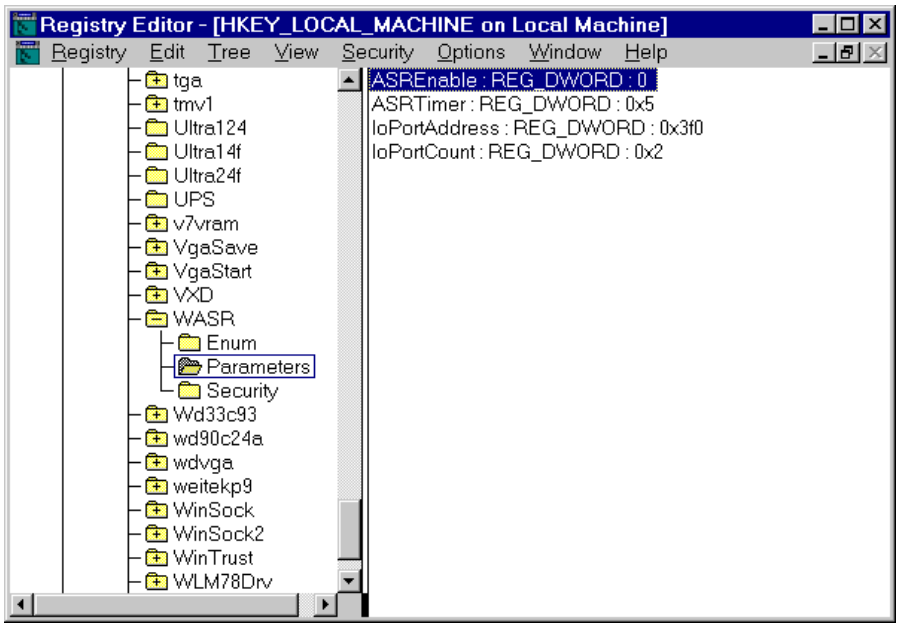
Hkey_Local_Machine\System\CurrentControlSet\Services\ASR\Parameter\ASREnable

(for P65UP8 + ASMM card)



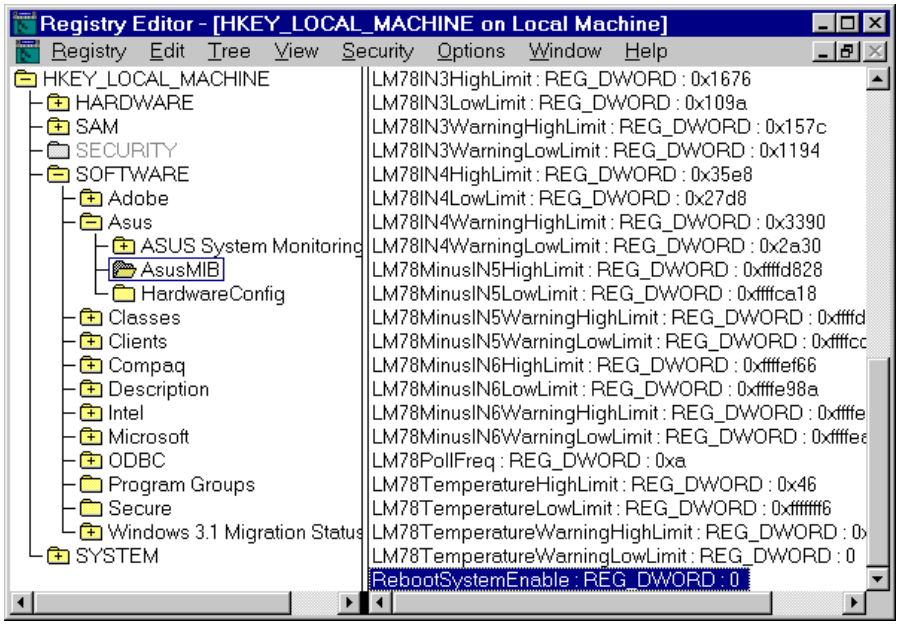
Hkey_Local_Machine\System\CurrentControlSet\Services\WASR\Parameter\ASREnable

(for P2B series)



To turn ON/OFF the Reboot System function:

Hkey_Local_Machine\Software\ASUS\ASUSMIB\RebootSystemEnable

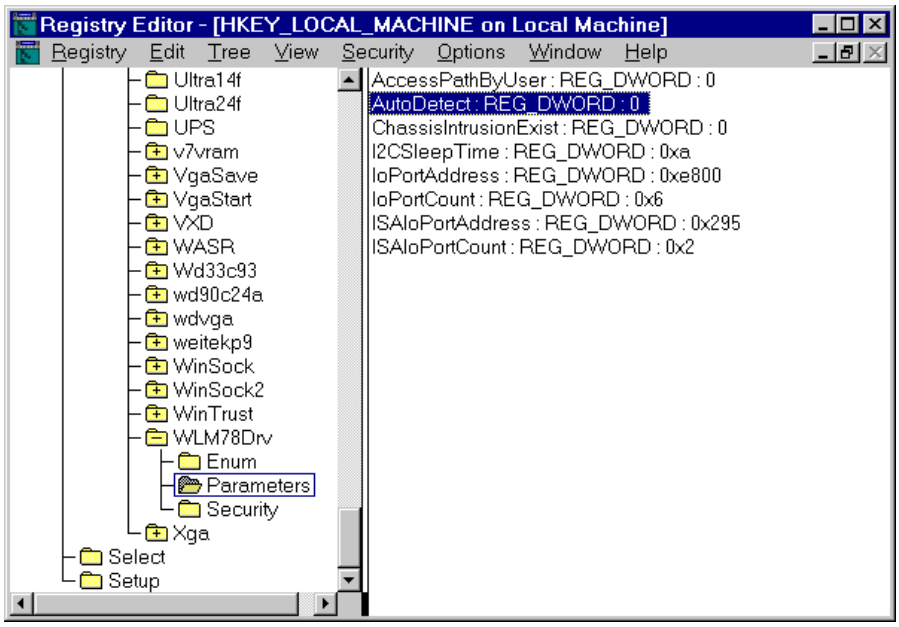


To enable the Auto hardware detect function:

Hkey_Local_Machine\System\CurrentControlSet\Services\WLM78Drv\Parameter\AutoDect (for P2B series).

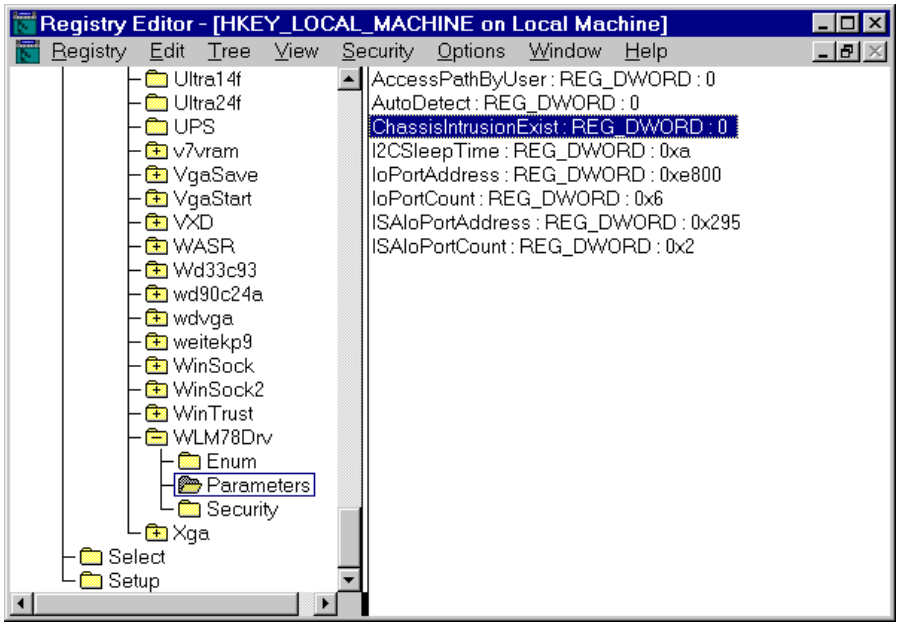
Hkey_Local_Machine\System\CurrentControlSet\Services\LM78Drv\Parameter\AutoDect (for P65UP8 & P2L97-DS).

Notes: If you want to add addition hardware (like FAN) to system, you can modify the value of AutoDetect from 0 to 1 without re-install the ASMA. After you modify the value of AutoDetect, please reboot your system..


Registry Editor - [HKEY_LOCAL_MACHINE on Local Machine]
Registry Edit Tree View Security Options Window Help
Ultra14f
Ultra24f
UPS
v7vram
VgaSave
VgaStart
VXD
WASR
Wd33c93
wd90c24a
wdvga
weitekp9
WinSock
WinSock2
WinTrust
WLM78Drv
Enum
Parameters
Security
Xga
Select
Setup
AccessPathByUser : REG_DWORD : 0
AutoDetect : REG_DWORD : 0
ChassisIntrusionExist : REG_DWORD : 0
I2CSleepTime : REG_DWORD : 0xa
IoPortAddress : REG_DWORD : 0xe800
IoPortCount : REG_DWORD : 0x6
ISAIoPortAddress : REG_DWORD : 0x295
ISAIoPortCount : REG_DWORD : 0x2

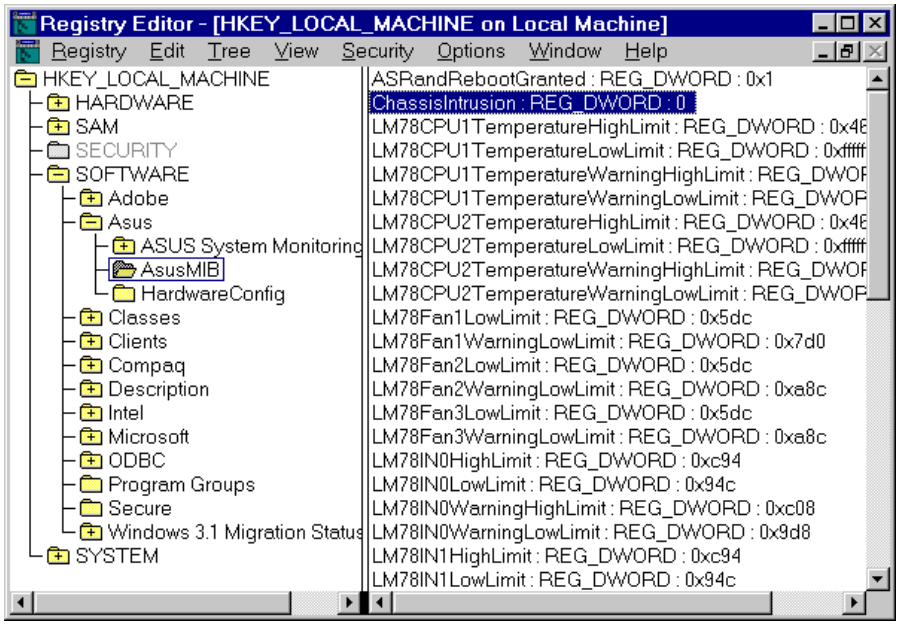
To enable the Chassis Intrusion Exist function:

Hkey_Local_Machine\System\CurrentControlSet\Services\WLM78Drv\Parameter\ChassisIntrusionExist



To turn ON/OFF the Chassis Intrusion function:

Hykey_Local_Machine\Software\ASUS\ASUSMIB\ChassisIntrusion



2.3 Troubleshooting

1. How to disable the on-board LM78, if you want to install a ASMM.

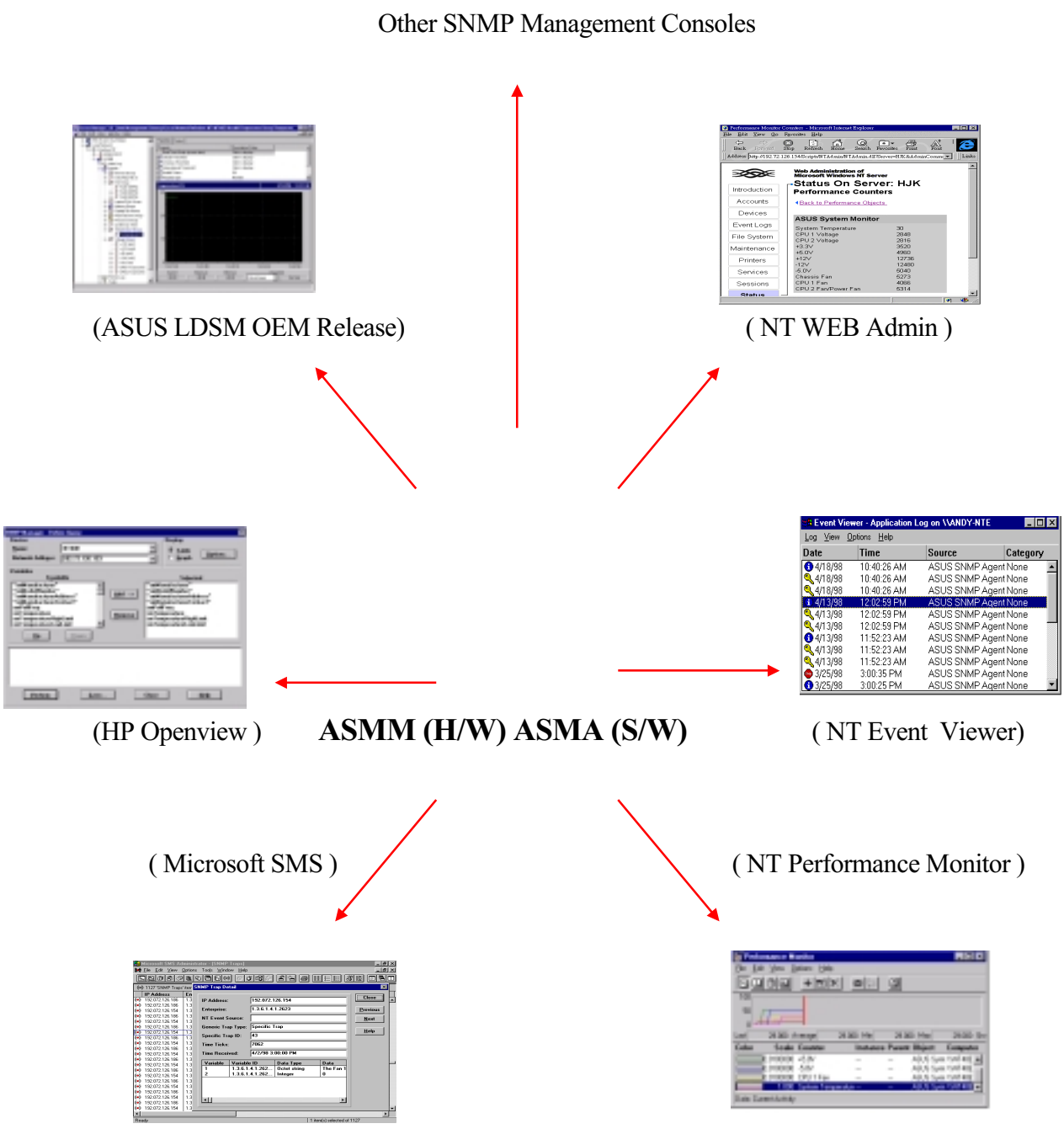
Current BIOS can not auto-detect the on-board LM78 and LM78 on ASMM card such that a hardware conflict occurs and results in a system warning. Future BIOS will auto-detect these two and automatically disable the on-board one. To disable the on-board LM78 currently, the following operation steps are provided:

1) Format a bootable floppy disk (DISKA)
2) Copy the PCI control program PCICFG.EXE on to DISKA
3) Copy the DOS utility DEBUG.COM onto DISKA
   note: the version of debug.com must be the same as the DOS version on DISKA or it can not be executed.
4) Adjust the BIOS booting sequence to A:, C: (boot from floppy first)
5) Insert the DISKA and boot the system
   note: Ignore the hardware monitor error as a result of LM78s confliction.
6) Under prompt sign A>, type ***PCICFG***<enter>
7) Under prompt sign BUS00>, type ***WD 1 3 60 00670290***
   note: The on-board LM78 is now disabled
8) Under prompt sign BUS00>, type ***Q***<enter> to exit from the PCI control program.
9) Under prompt sign A>, type ***DEBUG***<enter>
10) Under prompt sign >, type ***A***<enter>
11) Under prompt sign xxxx:0100, type ***int 19***<enter>
12) Under prompt sign xxxx:01yy, type <enter>
13) Remove the DISKA from floppy drive and leave it open
14) Under prompt sign >, type ***G***<enter>
15) Now, you can see the O.S. from hard disk boots-up and LDSM can work with the LM78 on ASMM.

If your motherboard does not equip with LM78, everything goes fine with LDSM.

2. What kind of environment can be used to monitor the ASMM/ASMA information ?

ASUS LDSM OEM Release, HP Openview, NT performance Monitor, Microsoft SMS Microsoft Web Administration , NT Event Viewer and other SNMP Management Console.



Chapter 3 NT Performance Monitor

NT Performance Monitor - is a graphical tool for measuring the performance of your own computer or other computers on a network. On each computer, you can view the behavior of objects, such as processors, memory, cache, threads, and processes.

The following overview lists how you use Performance Monitor to view the performance of objects: Simultaneously view data from any number of computers. View and dynamically change charts reflecting current activity and showing counter values that are updated at a user-defined frequency. Export data from charts, logs, alert logs, and reports to spreadsheet or database programs for further manipulation and printing. Add system alerts that list events in the Alert Log and notify you either by reverting to Alert view, logging the event in Event Viewer's Application log, or issuing a network alert. Run a predefined program either every time or only the first time a counter value goes over or under a user-defined value. Create log files containing data about objects on different computers. Append selected sections of existing log files to a single file, forming a long-term archive.

Performance Monitor consists of four main windows, which you display by clicking Chart, Alert, Log, or Report on the View menu. These windows contain different information and have only the menu bar, status bar, and toolbar in common. You can press the F1 key to see Help about any Performance Monitor command. On the Options menu, Data From is available in any of the four windows. Use this command to switch from working with current values for current activity (real time data) to viewing and manipulating existing log files. The default is current activity.

There are two ways that user can monitor system temperature, working voltages and fan speed from NT Performance Monitor.

Method I:

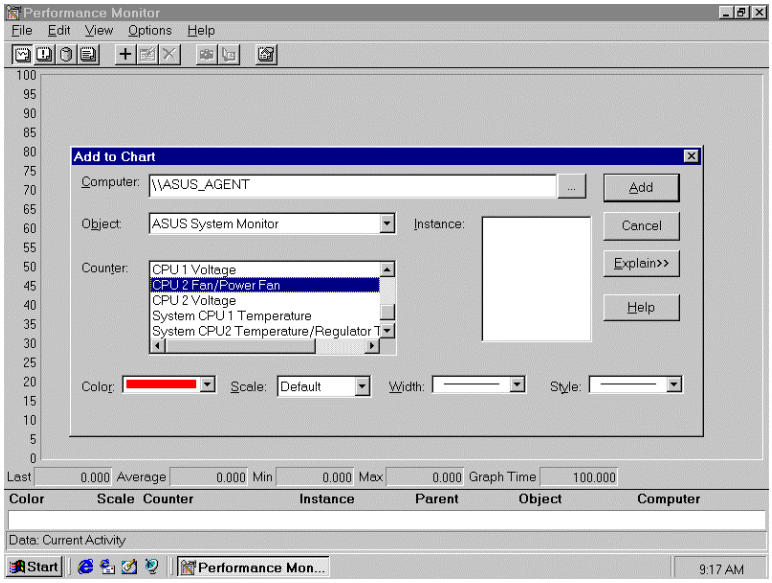
1. From the Windows NT desktop, choose **Start** select **Programs**, Select **ASUS System MonitorAgent**, Select **Monitor**.
2. From the **Monitor**, you can monitor the status of system's temperature, voltage and fan speed.

