

Contents

Introduction	1
Features	3
 1 Getting started	 7
Welcome	9
Features	10
System requirements	12
ASM Pro Console	12
ASM Pro Server Agent	12
System setup	13
Installing ASM Pro Console	13
Installing ASM Pro Server Agent	13
Installing the Novell NetWare Server Agent	14
Installing the SCO OpenServer Agent	15
Installing the SCO UnixWare Server Agent	16
Installing the Microsoft Windows NT V4.0 Server or Windows 2000 Server/Advanced Server Agent	18
Installing the RedHat Linux Server Agent	19
 2 Quick tour	 21
ASM Pro console	23
Understanding system listing	24
Customizing system listing	26
User interface (UI) tab	27
Warning tab	28
Configuring polling interval	28
System alert manager	30
Assigning event handler	32
Event viewer	35
Remote console	38
Asset manager	40
CMOS setup manager	44
BIOS flash manager	46
 3 ASM Pro Console	 49
Launching ASM Pro Console	51
Initializing and changing the password	51

ASM Pro Console user interface	53
Menu bar and toolbar	53
Using Auto Discovery to add a system to the	
System Listing	60
Auto Discovery Commands	61
Adding a system from Auto Discovery to System	
Listing	61
Specifying options	63
Manually adding a system	64
Removing a system from the list	64
Working with System Listing	65
System organizer	67
System symbols	67
Customizing System Listing	68
User interface (UI) tab	68
Warning tab	69
System information and performance monitoring	70
System information	70
Basic information	70
DMI BIOS information	72
Input/Output device information	78
Storage information	79
Operating system information	81
Network information	87
System resource information	88
Performance monitoring	92
Configuring polling interval	92
Processor performance (for server system)	92
Kernel performance (for desktop system)	93
Memory utilization	94
Disk utilization (for server systems only)	96
File system utilization	98
NIC (Network Interface Card) utilization	
(for server system only)	98
Hardware status	100
Health monitor	100
IPMI (Intelligent Platform Management Interface)	103
MIB-II information	107
System	107
Interface	108
AT (Address Translation)	112
IP (Internet Protocol)	112
ICMP (Internet Control Message Protocol)	115
TCP (Transmission Control Protocol)	117

UDP (User Datagram Protocol)	120
SNMP (Simple Network Management Protocol)	121
Redundant power supply	124
Fault management	125
Threshold settings	125
Hardware errors	127
 4 System Alert Manager (SAM)	 131
SAM user interface	133
Viewing system alert	135
SNMP traps	135
Trap types for server systems	137
DMI indications	138
DMI indication types	140
Alert via LAN (Local Area Network)	140
AVL alert types	141
Saving and loading system alert log files	142
Event viewer	143
Saving and loading event log file	143
Retrieving multiple event log information	143
Displaying single event log information	144
Event types	144
Event handler setup	148
Event handling method	149
Console side action	150
Page setup for printing	153
 5 ASM Pro Server Agent utilities	 155
asmconfig for SCO OpenServer	158
SNMP config	158
Manager information	159
Event action	160
Password	161
Threshold	161
Event log	162
Quit	163
asmcfg for SCO UnixWare	165
Config > SNMP	165
Config > ASM Pro_Password	166
Config > Manager_Info	167
Config > Threshold	167
Config > Event_Actions	168
asmcfg for Windows NT	169

SNMP Config	169
Manager information	170
Server information	170
Event action	171
Event log	172
Password	172
Saving changes in asmcfg	173
asmcfg for NetWare	175
Password	175
Out of band	177
Manager information	177
Server location	178
Event handling	178
Trap target	179
Saving changes in asmcfg	181
Uninstalling ASM Pro server agent	182
asmcfg for Linux	183
SNMP_Config	183
Manager information	184
Event action	185
Password	186
Threshold	187
Event log	188
Quit	189
 6 ASM Pro Local Console	 193
Basic system information	195
Physical and partition information	196
Accessing physical storage device information	196
LAN adapter, TCP/IP, and modem setting	198
LAN (Local Area Network)	198
TCP/IP (Transmission Control Protocol/ Internet Protocol)	199
Modem	199
System performance information	200
CPU utilization	200
Virtual memory manager	201
Swap file	201
File system	201
System health status	203
Fan	203
Temperature	203
Voltage	204