Method II:

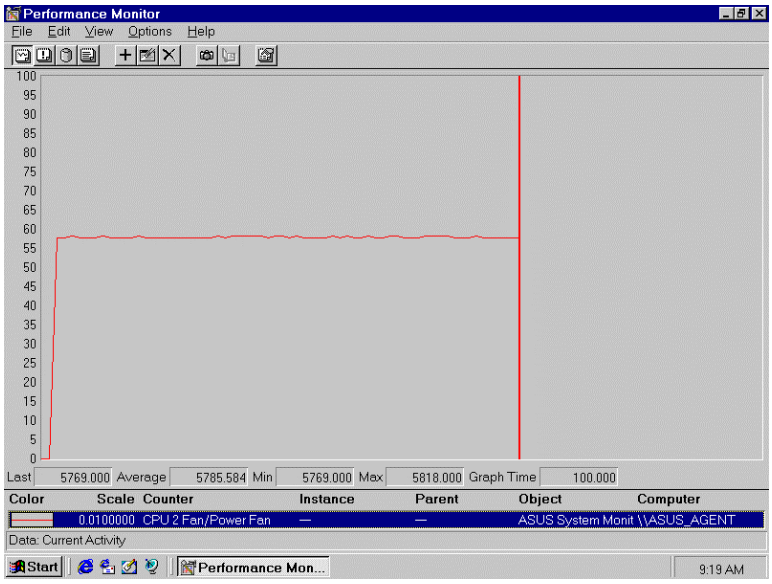
1. From the Windows NT desktop, choose **Start | Programs | Administrative Tools | Performance Monitor.**
2. Choose **Edit** menu, Select **Add to Chart**

3. Select the computer that you want to monitor, click **OK**.
4. From the **Object Box**, select **ASUS System Monitor**. It will displays ASUS System Monitor performance list in the **Counter Box**.

5. To see a description of a counter, click the **Counter** in the Computer list box, and click the **Explain** button. This displays a **Counter Definition** panel that describes the counter.
6. In the **Counter** list box, click a performance counter you want to monitor, and click the **Add** button. Repeat this step for all counters you want to monitor.



7. When you are finished adding counters to the chart, close the **Add to Chart** dialog box., You can now observe the color-codes graphs of the counters you have

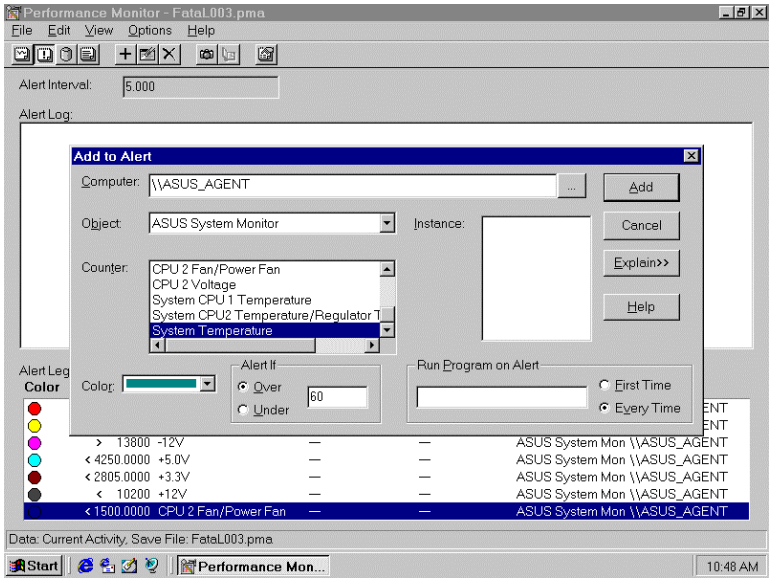


choosen as they Illustrate current.

Note: Using Method II, you can monitor another computer that installed ASUS system monitor agent remotely from the network.

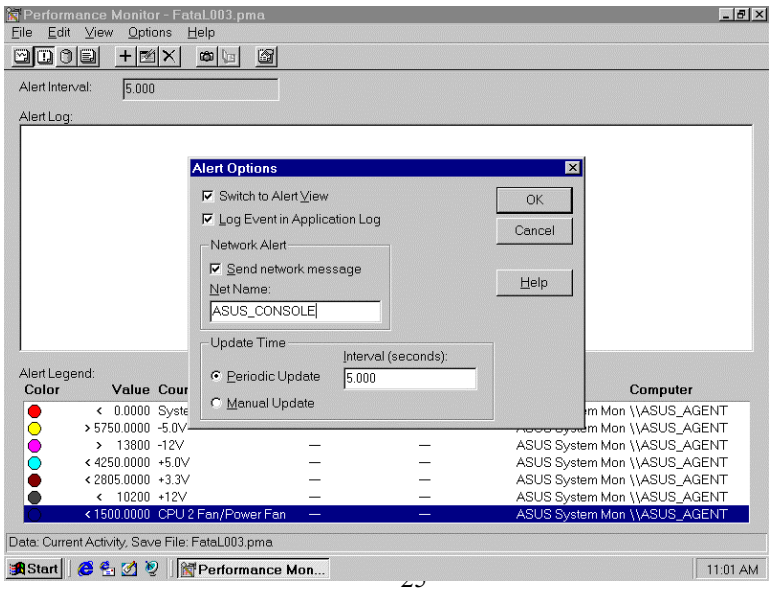
To configure the threshold of Fan/Voltage/Temperature in NT performance monitor extension

1. From **Start**, Select **Programs**, Select **ASUS System Monitoring Agent**, Select **Alert**, choose the threshold you want to monitor.
2. Choose **Edit** menu, Click Add to **Alert**
3. Select **Computer**, **object**, **counter**, Set Alert threshold value, click **Add**, click

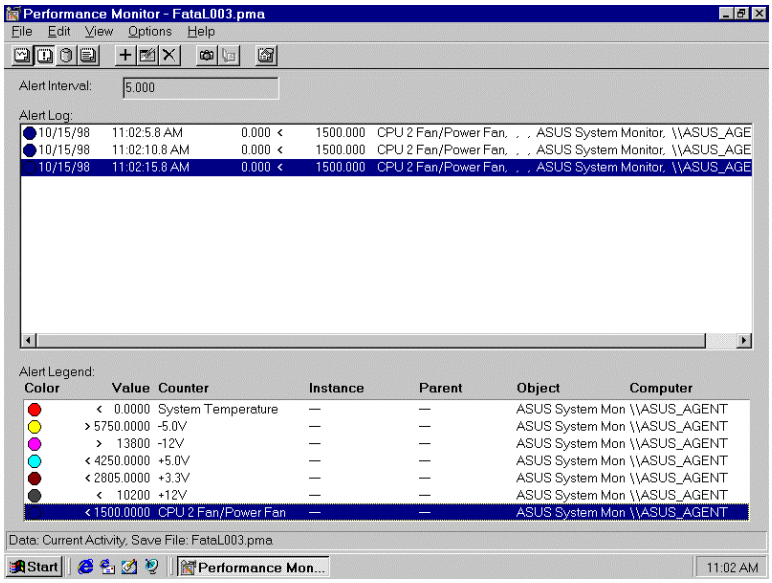


done.

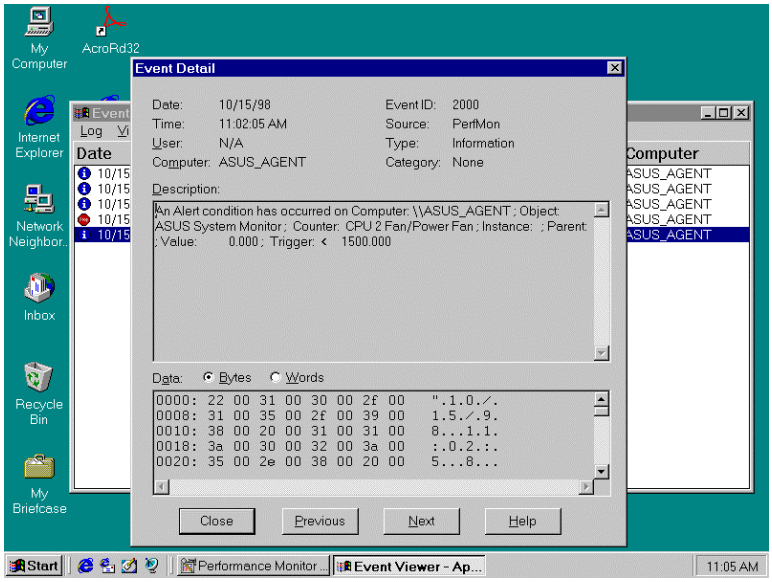
4. Choose **Options** menu, click **Alert**.
5. Select **Send network message**, Type the computer name where the alert message you want to sent.



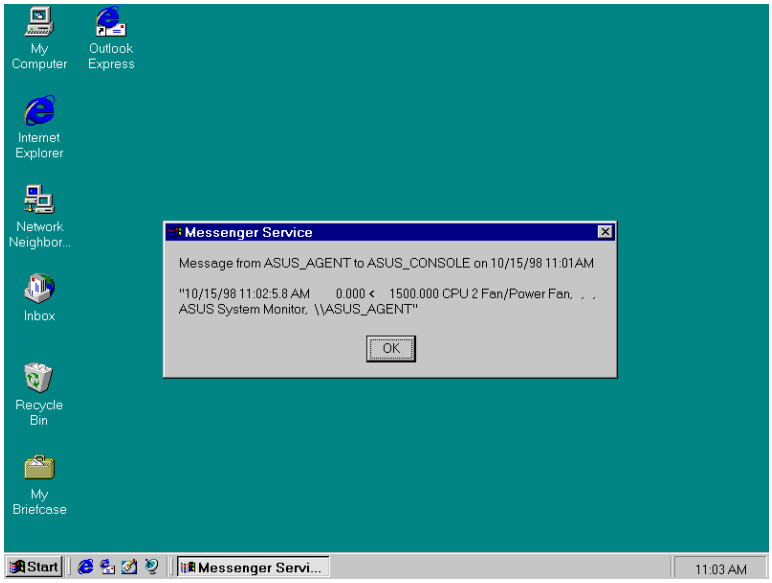
6. You can stop the CPU fan to generate a alert.



7. Using Event viewer to view this alert message.


My Computer
AcroRd32
Internet Explorer
Network Neighbor..
Inbox
Recycle Bin
My Briefcase
Event Detail
Date: 10/15/98
Time: 11:02:05 AM
User: N/A
Computer: ASUS_AGENT
Event ID: 2000
Source: PerfMon
Type: Information
Category: None
Description:
An Alert condition has occurred on Computer: \\ASUS_AGENT ; Object: ASUS System Monitor ; Counter: CPU 2 Fan/Power Fan ; Instance: ; Parent: ; Value: 0.000 ; Trigger: < 1500.000
Data: Bytes Words
0000: 22 00 31 00 30 00 2f 00 ".1.0./.
0008: 31 00 35 00 2f 00 39 00 1.5./.9.
0010: 38 00 20 00 31 00 31 00 8...1.1.
0018: 3a 00 30 00 32 00 3a 00 :.0.2.:.
0020: 35 00 2e 00 38 00 20 00 5...8...
Close
Previous
Next
Help
Date
Computer
ASUS_AGENT
Start
Performance Monitor
Event Viewer - Ap...
11:05 AM

8. This alert message will send to CONSOLE.



Chapter 4 NT Event Viewer

Event Viewer - is the tool you can use to monitor events in your system. You can use Event Viewer to view and manage System, Security, and Application event logs.

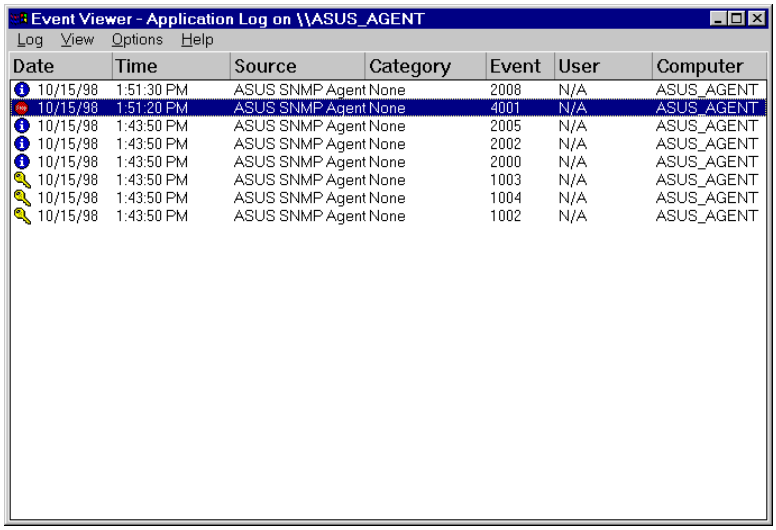
Event: In the Windows NT operating system, an event is any significant occurrence in the system or in an application that requires users to be notified. For critical events such as a full server or an interrupted power supply, you may see a message on screen. For many other events that do not require immediate attention, the Windows NT operating system adds information to an event-log file to provide information without disturbing your usual work. This event logging service starts automatically each time you start you computer running Windows NT.

System Log: The System log records events logged by the Windows NT system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log.

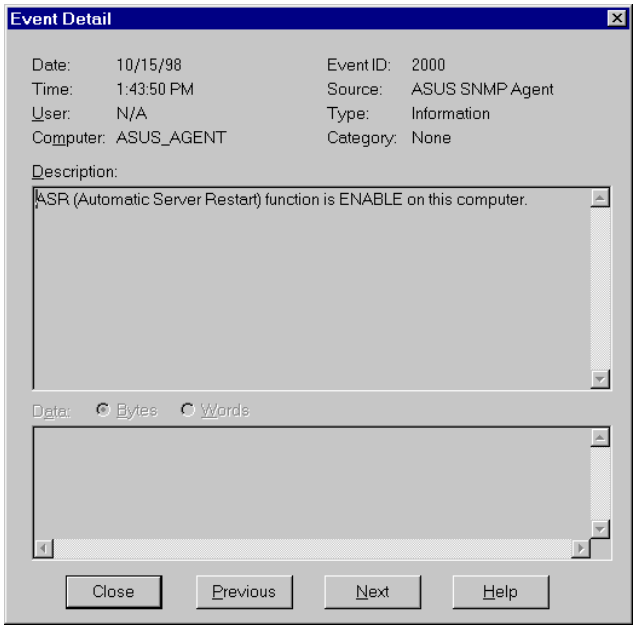
Security Log: The Security log records security events. This helps track changes to the security system and identify any possible breaches to security. For example, attempts to log on the system may be recorded in the Security log, depending on the Audit settings in User Manager. You can view the Security log only if you are an Administrator for a computer.

Application Log: The Application log records events logged by applications. For example, a database application might record a file error in the Application log. ASUS ASMA will generate some special events in this log.

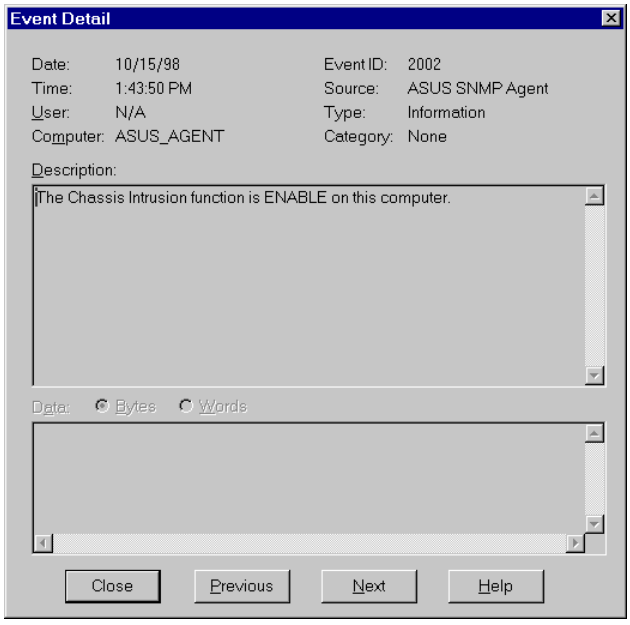
ASMA events information in Event Viewer:


Event Viewer - Application Log on \\ASUS_AGENT
Log View Options Help
Date Time Source Category Event User Computer
10/15/98 1:51:30 PM ASUS SNMP Agent None 2008 N/A ASUS_AGENT
10/15/98 1:51:20 PM ASUS SNMP Agent None 4001 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 2005 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 2002 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 2000 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 1003 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 1004 N/A ASUS_AGENT
10/15/98 1:43:50 PM ASUS SNMP Agent None 1002 N/A ASUS_AGENT

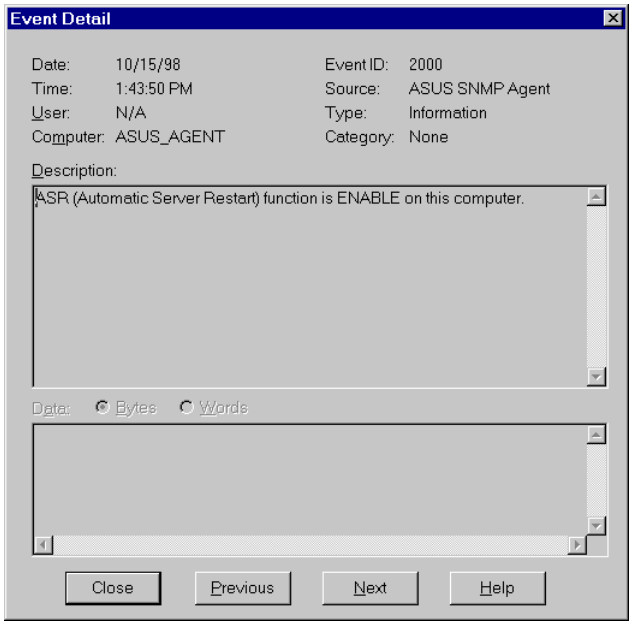
To show a Automatic Server Restart Function Enable/Disable event in Event Viewer:



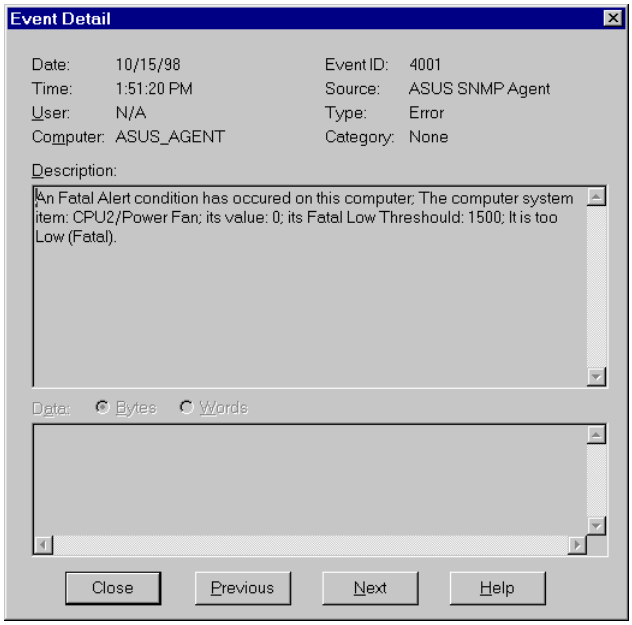
To show a Chassis Intrusion Function Enable/Disable event in Event Viewer



To show a Reboot Management function Enable/Disable event in Event Viewer:



ASMA will generate the SNMP Trap and a event of NT event log , if an alert occurs.



Chapter 5 NT Web Admin

Web Administration for Microsoft Windows NT Server enables you to remotely administer Microsoft Windows NT Server using existing HTML browsers. Web Administration is not designed to replace existing administrative tools for Windows NT servers; instead, it is to enable you to perform limited administrative tasks when you are roaming, away from your usual workstation. Web administration is a tool that is implemented to work in conjunction with Microsoft Internet Information Server 2.0. User can monitor system temperature, working voltages and fan speed from Web Performance Monitor. You can install the Web Administration software on any server that run Windows NT server 4.0 and Microsoft Internet Information Server (IIS). Installing the Web Administration software on the server causes the server to publish web pages that include forms you can use to administer that particular server. The Web Administration tool is intended for existing Windows NT server administrators who have performed tasks with the regular administrative tools on Windows NT 3.51 and NT 4.0.

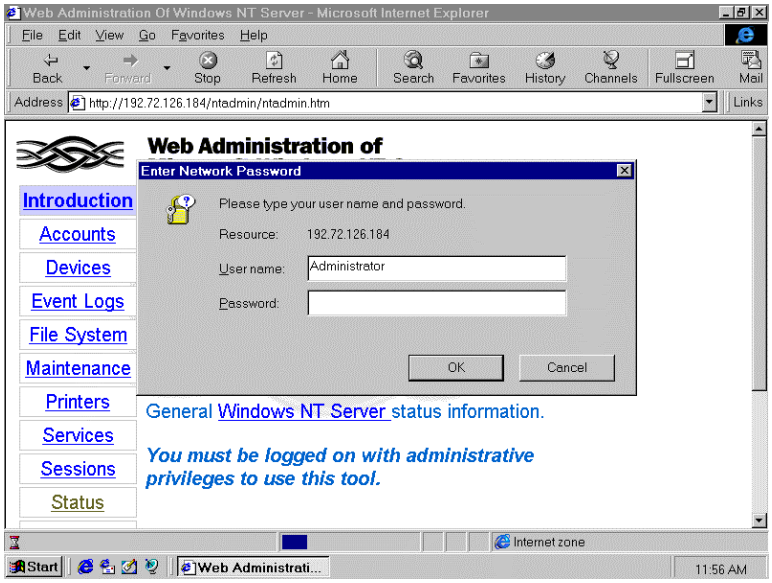
You may download the Web Administration program from Microsoft Web site at following URL: http:// www.microsoft.com/ntserver/webadmin/dlnowdl.htm?

To manage the ASMM in Web Administration program:

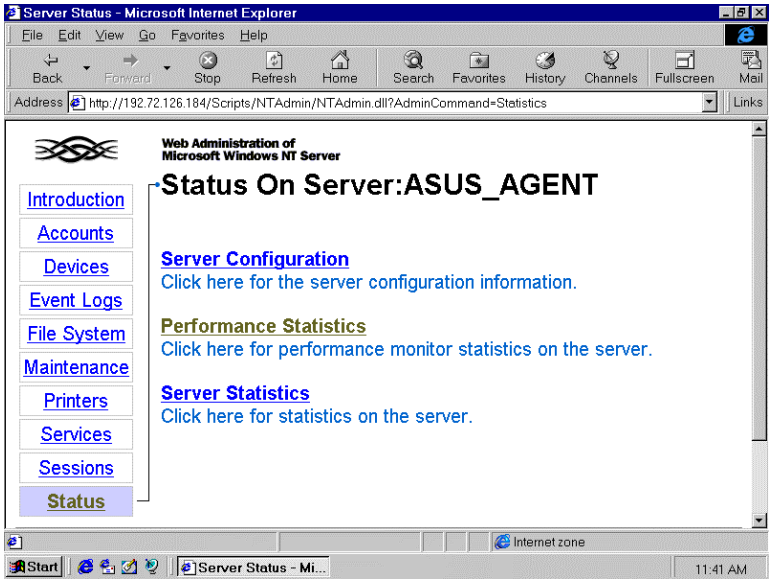
.

1. Run Web Browser (IE or Netscape).

2. Type the address at your Browser such as
   http://server_name or IP address/ntadmin/ntadmin.htm.

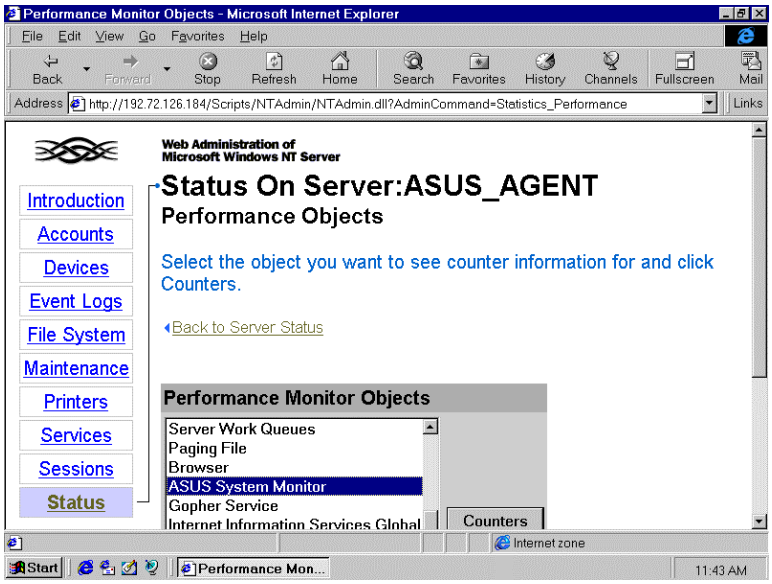


3. Click the **Status**. Type your user name, password.

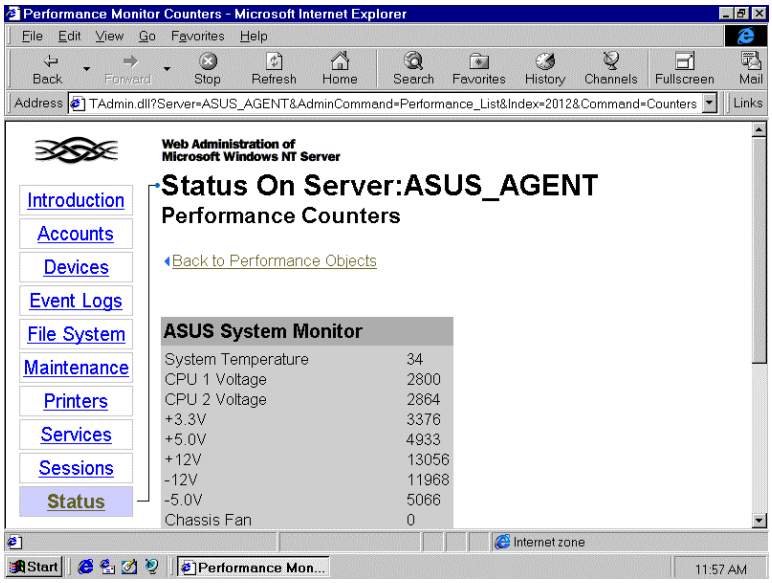


4. Click **Performance Statistics**.

5. Select **ASUS System Monitor** and Click **Counter** button



6. When prompted, you can observe the status of system's temperature,



voltages fan speed, and so on.

Chapter 6 ASUS LDSM OEM Release

LANDesk Server Manager provide administrators with a proactive management solution and emergency-management recovery tools to help maximize business-critical server uptime. From a centralized console, LANDesk Server Manager product monitor critical parameters on either Microsoft Windows NT or Novell Netware Server. Through enhanced alerting features and server health monitoring, LANDesk Server Manager notify the LAN administrator when a server reaches a predefined threshold. (ASUS provides an ASUS OEM version of LDSM in the package. In this LDSM, it added a ASMA patch for LDSM; therefore, you can monitor ASMA information from LDSM console).

The following figure highlights the high level architecture of LDSM with new or changed components shaded.

Management Console Features:

LDSM has been re-architected with a new console GUI that follows Microsoft COM and MMC models. The Management Directory (MD) is the part of Management Console that handles the under-the covers functionality of the console. Management Directory discovers and exposes managed objects with their associated management functionality in a standard and unified manner. One of the key features of the console is the server health view, which offers a color-coded view of pre-defined parameter thresholds and limits. Using Active X technology , it will be easier to create, maintain and enhance.

Managed Server Features:

Data Collection Agent (DCA), allows data from independent data sources registered with the Message System to be grouped together. Data collection agent supports the LDSM enriched abstractions goal, by collecting data from multiple agents, grouping it in a meaningful way and reducing communications overhead. Rather than multiple agents or proxies collecting data and communicating to the console through the message system, now there is just one agent (the DCA) performing this task.

LANDesk Server Manager server side architecture is composed of several agents and specialized pieces that gather, and share information with other agents and management console. It is through these agents and services that the Network Operating System (NOS)

and the Server Monitoring Module are monitored, information communicated to the console.

There are two alertable parameter types in LDSM:

Graphable parameters that have three independently configurable thresholds: informational, non-critical and critical.

Event-only parameters that track single operating system event, such as loading and NLM. The administrator can configure alerts for both Netware and Windows NT servers. The following is a look at where the AMS2 alert occur on the network:

1. Message Box
2. Broadcast Message
3. Windows NT Event Logging
4. Send Internet Mail
5. Program Execution
6. Paging
7. SNMP Trap

SNMP Trap Generation

AMS2 supports the configuration of actions based on a given event or alert. One of the action is to generate an SNMP trap. The system may be configured to send the trap to a SNMP management console. SNMP requires that the address (either IP or IPX) for the system receiving the trap be configured in advance. The method for specifying the trap destination address depends on the operation system of the device generating the trap.

Common Base Agent (CBA) is made up of several modules that provide basic common denominator services that are protocol and OS independent.

Message System

The messaging system is the glue that holds the Agent together. Because the native capabilities will differ from NOS to NOS, the Agent messaging API could require features that are not present on some OS. The CBA messaging system is a service library callable by all Agent modules. The way it is packaged will be on each NOS; a DLL on NT, a NLM on Netware. The messaging system has a given set of API function calls making it capable of handing all of the messaging needs for LDSM. Message System is the CBA highest-level module and provides local and remote process-to-process messaging.

Ping Discovery System (PDS)

PDS is a process by which a console node discovers other nodes that are capable of being managed. This service is used by the LDSM console to discover the servers with LDSM installed. This service has two parts:

Full discovery - a ping is sent over the network to which LDSM servers to reply. If a CBA is present on the server, a ping is sent back to the requesting console with its reply information. This information is stored on the console used to populate the discovered server tree for that console.

Refresh discovery - is similar to full discovery option, but rather than sending a packet on the wire to all servers, it uses the information stored at the console as a request list, and send s a ping only to those servers. The discovered server tree list is rebuilt based on the reply from those servers at that moment. If the server fails to reply, its discovered icon is grayed in the tree, indicating it is no longer available.

Network Transport Service (NTS)

Network Transport Service is a set of APIs which shield LDSM from the complexities of networking protocol detail of sending and receiving data. NTS is designed so that it will not have to change for different operating systems. For example, the SMM agent will use the same NTS API whether it is running on Netware or Windows NT. The NTS code is optimized to take advantage of the services available on a particular operating system, and are transparent to the LDSM agents. NTS offers routines, which allow for guaranteed delivery of sequenced packets. The protocol is designed to allow packets to be sent in size of up to 65,535 bytes. NTS will fragment the packet on the network wire and receive the packet into a buffer of at least the same size. NTS consists of three main pieces. A transport layer that communicates to the network. A message system that process information between each of the multiple agents on a server. A proxy which services as a bridge connecting this message system and transport layer.

Before you install the LDSM, please make sure you already installed the ASMM into the server. The ASMM is fully compatible with LDSM, HP Openview, NT Performance Monitor, NT Web Admin, Microsoft SMS and so on.

Installing ASUS LDSM OEM

Step1: installing and configuring SNMP.

1. At the Microsoft SNMP Properties dialog, click the **Traps** tab.
2. In the **Community Name** box, type a name for the SNMP community, such as public.
3. Click the **Add** button.
4. Below the **Trap Destinations** box, click the Add button.
5. Type the **IP address** or **computer name** of your network's SNMP management station.
6. Click the **Add** button.
7. Click the **OK** button.
8. Click the **Close** button.
9. When prompted , click the **Yes** button to restart your computer.

Step2: installing Windows NT Service Pack3 (or above).

Step3: installing LDSM.

1. Insert the ASUS install CD.
2. Click Install LDSM.
3. Select **Install** to install LDSM and Click **Next**.
4. Select Yes to agree the license and Click **Next**.
5. Type the Registration Key and Click **Next**.
6. Click Plan to view installation help, Click **Next**.
7. Select LDSM components that you wish to install, Click **Next**.
8. Select Server to install LDSM Agent. Click **Next**.
9. Specify a Windows NT group or user that can remote control the server , Click **Next**.
10. Re-check your setting and Click **Install**.
11. Wait for Transferring files and Click **Next**.
12. Wait for Transferring AMS Services and Click **Next**.
13. Select Reboot now and Finish to restart your computer.

Note1: If you install LDSM Agent to Windows NT, You must install ASMA first.

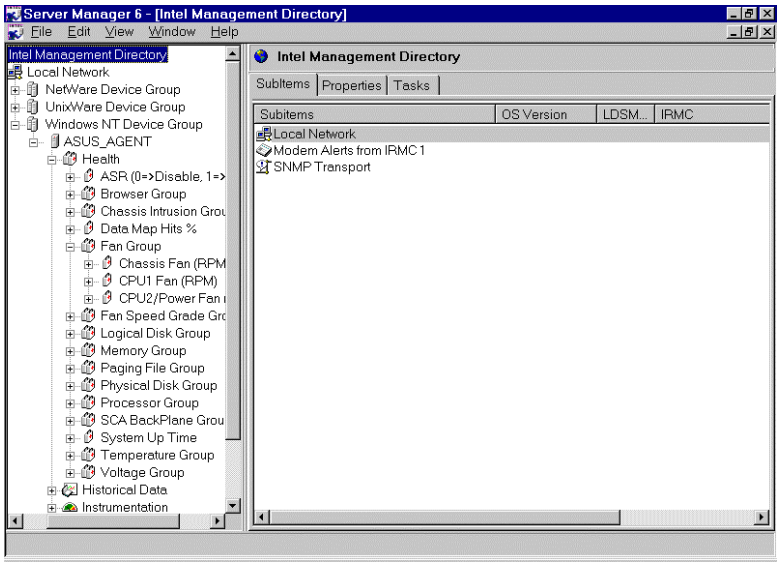
To configure LDSM Agent for Netware 4.x/5.x.

1. Edit \SYS\System\AUTOEXEC.NCF.at Netware Agent.

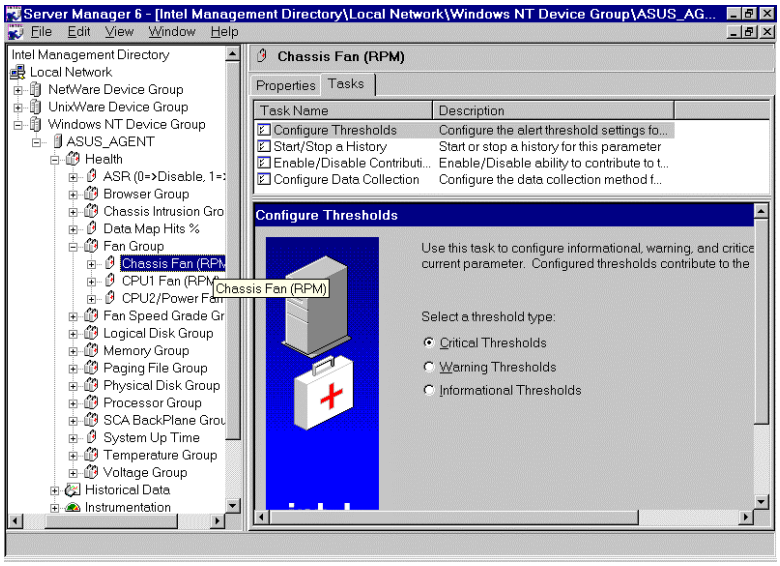
2. LDSM default to mask sm_auto.ncf, unmask it.
3. In the last line, add asusldsm.ncf
4. Edit \SYS\System\ASUSMIB.INI to configure ASMM function at Netware Agent.
   Default value is as follow.
   ASREnable=0 ---------- Disable ASR. Set 0 to disable. Set 1 to enable.
   ASRTimer=5 ---------- ASR Polling Time (unit: Min)
   ChassisIntrusionExist=0 ----- ChassisIntrusionExist. Set 0 to disable,
   Set 1 to enable photo sensor.
   Set 2 to enable micro switch.
5. Restart Netware Server.

To configure the LDSM for monitoring ASMM information:

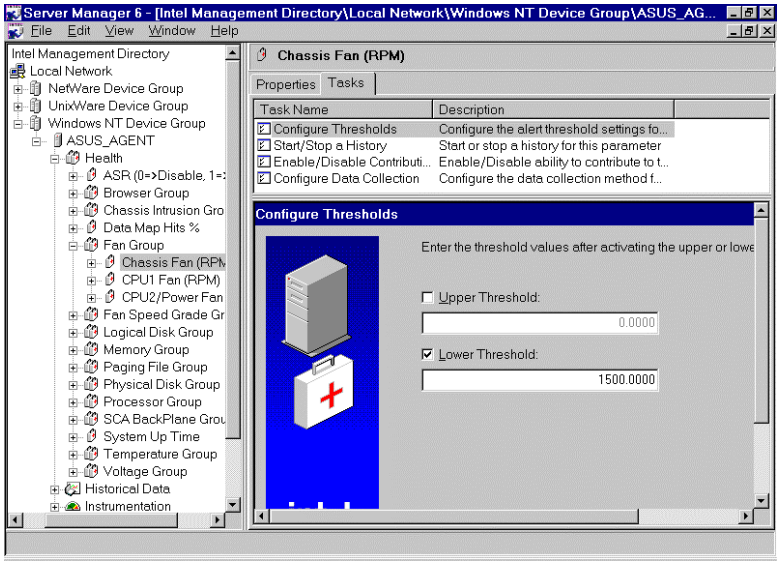
1. From the Windows NT desktop, choose **Start | LANDesk Server Manager | Local Network**
2. Click the Fan Group and Task.



3. Configure the Thresholds step by step.
   a. Select Threshold type.

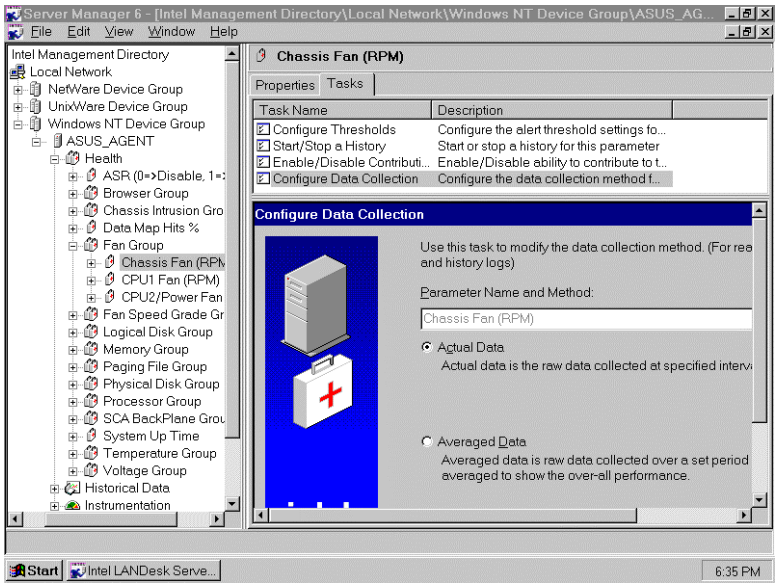


b. Set Threshold value.

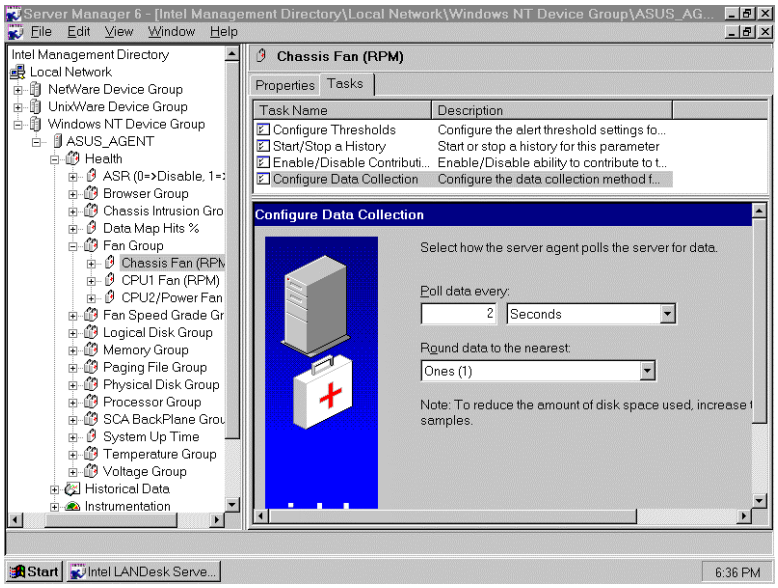


4. Configure the data collection method.

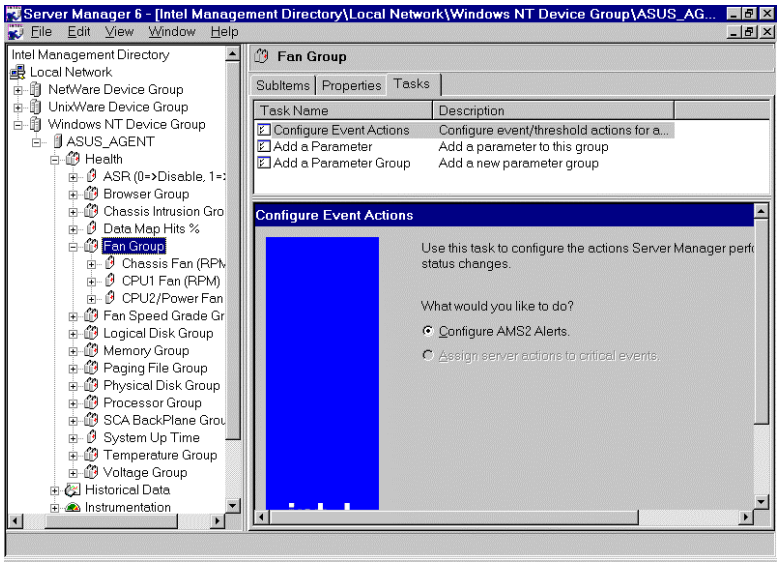
a. Modify the data collection method.