CPU, memory, and onboard chips	205
Processor	205
Memory	206
Onboard device	206
System resource	207
I/O device information	208
System event log	208
 7 ASM Pro MIB Browser	 211
Installing ASM Pro MIB Browser	213
User interface	214
Menu bar and toolbar	214
MIB tree window	219
MIB tree	219
Selection window	220
Description window	220
Status bar	220
Functions	221
Selecting browsing systems	221
Auto Discovery dialog box items	222
Setting up browsing options	223
Configure timer dialog box items	224
Configuring community and port	224
Defining a new query	225
Selecting a query	226
Select query dialog box items	226
Managing the database	227
Initializing the database	227
Adding a new MIB	228
Removing a MIB	229
Adding an OID	229
Removing an OID	229
Removing all OIDs	229
Browsing OIDs (SNMP table)	229
SNMP table (Simple Network Management Protocol)	230
Set operation	231
Decimal or hexadecimal	231
Activating the log file	232
Enumeration display	232
Setting the time interval for polling	233
Rotating the SNMP table	233
Finding OIDs in the SNMP table	233

Taking a walk through the MIB	233
Walk operation window	234
Finding an OID	235
Saving information	236
 8 ASM Pro MIF Browser	 237
Installing ASM Pro MIF Browser	239
User interface	240
Menu bar, toolbar, and system list box	240
MIF tree window	243
Information window	244
Query window	244
Status bar	244
Functions	245
Selecting browsing systems	245
Manually adding a system	246
Sweeping subnets	247
Starting a new connection	247
Setting up browsing and default connection options	248
Browsing the DMI table	250
Changing table Attribute Value	250
Viewing table document properties	251
Defining a new query	252
Selecting a query	253
 9 Asset Manager	 255
Introduction	257
Asset Manager user interface	258
Menu bar and toolbar	258
System list combo box	260
Auto Discovery	260
Auto Discovery dialog box items	260
Asset control	262
Updating hardware and software information	263
Asset statistics information	264
Asset information query	266
Asset log	267
Asset history	269
Viewing and comparing different log versions	269
 10 Statistics Viewer	 271
Adding Statistics Viewer to your system	273

Statistics Viewer user interface	274
Viewing statistical information	276
Recording utilization information	276
Saving and loading query files	279
Working with statistics graph view	280
 11 Alert via LAN	 283
Alert via LAN Manager function	285
Menu bar and toolbar	285
Information tab	287
Network tab	288
Timers tab	289
Alerts tab	290
Saving the Alert via LAN Manager settings	291
Alert via LAN local function	292
Information tab	292
Network tab	293
Timers tab	294
Alerts tab	294
Updating the onscreen information	295
Quitting alert via LAN agent	295
Getting help information	295
 12 Remote Console	 297
Remote Console administrator function	299
Menu bar and toolbar	300
Establishing a connection to an ASM Pro server system	301
File transfer function	302
Disconnecting from an existing remote console connection	303
Remote console server function	304
Menu bar	304
Setting a password	305
User setting	306
Chatting	308
 13 CMOS Setup Manager and BIOS Update Manager	 311
CMOS Setup Manager	313
Menu commands	314
Installation and uninstallation	315
Selecting browsing systems	315