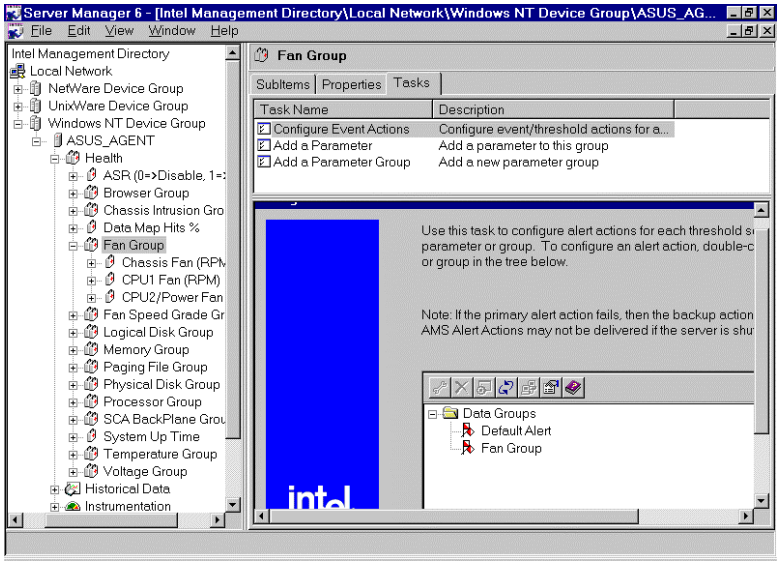
b. Select how the server agent polls the server for data.



5. To configure the Event in LDSM.

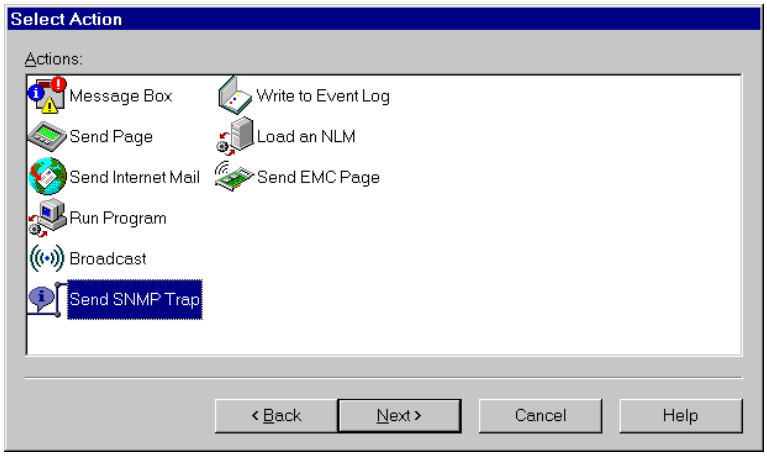


a. Choose Task, Select Configure Event Action.

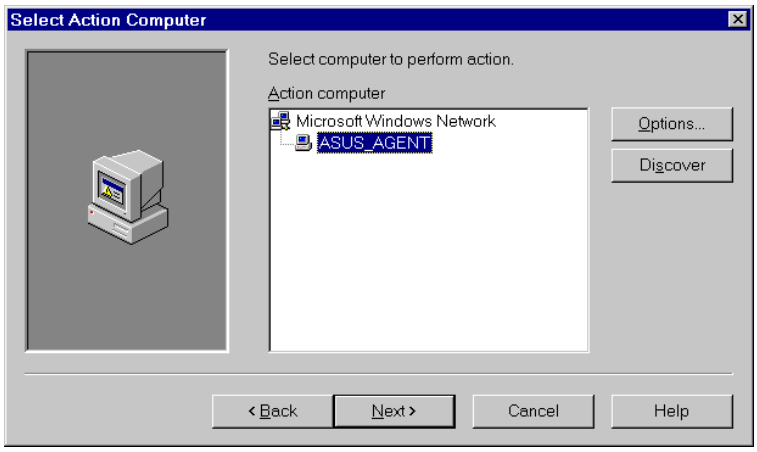


b. Double Click Fan Group.

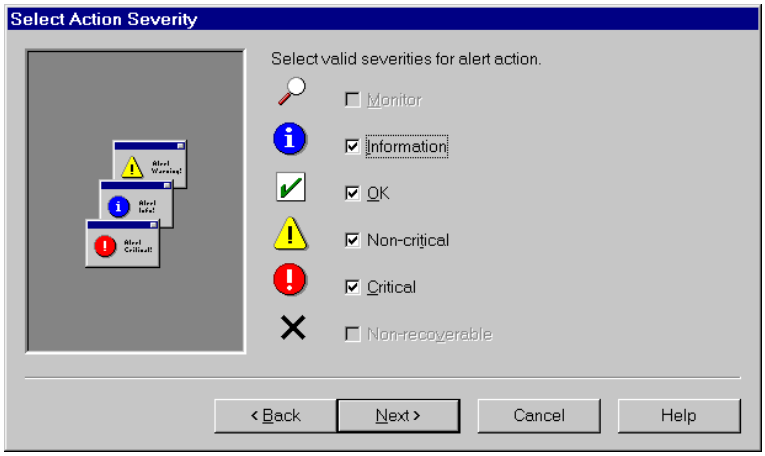
c. Select Send SNMP Trap, Click Next.



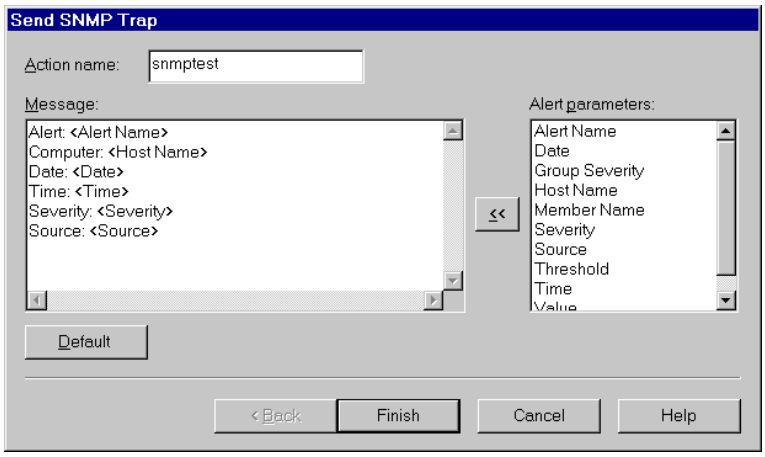
d. Select Action Computer, Click Next.



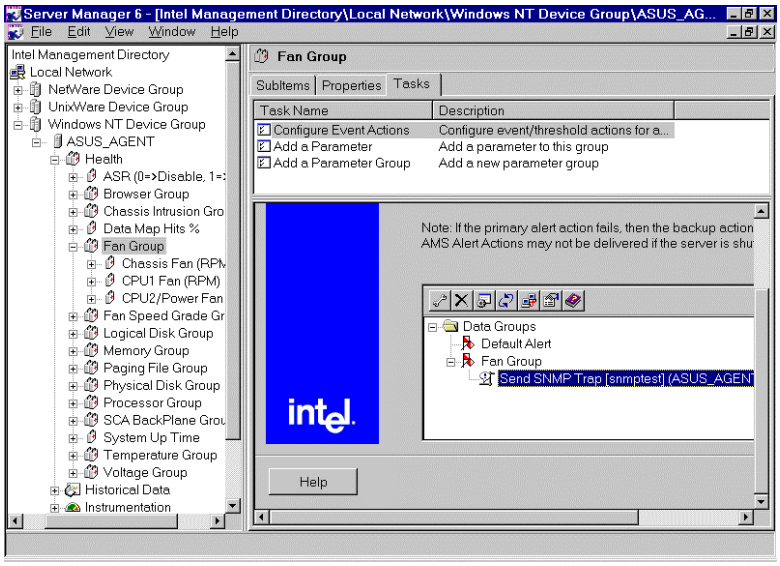
e. Select valid severities for alert action.



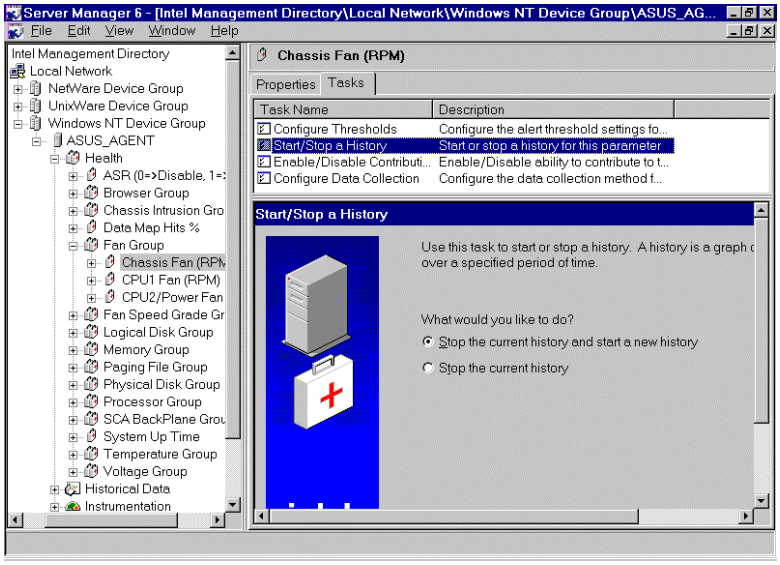
f. Type Action name, Select Message, Click Finish.


Send SNMP Trap
Action name:
snmptest
Message:
Alert: <Alert Name>
Computer: <Host Name>
Date: <Date>
Time: <Time>
Severity: <Severity>
Source: <Source>
Alert parameters:
Alert Name
Date
Group Severity
Host Name
Member Name
Severity
Source
Threshold
Time
Value
<<
Default
< Back
Finish
Cancel
Help

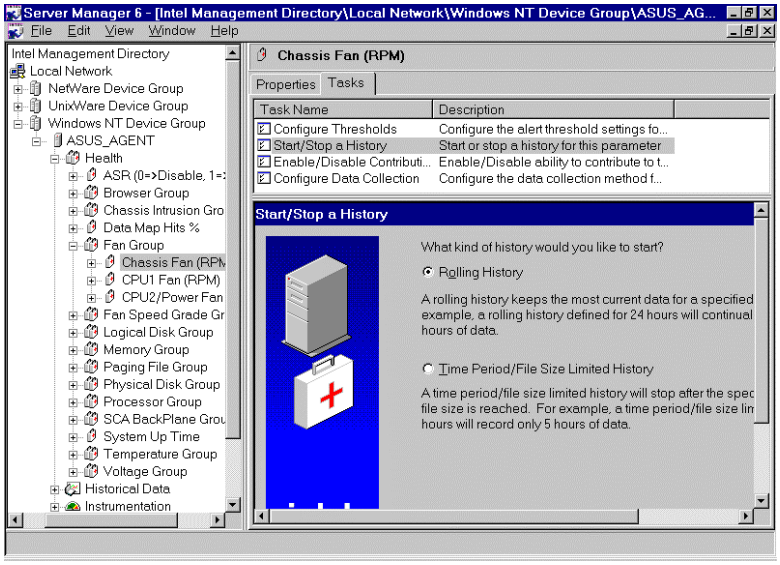
g. Then Configure Event Action is OK.



6. To configure a history log for ASMM information.

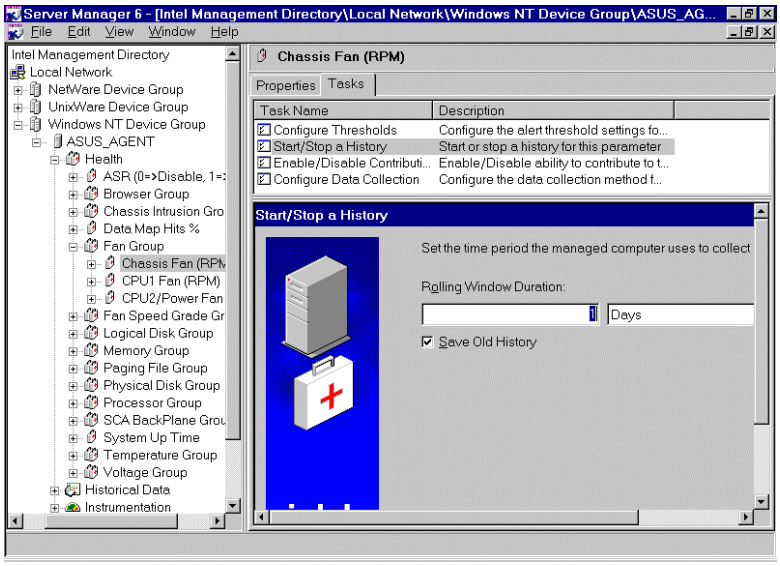


a. Select Star a new History, Click Next

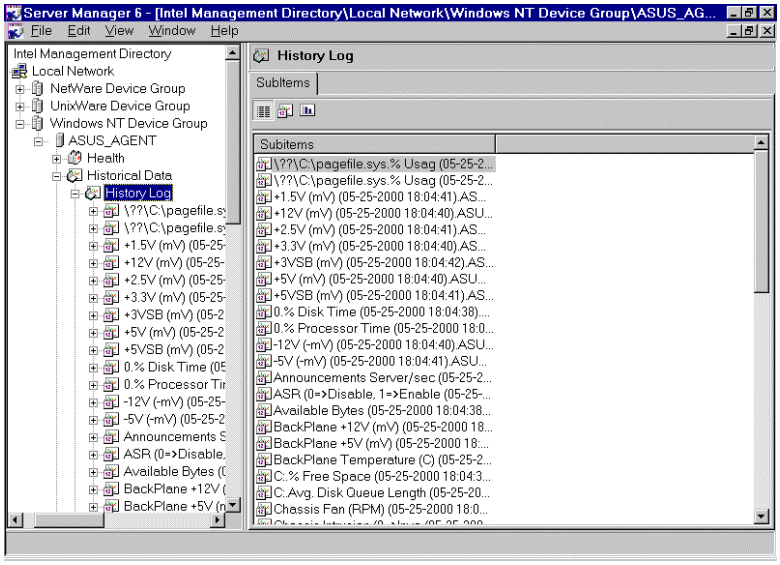


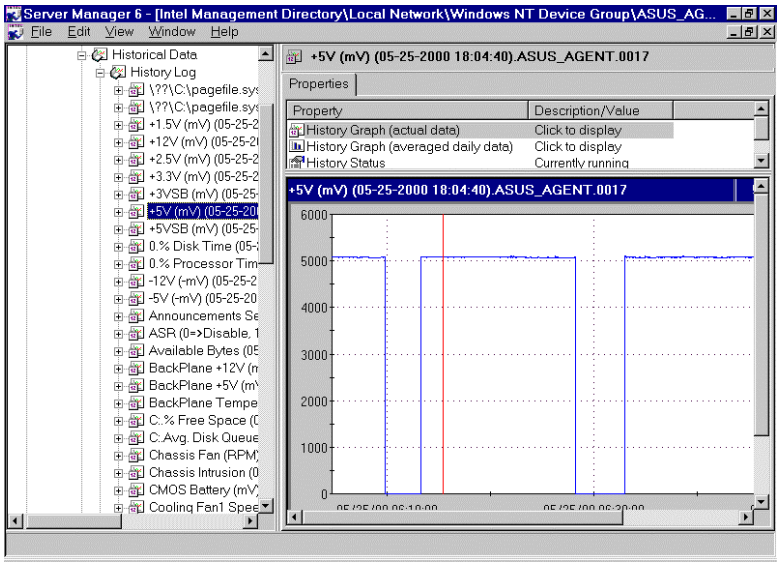
b. Select the kind of history, Click next

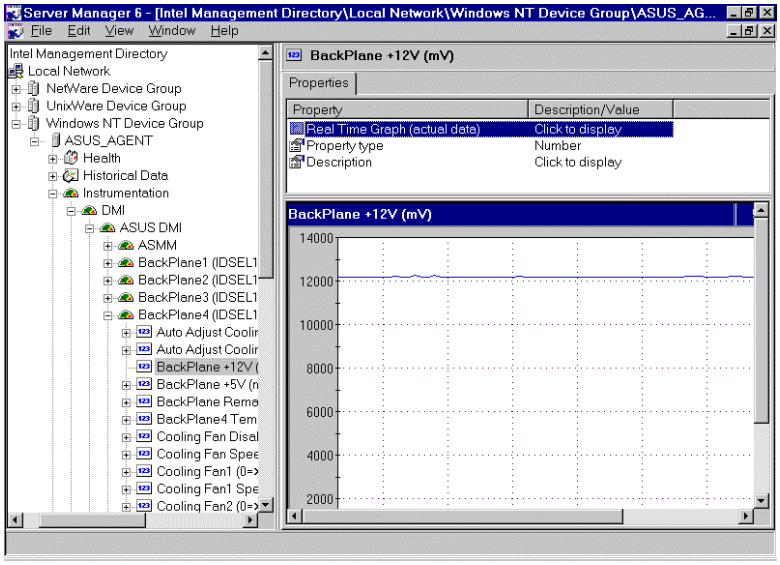
c. Set the time period the managed computer uses to collect data.



7. To view a History log for ASMM information.



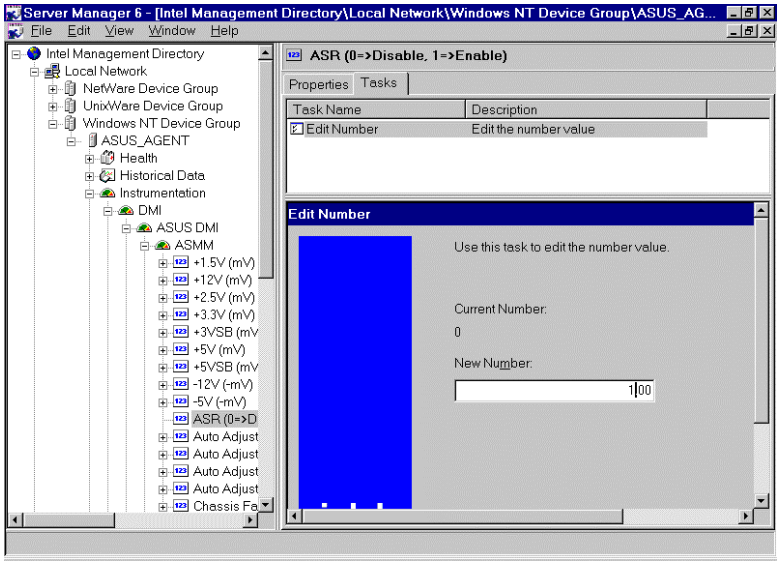




8. To monitor the DMI information.

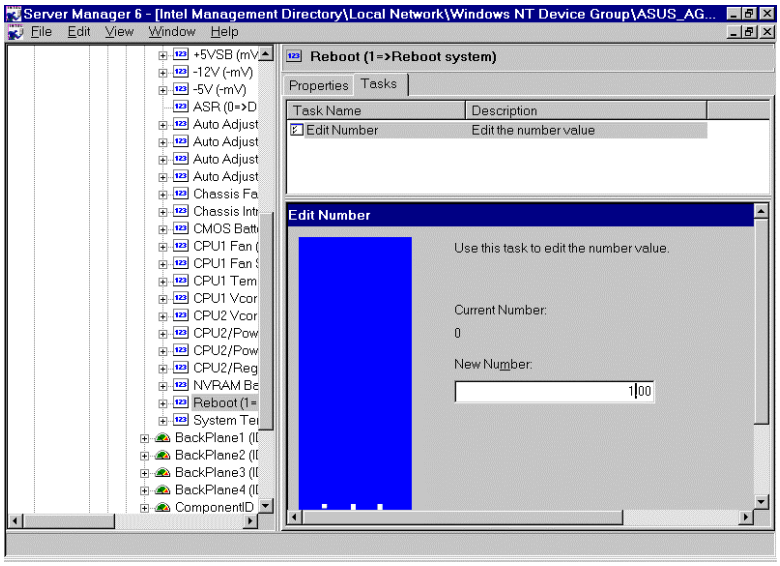
9. To Enable ASR

Set the number to 1, it will Enable the ASR



10. To configure Remote Reboot.

Set the number to 1, it will remote reboot the agent.