Auto Discovery dialog box items	316
Basic operations	317
Advanced operations	320
BIOS Update Manager	322
Menu commands	322
Installation and uninstallation	323
Selecting browsing systems	323
Auto Discovery dialog box items	324
Basic operations	326
Update operations	326
 14 Remote Diagnostic Manager (RDM)	 331
Overview	333
RDM architecture	333
ASM Pro Server Agent	333
RDM Console	334
RDM connectivity	334
RDM features	334
Remote management features	334
RDM Console features	335
RDM installation	336
System requirements	336
RDM server requirements	336
RDM Console requirements	336
Connecting communication peripherals	337
Installing RDM Utilities	337
RDM Console setup	340
Installing the RDM Console software	340
Uninstalling the RDM Console software	341
Configuring the RDM functions in server	342
RDM operation modes	342
RDM local mode	342
RDM remote mode	342
RDM runtime mode	342
RDM BIOS	343
Entering the RDM BIOS	343
RDM 4.5 BIOS version	344
Console redirection	344
Hidden partition	344
Communication protocol	345
COM port baud rate	345
Remote Console phone number	345
Dial out retry times	346

Modem initial command	346
RDM work mode	346
Waiting mode password	347
Paging	347
System critical paging numbers	348
Paging times	348
Setting RDM operation modes	349
RDM local mode	349
RDM remote mode	349
RDM runtime mode	351
Using the RDM Console	355
Running the RDM ConsoleRDM Console	355
Starting the RDM Console	355
Connecting to the RDM server	355
EMP (emergency management port) console	356
EMP console buttons	357
EMP console functions	359
RDM reboot options	360
RDM Console options	362
RDM Console utility	362
RDM Console utility menus	363
RDM Console toolbar buttons	365
RDM Console functions	366
Viewing a snapshot file	366
Clearing the screen	367
Saving a log file	367
Disabling the saving log file function	368
Configuring RDM Console settings	368
Setting the font properties	369
Creating a new ASM Pro Server Agent	370
Sending files	372
Receiving files	374
Refreshing the screen	375
Rebooting the server	375
SCO OpenServer, UnixWare and	
Internet FastStart Installation	377
SCO OpenServer 5	377
SCO UnixWare	377
SCO Internet FastStart	378
Troubleshooting	380
ASM Pro Server Agent troubleshooting	380
RDM Console manager troubleshooting	380
Modem troubleshooting	381
Hidden partition troubleshooting	381

BIOS messages	381
15 ASM Pro Web-based Manager	385
Installing AWM and Microsoft Internet Information Service (IIS)	387
System requirements	387
Setting up Microsoft IIS	387
Installing AWM	388
Running AWM	389
AWM user interface	391
Deleting a device from the system listing	393
Auto Discovery	394
Using Auto Discovery to add a network device	394
Adding a device to the system listing	395
Management pages	396
ASM Pro Management Pages	396
Basic System Information	396
O.S. information	399
DMI BIOS Information	405
I/O device information	412
Network information	413
System resource information	414
Resource	417
Performance	420
Processor performance	420
Memory utilization	422
Storage utilization	423
System Hardware	423
IPMI information	423
IPMI Sensor	424
System event log	425
FUR product	426
FUR board	427
FUR chassis	428
MIB-II configuration information	428
System information	429
Interface	430
AT (Address Translation)	433
IP (Internet Protocol) group	434
ICMP (Internet Control Message Protocol)	437
TCP (Transmission Control Protocol)	439
UDP (User Datagram Protocol)	442
SNMP (Simple Network Management Protocol)	444
Configuring event handler	446

Event actions	448
Real time monitoring	449
 A Troubleshooting	 441
General ASM Pro troubleshooting	443
ASM Pro agent for SCO OpenServer troubleshooting	449
ASMSMUXD	449
ASMCONFIG	452
BPBSMUXD	452
BPBCONFIG	452
IPMSMUXD	453
ASM Pro Agent for SCO UnixWare troubleshooting	454
ASMSMUXD	454
ASMCFG	455
BPBSMUXD	456
IPMSMUXD	457
XASMMON	457
ASM Pro Windows NT troubleshooting	459
Hardware common part troubleshooting	468
 B RAID utilities	 471
ASM Pro Mylex RAID utility	473
Mylex RAID controller monitor	473
Controller tab	473
Disk tab	473
Controller statistic tab	474
Disk statistic tab	475
Physical disk statistic graph tab	475
Logical disk statistic graph tab	476
ASM Pro DPT RAID utility	477
HBA (Host Bus Adapter) tab	477
Bus tab	479
Device tab	480
Array tab	482
Statistic tab	484
Graph tab	485
 C ASM Pro Adaptec CI/O utility	 505
Adaptec CI/O monitor window	507
Controller tab	507
Device tab	509
Bus port tab	511