LDSM Application Integration Modules:

Application Integration Modules (AIMs) enable you to integrate managed desktop, mobile, and server systems running LDSM and LCM into popular enterprise management consoles, including:

HP Openview – Network Node Manager V5.01 for Windows NT

Tivoli TME – NetView V5.0 for Windows NT

Computer Associates Unicenter TNG for Windows NT

Key Feature:

1. Receiving and interpreting SNMP traps from LDSM/LCM managed nodes.
2. At-a-glance summary of **health** for managed nodes.
3. Icons that indicate warning and critical alerts on managed nodes.
4. Configuring device and send SNMP traps required several steps, as outlined by the enterprise management application.
5. For more information, please refer to http://www.intel.com/network/AIMs

In this OEM release, ASUS develops a DMI (2.0) CI (Component Interface) for Intel LDSM 6.1. This DMI CI will call ASMM (ASUS System Monitoring Module) driver to collect system fan speeds, working voltages, chassis intrusion status, system and cpu temperature. Our customer could see/monitor these informations through LDSM. Currently, ASUS developed this DMI CI for NT 4.0, Windows 2000 and Netware 4.x/5.x. The follow table is ASUS LDSM OEM function.

ASUS LDSM OEM function Table

Model / Function	P2B-LS Rev. 1.03 P2B-S Rev 1.03	P2L97-DS	P2B-D2 Rev 1.02	P2B-DS Rev. 1.03	P65Up8 / with ASMM card Rev. 1.04	CUV4X	CUR-DLS
Chassis Fan	X	X	X	X	X	X	X
CPU 1 Fan Speed	X	X	X	X	X	X	X
CPU 2 / Power Fan Speed	X (Power Fan)	X (CPU 2 Fan)	X (CPU 2 Fan)	X (CPU 2 Fan)	X (CPU 2 Fan)	X (Power Fan)	X
Chassis Fan Control						X	X
CPU1 Fan Control						X	X
CPU2/Power Fan Control						X (Power)	X
CPU 1 Vcore	X	X	X	X		X	X
CPU 2 Vcore		X	X	X			X
+3.3V	X	X	X	X	X	X	X
+5V	X	X	X	X	X	X	X
-5V	X	X	X	X	X	X	X
+12V	X	X	X	X	X	X	X
-12V	X	X	X	X	X	X	X
+1.5V						X	X
+2.5V						X	X
+3VSB						X	X
+5VSB						X	X
CMOS Battery						X	X
NVRAM Battery						X	X
System Temperature	X	X	X	X	X	X	X
CPU 1 Temperature	X		X	X		X	X
CPU 2 /	X		X	X			X

Regulator Temperature	(Regulator Temp.)		(CPU 2 Temp.)	(CPU 2 Temp.)			(CPU 2 Temp.)
ASR	X		X	X	X	X	X
Chassis Intrusion	X		X	X	X	X	X
Remote Reboot Management	X	X	X	X	X	X	X
Event Action	X	X	X	X		X	X
SCSI Backplane				X			X

(Notes: **X** is mean its VALUE is VALID in this mainboard)

LDSM can monitor the BackPlane's DriveBay status, the power system of DriveBay is good or bad, the cooling fan status of the BackPlane and the temperature of the BackPlane. It can also automatic adjust cooling fan speed depend on the temperature of the BackPlane.

LDSM OEM function on different BackPlane board

Function	DA-BP5 (Rev 1.03)	DA-BP5E	DA-BP4E	DA-BP3E
Temperature	X	X	X	X
Cooling Fan1 status	X	X	X	X
Cooling Fan2 status	X	X	X	X
Cooling Fan1 Speed (RPM)		X	X	X
Cooling Fan2 Speed (RPM)		X	X	X
+5V (mV)		X	X	X
+12V (mV)		X	X	X
LED/Fan Module status	X	X		
Drive(1~5) Plugin status	X	X	X	X
Drive(1~5) Power status	X	X	X	X
Cooling Fan Speed control	X			
Automatic Cooling Fan Speed Adjust	X			
Cooling Fan Enable/Disable	X	X	X	X
Backplane	X	X	X	X

Configuration Remap				
Drive Power off	X	X	X	X

LDSM can monitor the CPU1/CPU2/System temperature over the fatal high threshold value, then the event action will occur. The event action have reboot the system, power off the system and shutdown the system.

Default configuration for those new components/paths in Health Group

- Polling Rate : 2 seconds for all components/paths for monitor MB system
  5 seconds for all components/paths for monitor BackPlane system
- History Logs : ENABLED for all components/paths
- Critical Thresholds : DISABLED
- Warming Thresholds : DISABLED
- Informational Thresholds : DISABLED

Chapter 7 SNMP Management Station

7.1 HP Openview

The Openview SNMP program broadens the capabilities of SNMP-based management applications to control basic network devices and critical systems and applications. In addition to managing devices like routers, bridges, and hubs, the Extensible SNMP Agent allows you to manage applications, printers, users, and databases that are central to business success. The ability to control access to network and system resources and effortlessly monitor important network components gives you unprecedented visibility and control of your network infrastructure.

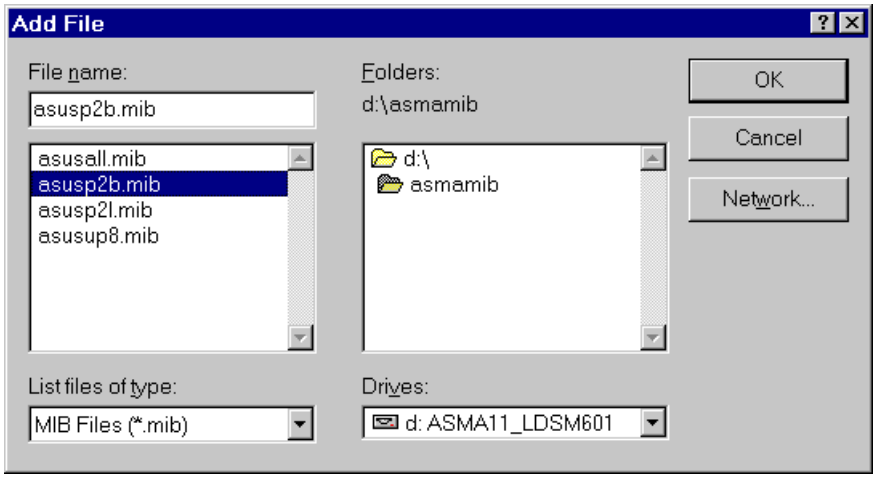
User may use HP Openview program to compile the ASUS MIB file, then user adds the compiled ASUS MIB file module to Openview to manage and operate the ASUS private Enterprise MIB with the computer system has installed ASUS System Monitoring Agent

To install a ASUS MIB file on HP Openview

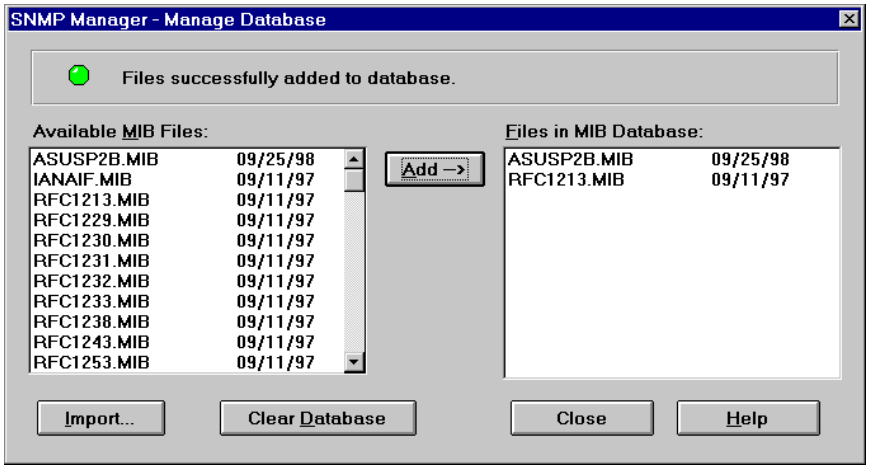
The Manage Database option is accessed from the SNMP Manager command under the Control menu. Manager Database accesses a compiler that adds ASUS MIB file to the MIB database; also adding to the list of variables displayed in the Defined Query window.

Installing ASUS MIB file to HP Openview

1. Click **Control** menu.
2. Select **SNMP Manager**.
3. Select **Manage Database**.
4. Click **Import**.
5. Select ASUS MIB file into **File Name**, Click **OK** button.

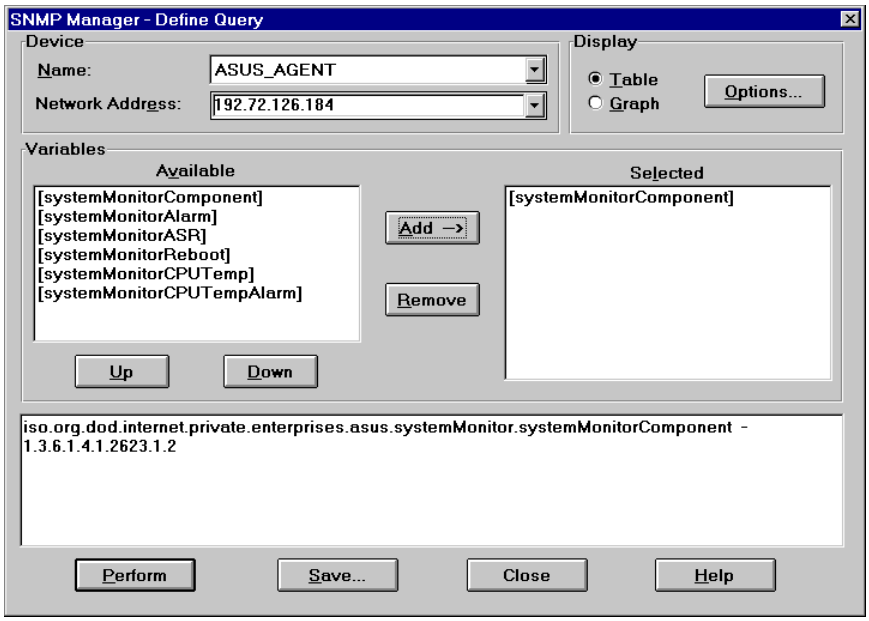


6. From Available MIB files box, select **ASUSMIB.MIB** and click **ADD** button.

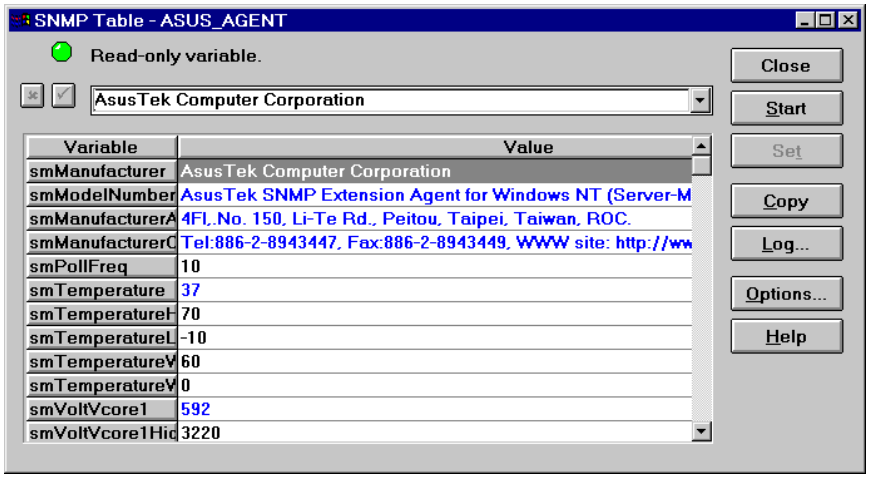


Using HP Openview to monitor ASUS Server

1. From **Control** menu, Select **SNMP Manager**, Select **Defined Query**.
2. Using **Up** and **Down** to \iso\org\dod\internet\private\enterprise\asus\systemMonitor

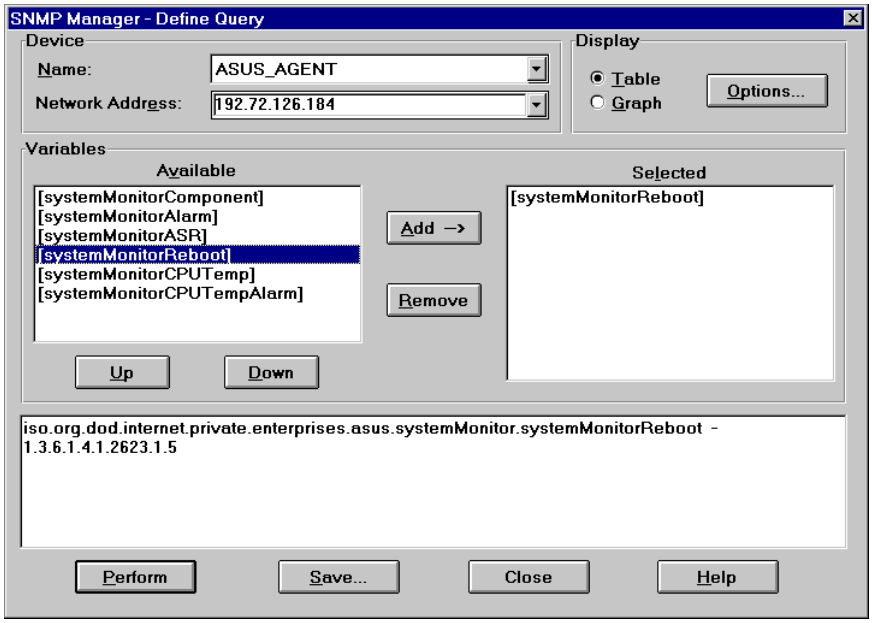


3. Select the Server name from **Name** box.
4. From **Available** box, Select **systemMointorComponent**, Click Add, Click **Perform.** Then you can view the information about ASMA

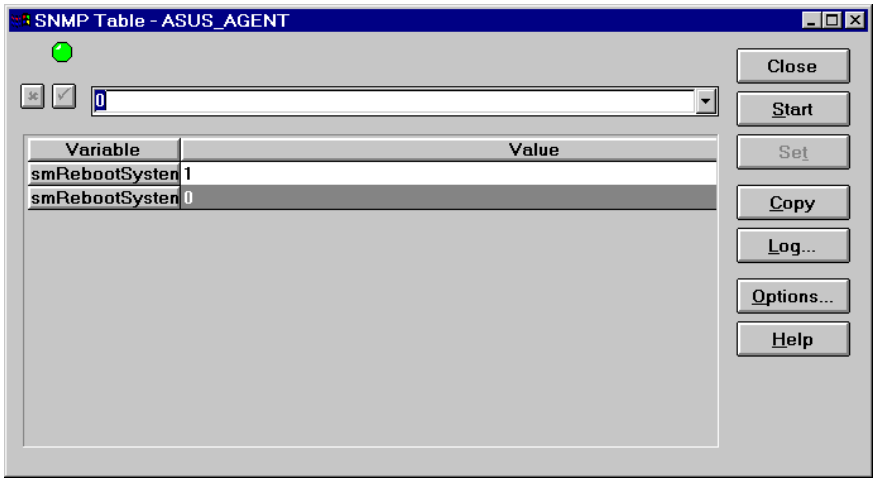


(View / Monitor ASMA Information)

5. Select the **systemMonitorReboot**, Click **Add**, Click **Perform**.



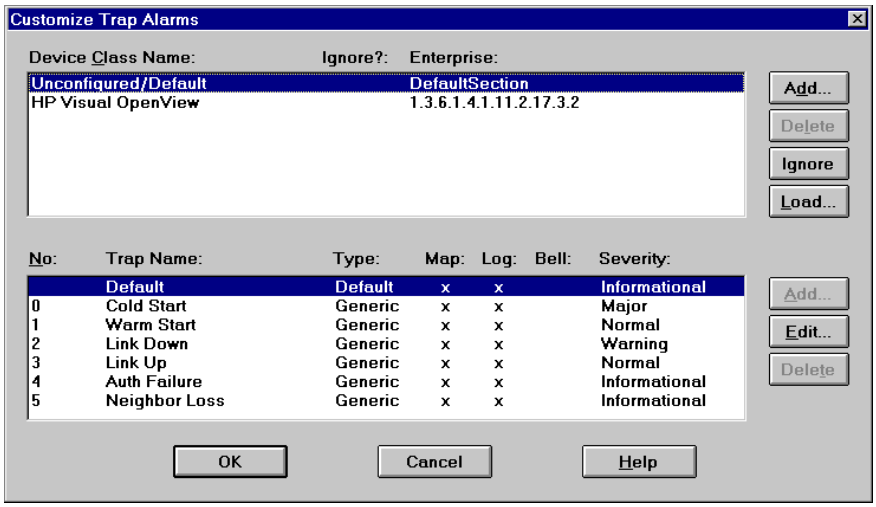
6. Modify the rmRebootSystemEnable variable from 0 to 1 and click SET.



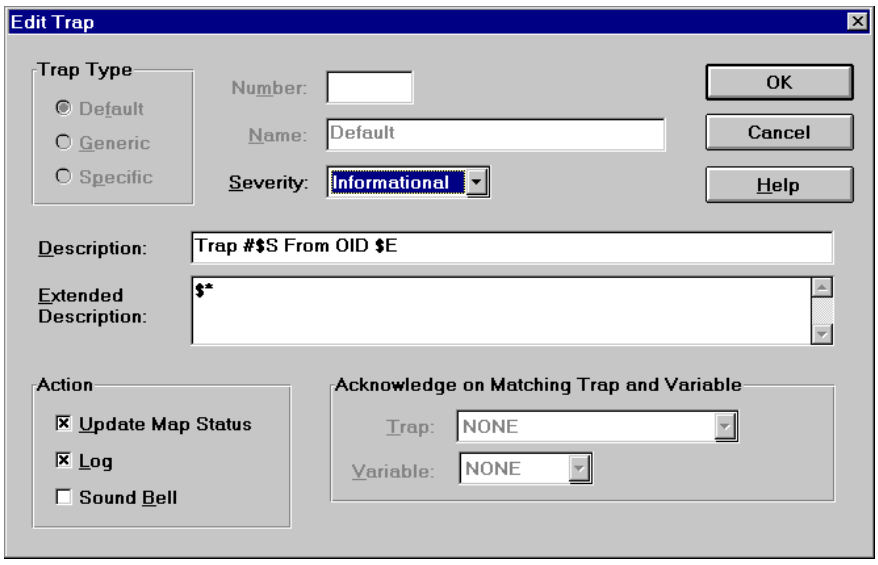
(Configure ASMA information)

Configing SNMP Trap for HP Openview:

1. From **Auto Discovery** menu, Select **Layout**, Select **Do Basic Layout**
2. From **Options** menu, Select **Customize Trap**
3. Select **Unconfigured/Default**, **Default**, Click **Add**.

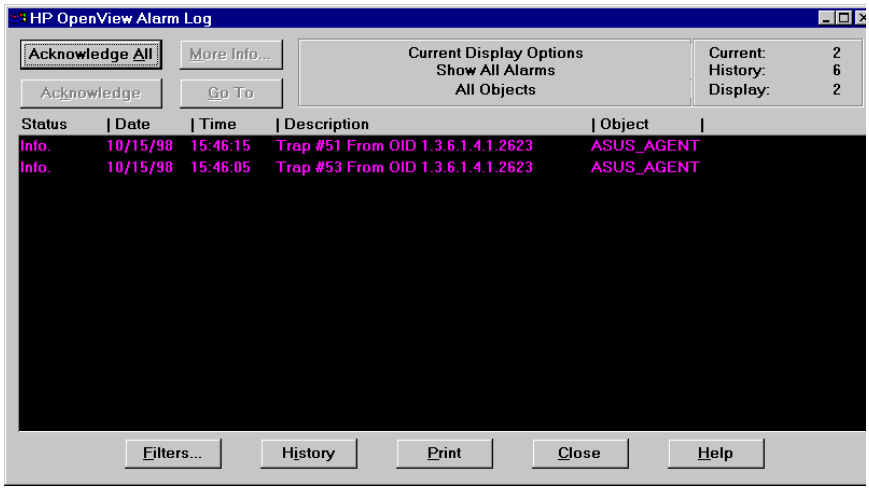


4. From **Extended Description box**, Type $*, Click **OK**.

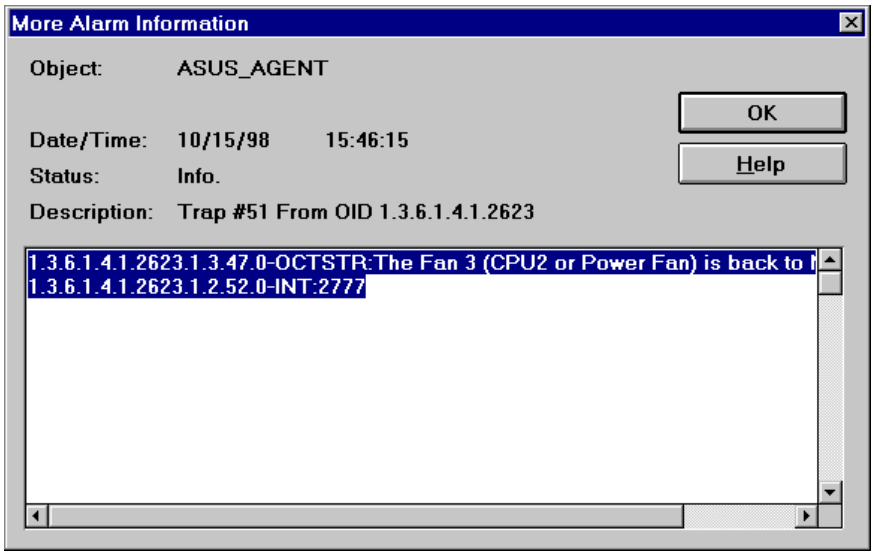


Receiving SNMP Trap

1. From **Monitor** menu, Select **Alarm Log**



2. Click **more info** to view the detail information.



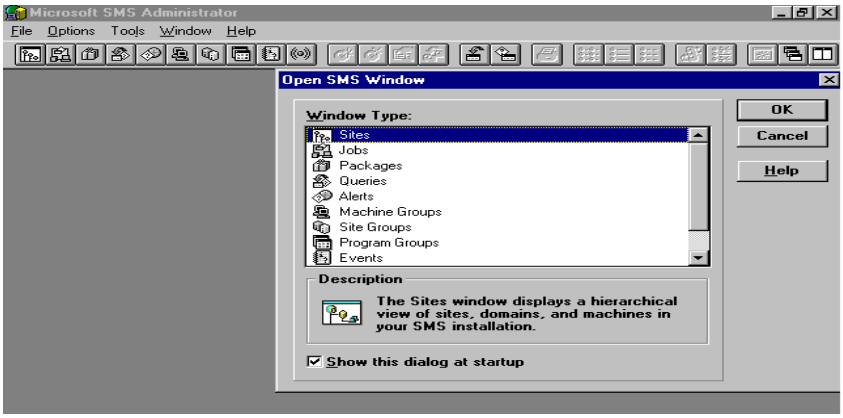
7.2 Microsoft SMS

Microsoft Systems Management Server (SMS) is a solution for centralized management of Windows-based environments. SMS offers features that can help administrators streamline their work and increase user productivity, and Microsoft has included the product in its Zero Administration Initiative for Windows — an effort designed to help companies lower the total cost of owning and operating technology.

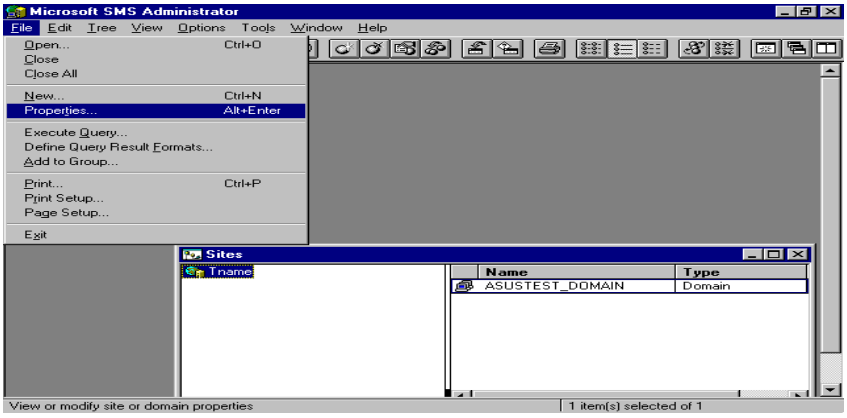
The session describes how to configure SMS to be a SNMP trap receiver. In 7.2.1, we discuss how to set up a SNMP filter to filter which SNMP traps we are interested. In 7.2.2, we introduce how to view the SNMP traps in your site. Finally, in 7.2.3, we provide another method (Query your site database) to get the traps that we are interested.

7.2.1 Create an SNMP trap filter

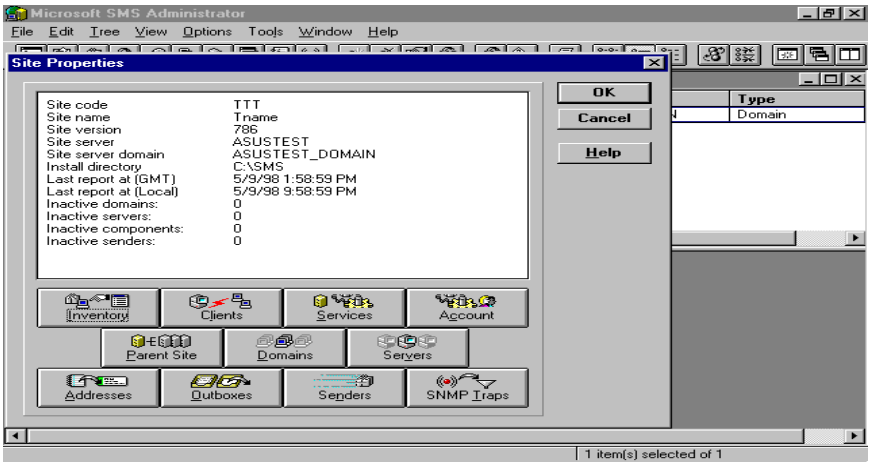
1. Start your SMS administrator, and open sites window.



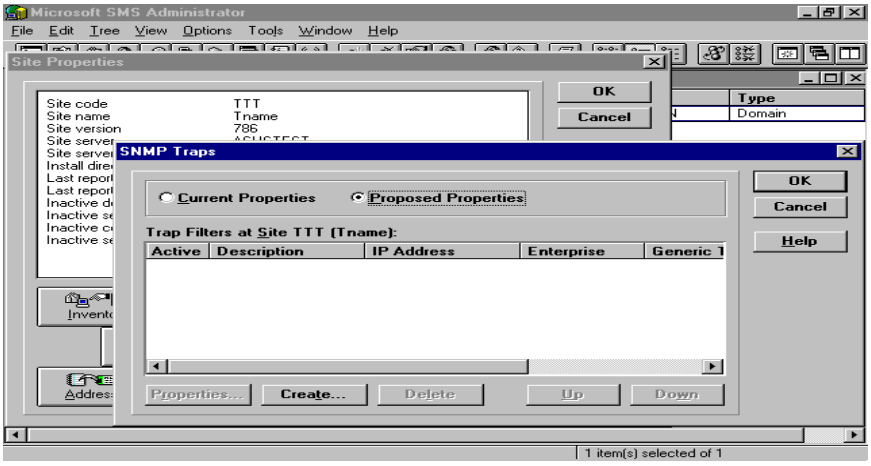
2. Click the site name, and select the properties from File menu.

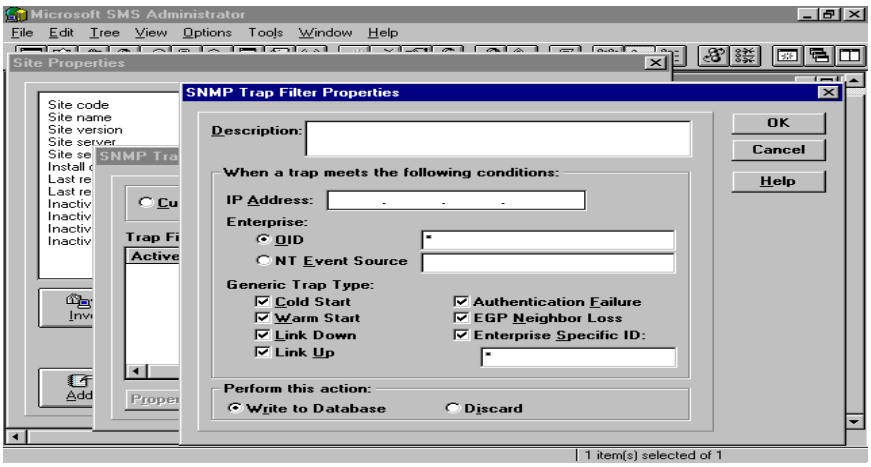


3. In the Site properties dialog box, choose and press SNMP Traps button, and then the SNMP trap dialog box will be shown.

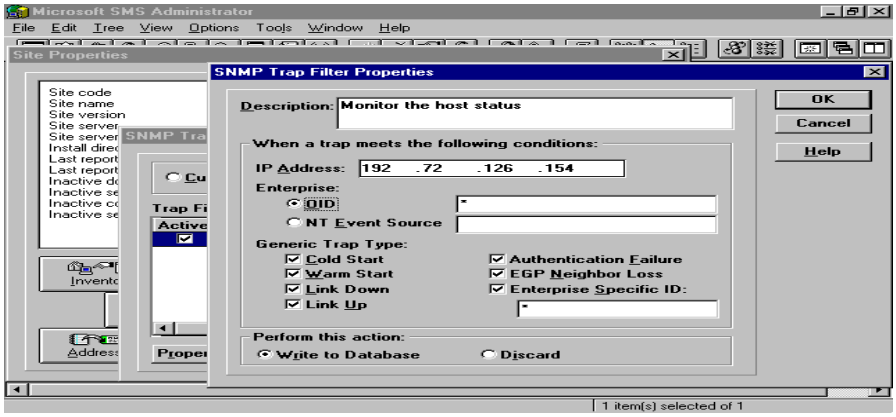


4. Check the proposed properties box and press the Create button, the other window (SNMP Trap Filter Properties) will be popped up.

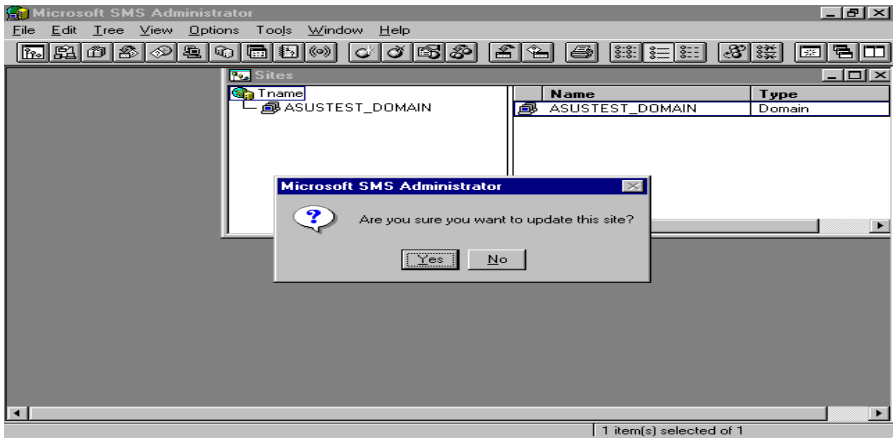




5. Fill out the conditions that traps will be caught and their description. In additions, choose the action type is either Write to Database or Discard, and then press OK button, a filter has been generated.



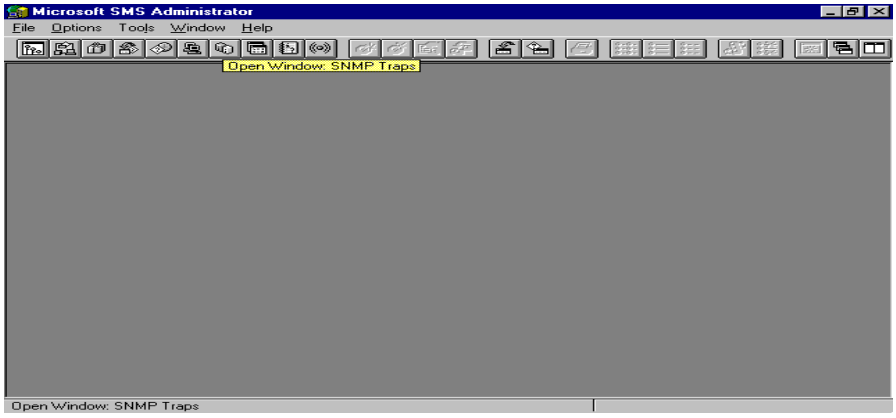
6. Press OK button in SNMP Traps and Site properties window, SMS will require you to confirm the settings you has generated mentioned above.



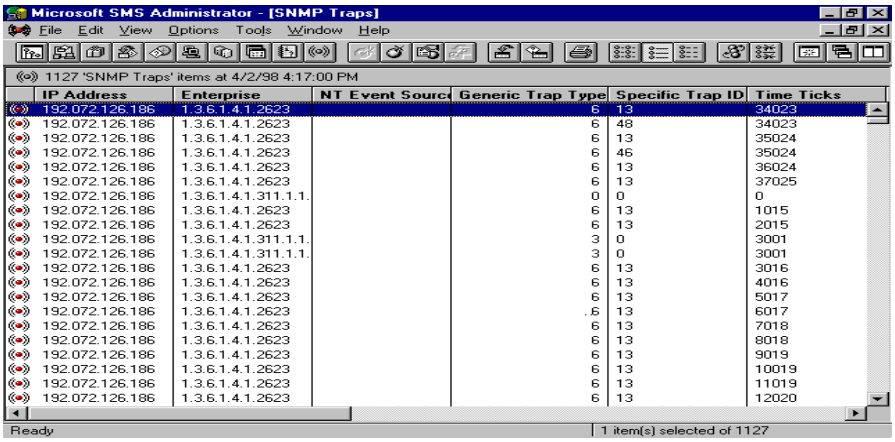
7. SMS updates the site database for this filter rule.

7.2.2 View SNMP traps in a Site

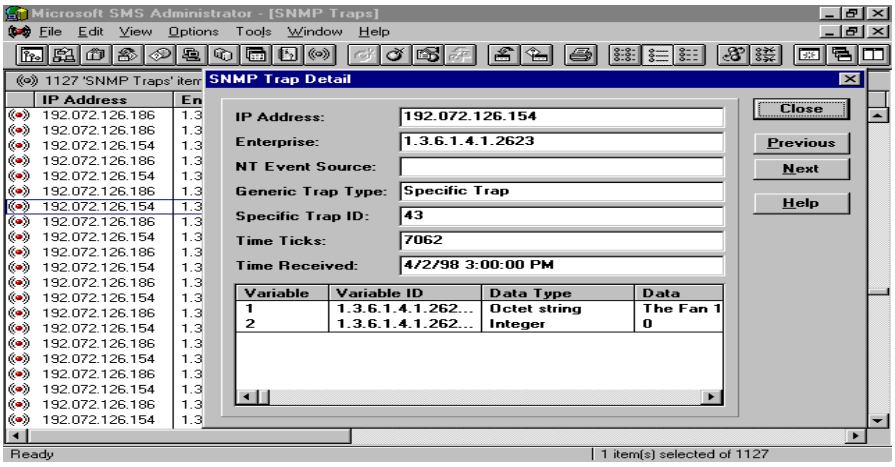
1. Start your SMS administrator.



2. Open SNMP Trap window, and then all the traps recorded in the site's database will appear.



3. The traps list shows every trap in different aspect (parameter) such as IP address, Enterprise, NT Event Source, Generic Trap Type, Specific Trap ID, Time Ticks, Time and Date Received, Number of Variables and Variable N Data.



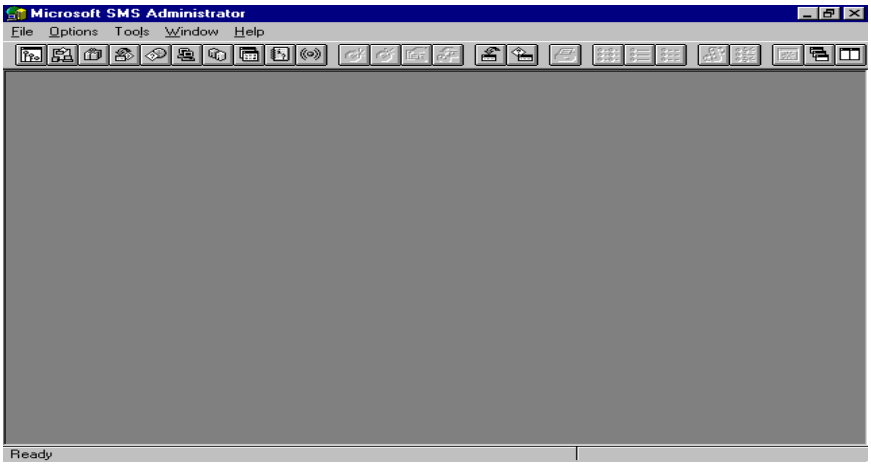
4. Double click in the trap you want to investigate in detail.

5. Choose either Previous or Next button to get the proceeding or following detail trap message.

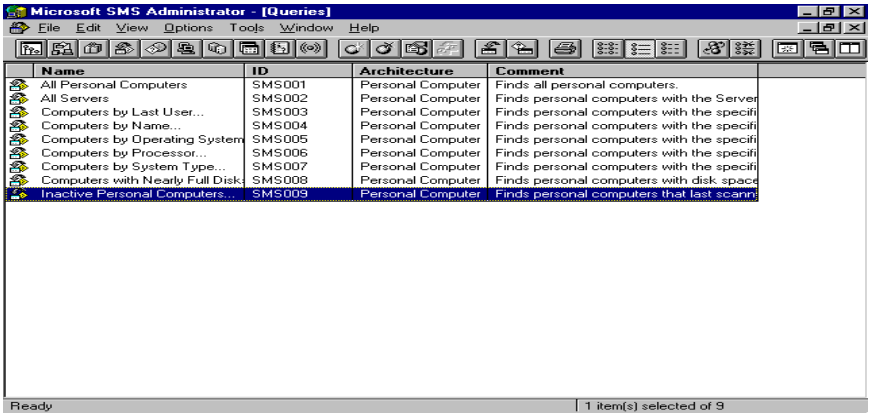
6. Press Close button, and then return to the original SNMP Traps window.

7.2.3 Query the database for SNMP traps

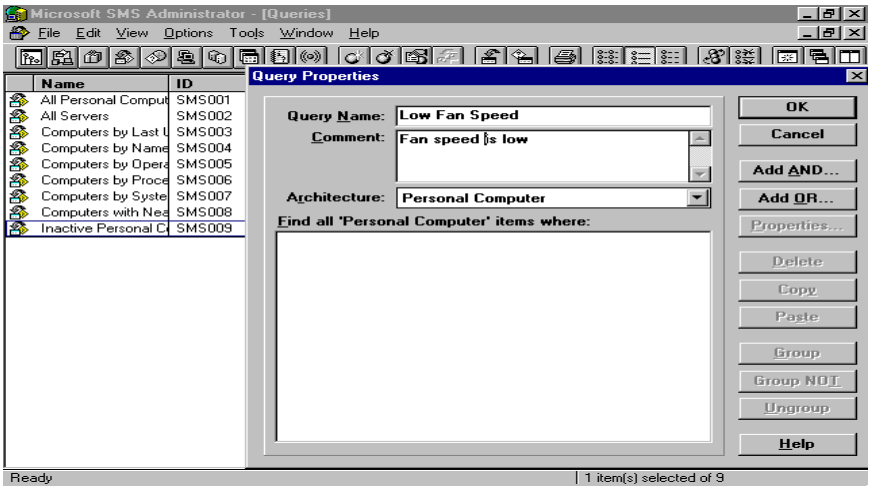
1. Start your SMS administrator.



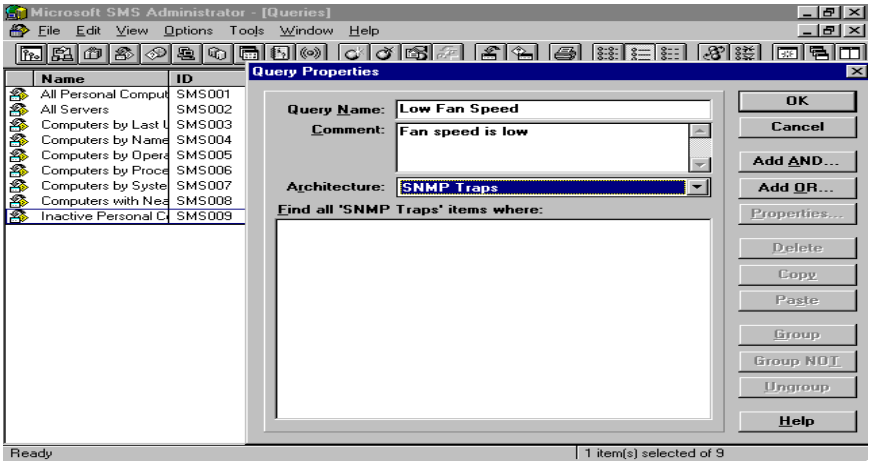
2. Open Queries window.



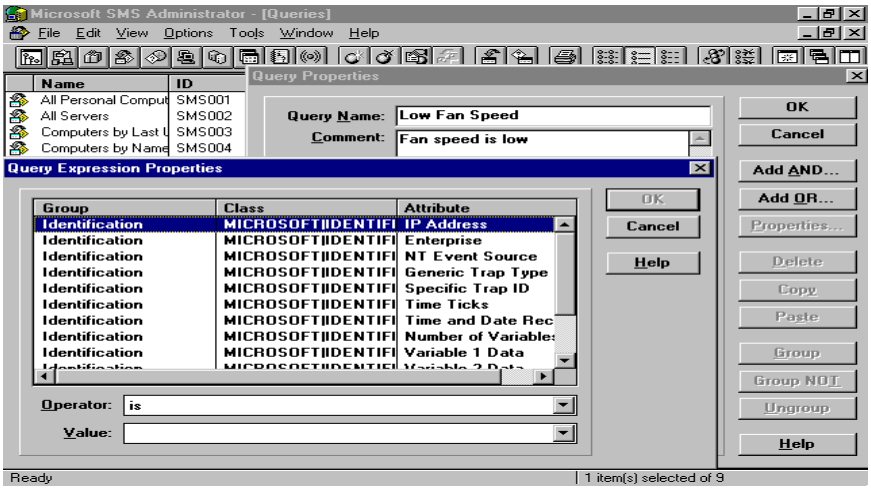
3. Choose New from File menu and fill out these fields such as Query Name and Comment.



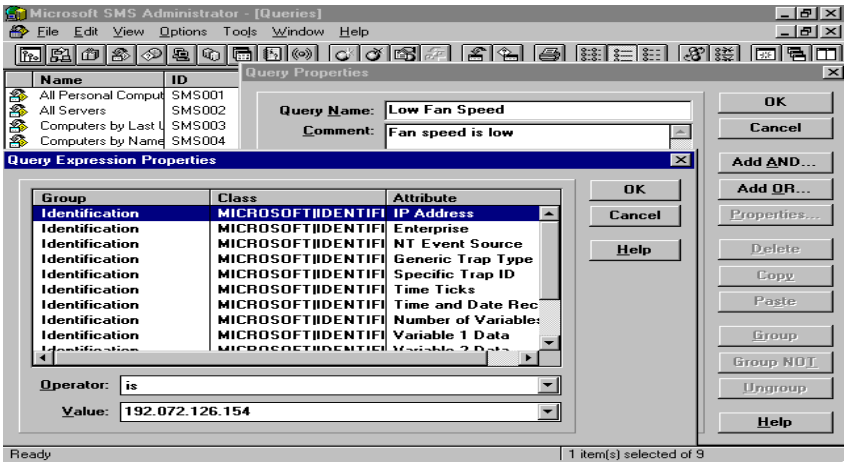
4. Choose SNMP Traps from Architecture field.



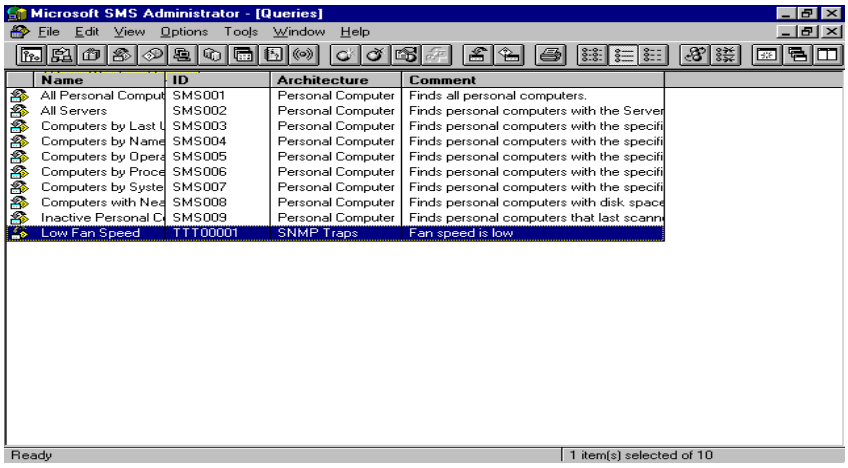
5. Press Add AND or AND OR button to add your query conditions, and then the Query Expression Properties dialog box will be shown.



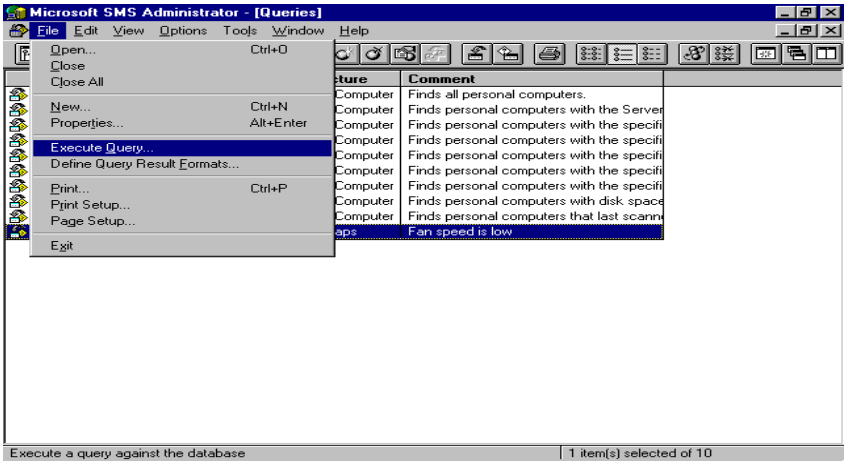
6. Select the Attribute column you want to operate with your expression, and fill out the condition as the expression form (Operator and Value).



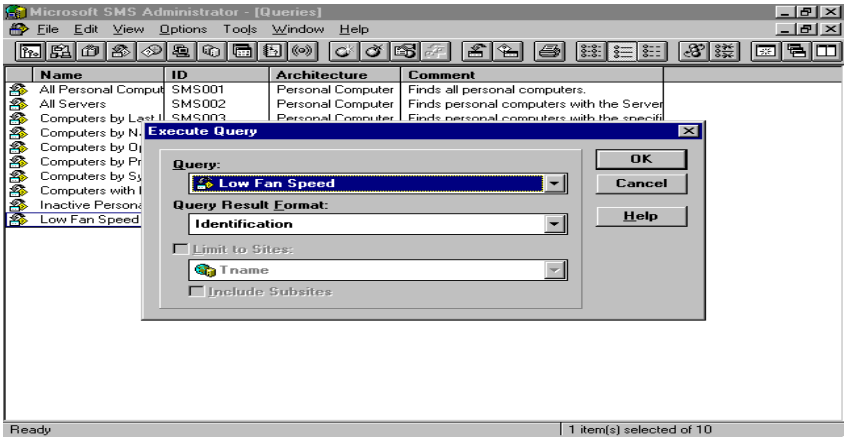
7. Press OK button in Query Expression Properties and Query Properties dialog boxes, and then the query condition is added in Query window.



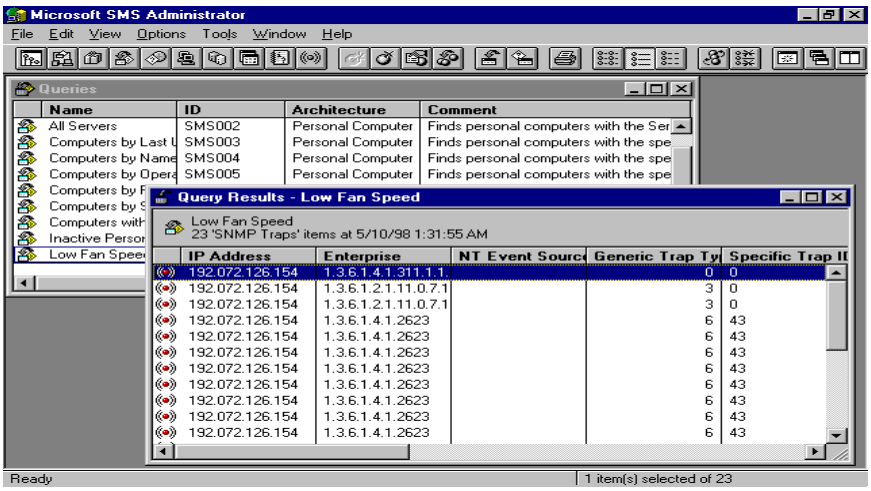
8. Choose Execute Query from File menu.



9. SMS confirms you whether the query action will be done.



10. The events you are interested will be queried out from SMS database.



7.3 Solaris Solstice Site/SunNet/Domain Manager

In this section, we will firstly introduce how to convert our ASUS MIB to schema file that Solstice knows, and then introduce how to load the schema file into the runtime database of Site/SunNet/Domain Manager. Finally, we will introduce how to get/set the values of attributes of the SNMP agent and describe how to view the SNMP traps from Site/SunNet/Domain Manager.

7.3.1 Convert ASUS MIB to schema file

In order to use our SNMP agent characteristic, firstly you should convert our MIB to schema file that Solstice knows. Furthermore, we also prepare our schema file, so you can skip the step except that upload the schema file from our CD to the UNIX via the ASCII mode of FTP and then copy the schema file into /opt/SUNWconn/snm/agents directory.

For example, you can type as follows in command line environment.

1. cd /opt/SUNWconn/snm/agents
2. cp /(our asusmib.mib path)/asusmib.mib .
3. mib2schema asusmib.mib

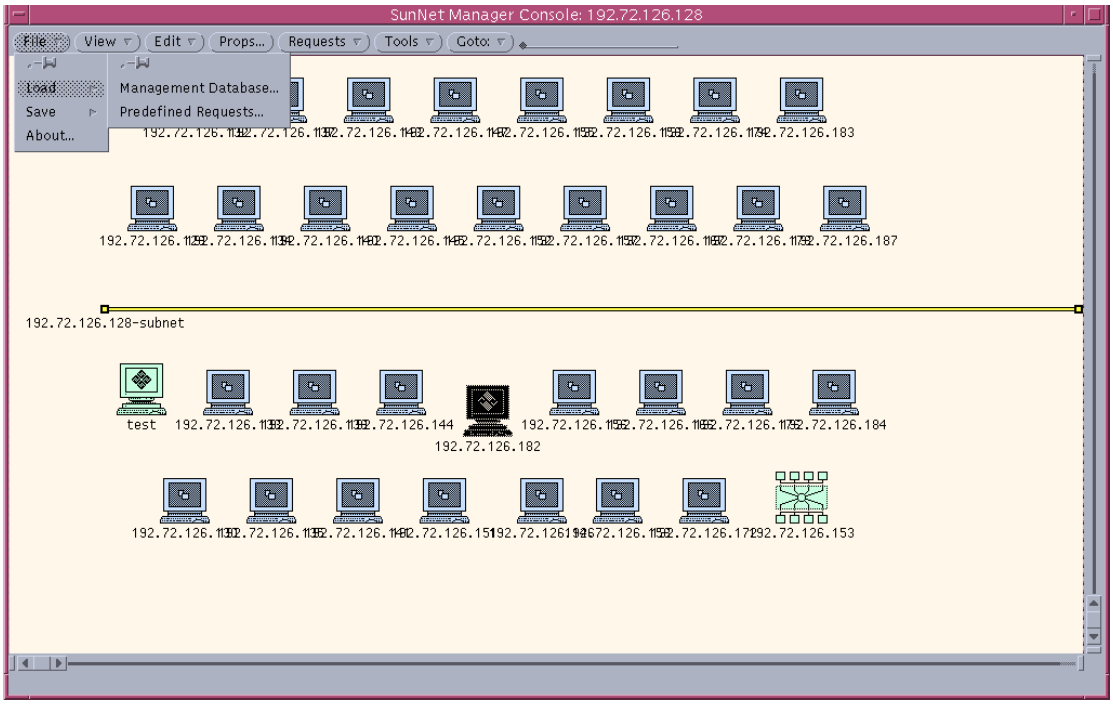
* If you find the schema file translated from asusmib.mib that contents of ^A (Ctrl+A) character, replace it with the space character in the entire file.

7.3.2 Load the schema file from your Domain Manager console

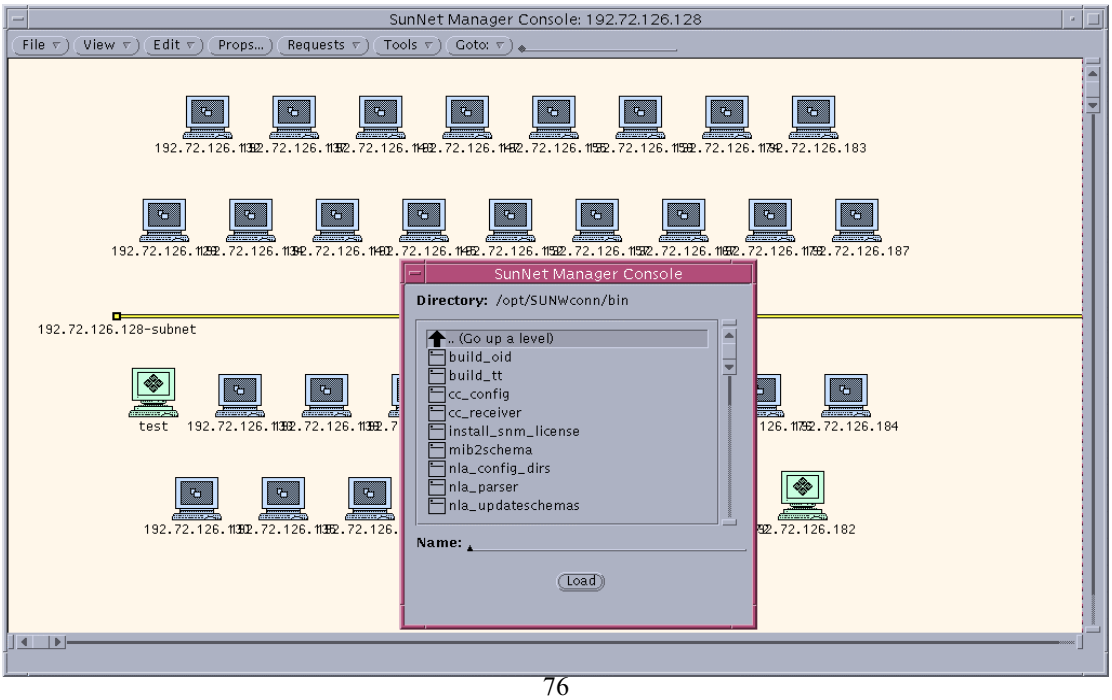
1.From the File menu, choose LOAD, and then choose Management Database….

P.S. If you see the following error message in the footer of Domain Manager console,and the detail error message shown in error report is **duplicate attribute name** , you can ignore it.

Load of asusmib.mib failed – see error report for details.

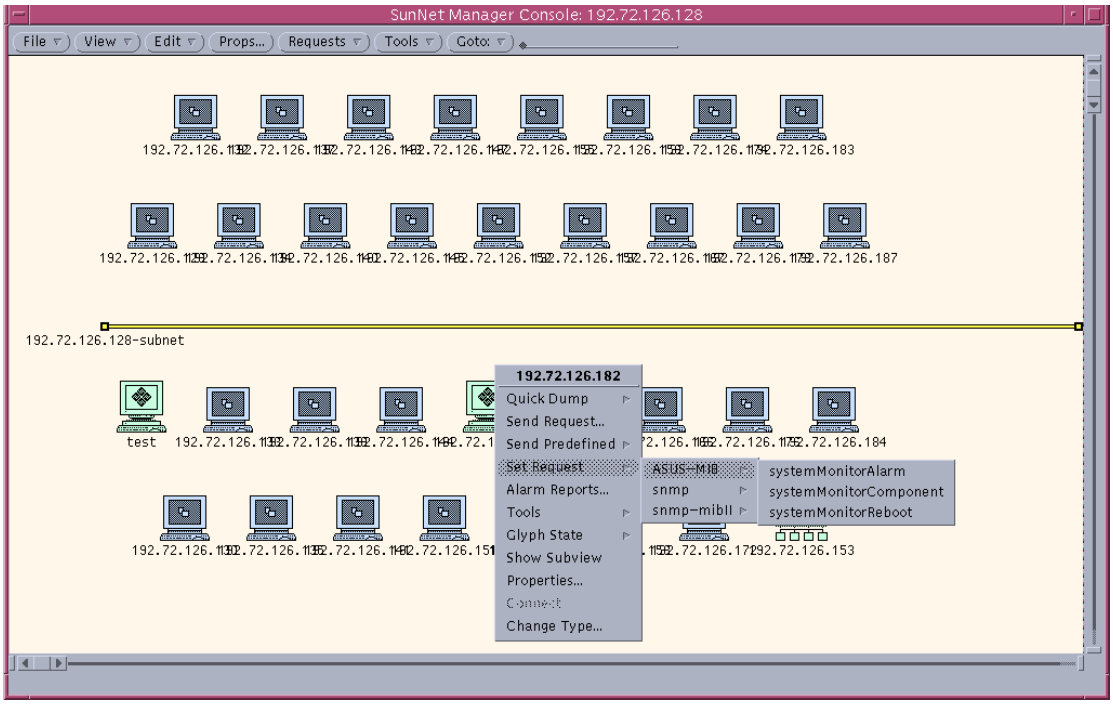


2. Select the file name you want to load.

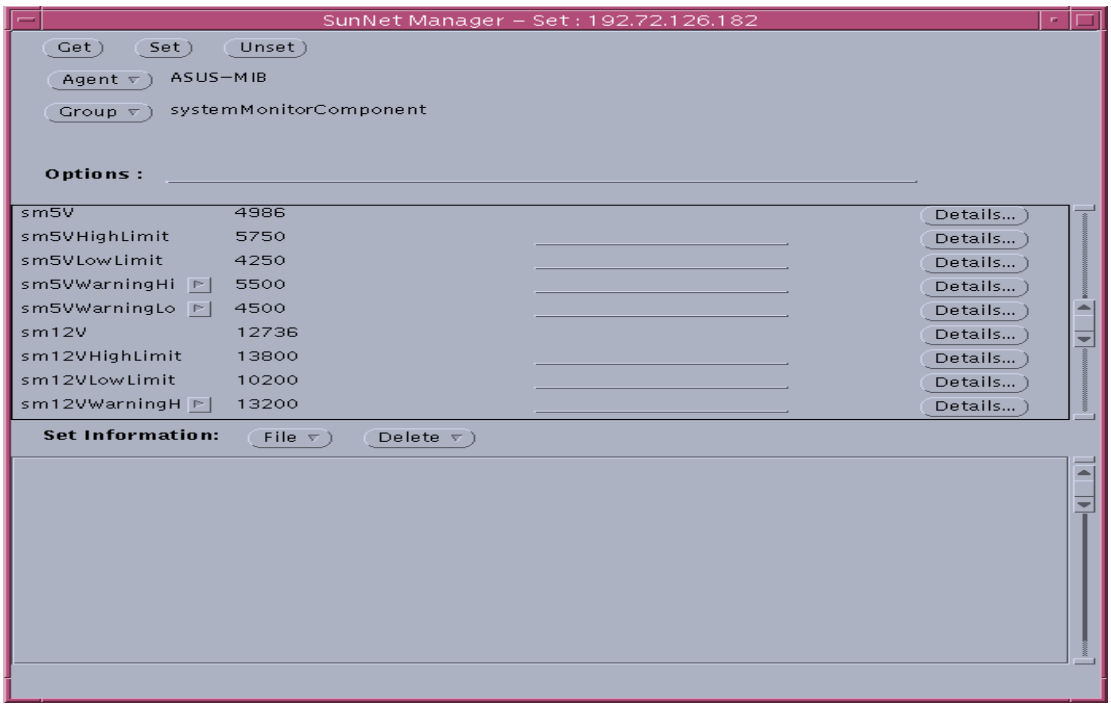


7.3.3 Get/Set the values of attributes of the SNMP agent.

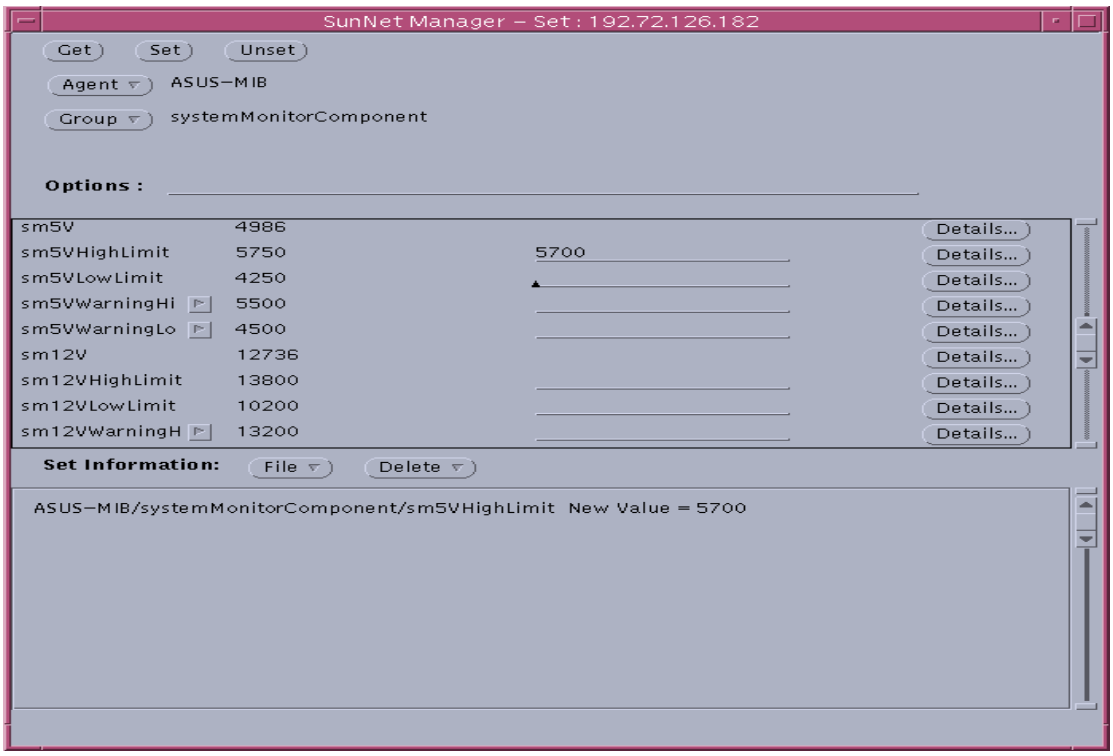
1. Over the target machine icon, press the right button, and choose the Set Request → ASUS-MIB → systemMonitorComponent.



2. Press the Get button on the top.

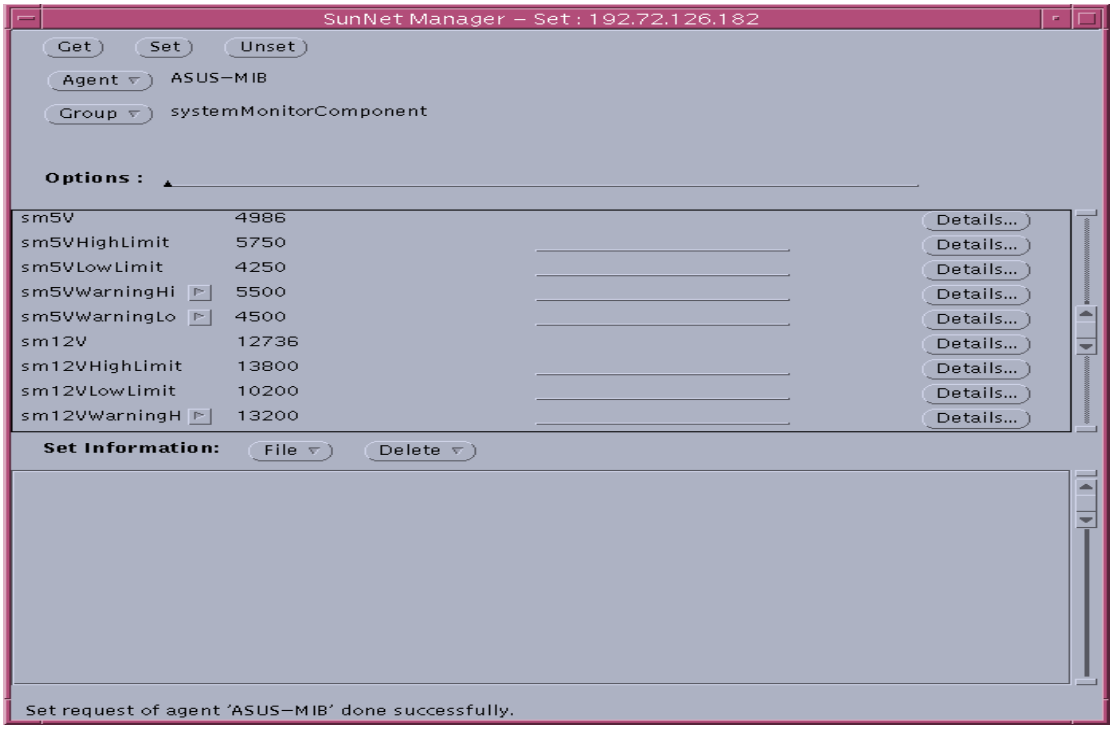


3. Input the new value of attribute that you want to modify on the middle portion.



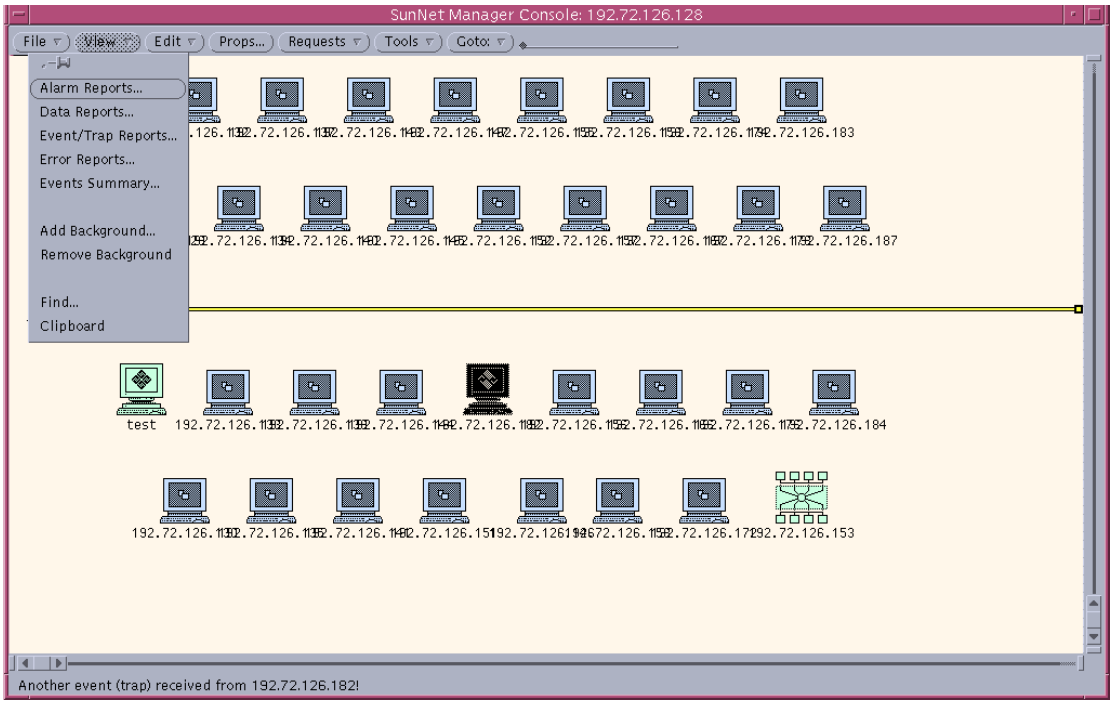
4. Press the Set button and then the following message will be shown in the footer.

Set request of agent **ASUS-MIB** done successfully.

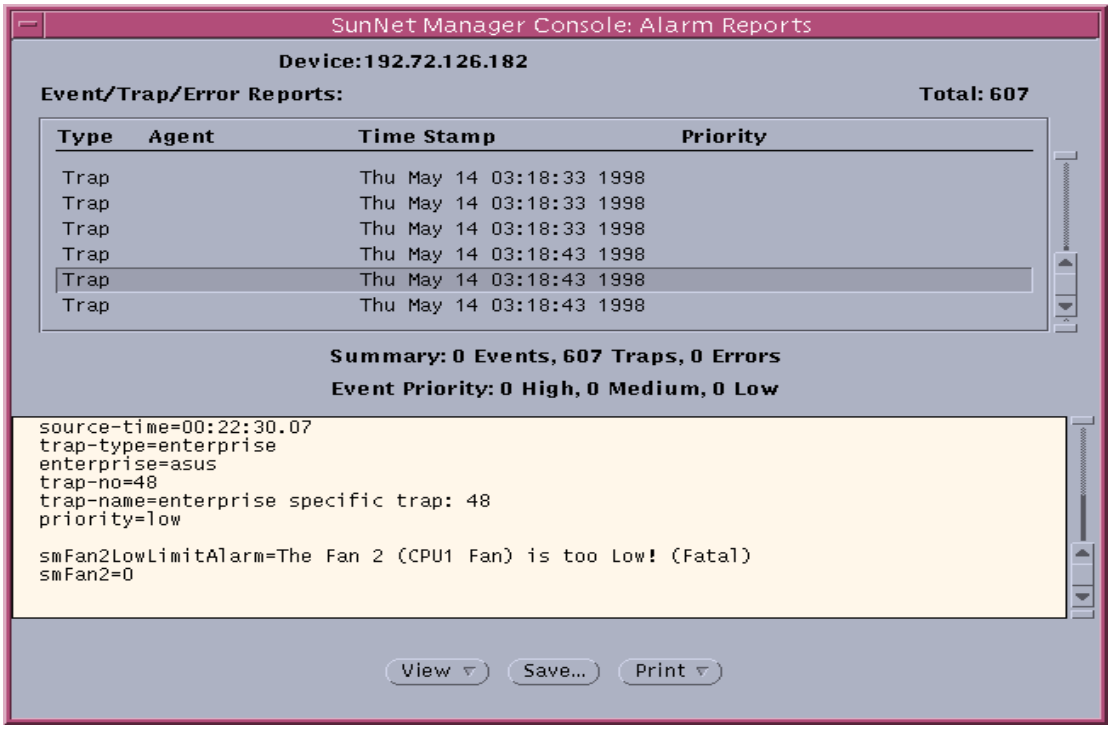


7.3.4 View the SNMP Trap

1. Over the target machine icon, press the left button. And then from the View menu, choose Alarm Reports….



2. Choose the trap that you want to view in detail.

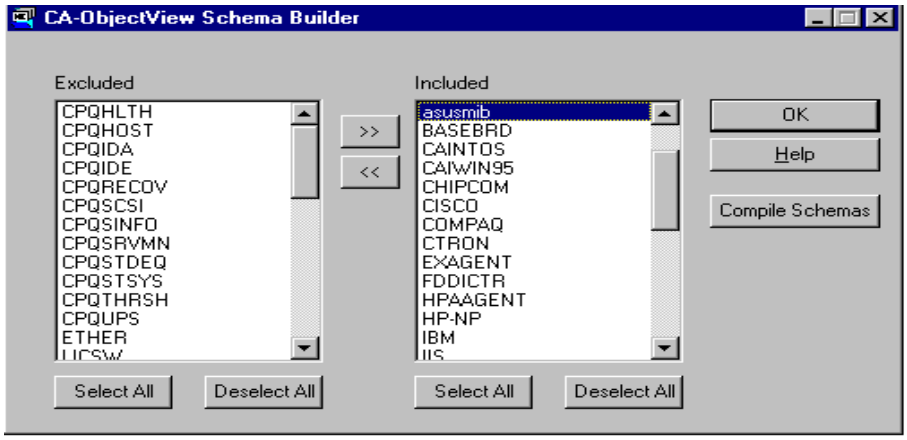


7.4 CA-TNG

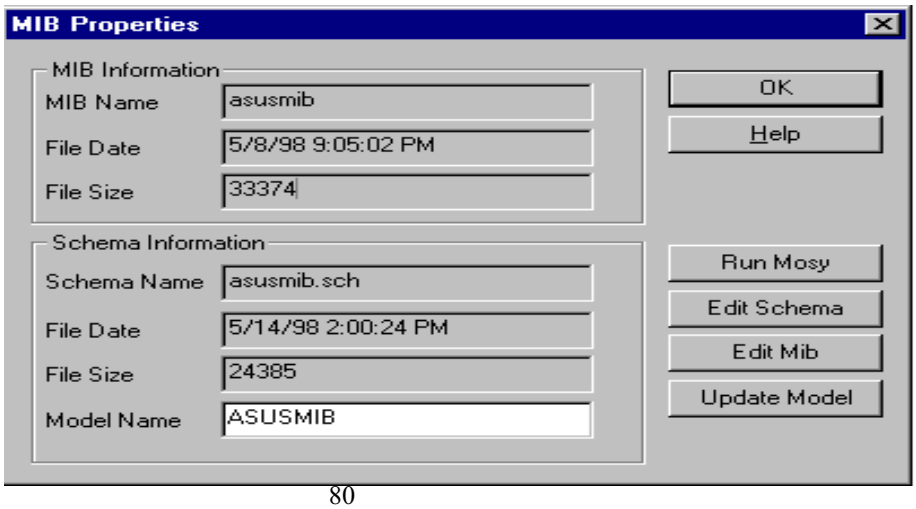
Unicenter TNG addresses today's most pressing IT management challenges through a tightly integrated set of core solutions. The breadth of these management solutions and their ability to work together delivers true end-to-end management of the environment and sets Unicenter TNG apart from other enterprise management offerings. Unicenter TNG's ability to manage the entire enterprise from a business process perspective renders it the industry's only practical solution for today's unwieldy environments. In fact, Unicenter TNG is widely recognized as the standard for enterprise management.

To monitor the ASMA in CA-TNG:
Step 1: Copy ASUS MIB file to \tngfw\schema\excluded

Step 2: Choose the ObjectView Schema Builder and In excluded box, please select ASUSMIB and click >> button.

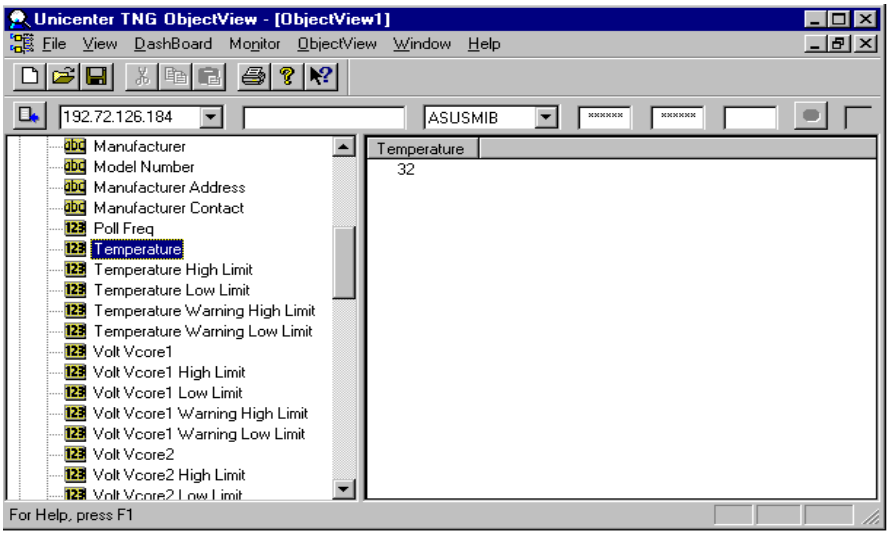
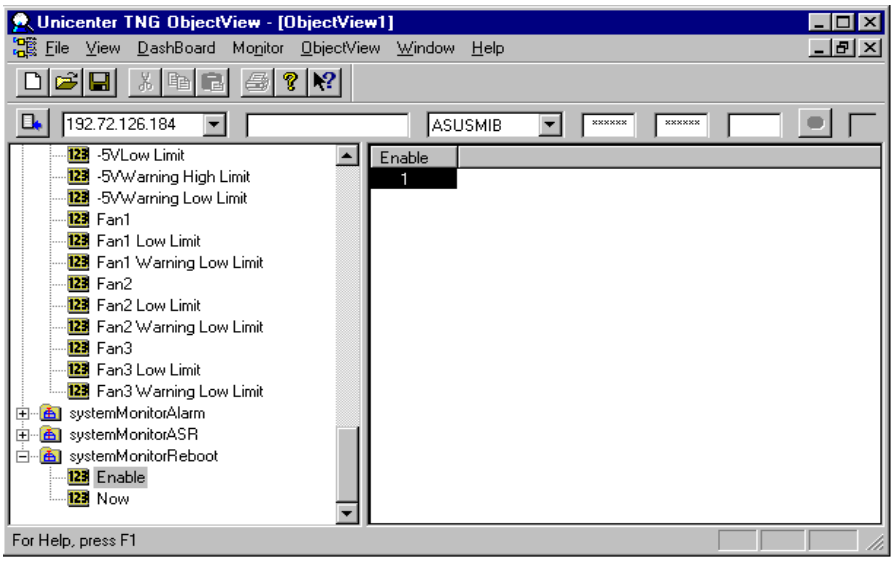


Step 3: Click the ASUSMIB in included box and fill in the name in Model Name. Than click the RUN MOSY tab.



Step 4: Return to the screen of CA-ObjectView Schema Builder and click the Complier.

Step 5: Choose the ObjectView and fill in the IP address and ASUSMIB.
Monitor the System Temperature from ASMA



Step 6: Monitor the value of Reboot Management System