Volume tab	512
Statistic tab	513
D Management system snap-in modules	515
CA Unicenter TNG	517
HP OpenView	519
MMC (Microsoft Management Console)	520

Advanced System Manager Pro
(ASM Pro) version 4.5
User's guide

Copyright © 2001 Acer Incorporated
All Rights Reserved.

Advanced System Manager Pro
(ASM Pro) version 4.5

User's guide

Changes may be made periodically to the information in this publication without obligation to notify any person of such revision or changes. Such changes will be incorporated in new editions of this manual or supplementary documents and publications. This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims the implied warranties of merchantability or fitness for a particular purpose.

Record the model number, serial number, purchase date, and place of purchase information in the space provided below. The serial number and model number are recorded on the label affixed to your computer. All correspondence concerning your unit should include the serial number, model number, and purchase information.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without the prior written permission of Acer Incorporated.

Model Number : _____

Serial Number: _____

Purchase Date: _____

Place of Purchase: _____

Acer and the Acer Logo are registered trademarks of Acer Inc. Other company's product names or trademarks are used herein for identification purposes only and belong to their respective companies.

Warranty/Limitation of Liability

Any software described in this manual is licensed “as is” and Acer and its suppliers disclaim any and all warranties, express or implied, including but not limited to any warranty of non-infringement of third party rights, merchantability or fitness for a particular purpose. Acer does not warrant that the operation of the software will be uninterrupted or error free.

Should the programs prove defective, the buyer (and not Acer, its distributor, or its dealer) assumes the entire cost of all necessary service, repair, and any incidental or consequential damages resulting from any defect in the software. Please see the Acer Limited Product Warranty for details of Acer’s limited warranty on hardware products. IN NO EVENT SHALL ACER BE LIABLE FOR ANY INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS OR DATA, EVEN IF ACER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Software License

Acer grants you a personal, non-transferable, non-exclusive license to use the software that accompanies your computer system only on a single computer. You may not (a) make copies of the software except for making one (1) backup copy of the software which will also be subject to this license, (b) reverse engineer, decompile, disassemble, translate or create derivative works based upon the software, (c) export or re-export the software to any person or destination which is not authorized to receive them under the export control laws and regulations of the United States, (d) remove or alter in any way the copyright notices, or other proprietary legends that were on the software as delivered to you or (e) sublicense or otherwise make the software available to third parties. The software is the property of Acer or Acer’s supplier and you do not have and shall not gain any proprietary interest in the software (including any modifications or copies made by or for you) or any related intellectual property rights. Additional restrictions may apply to certain software titles. Please refer to any software licenses that accompany such software for details.

Join Us to Fight Against Piracy

The Acer Group has been implementing a policy to respect and protect legitimate intellectual property rights. Acer firmly believes that only when

each and every one of us abides by such policy, can this industry provide quality service to the general public.

Acer has become a member of the Technology Committee of the Pacific Basin Economic Council which is encouraging the protection and enforcement of legitimate intellectual property rights worldwide. Moreover, in order to ensure quality service to all of our customers, Acer includes an operating system in Acer computer systems which is duly licensed by the legitimate proprietors and produced with quality.

Acer commits itself and urges all of its customers to join the fight against intellectual property piracy wherever it may occur. Acer will pursue the enforcement of intellectual property rights and will strive to fight against piracy.

Introduction

A network is made up of computers and network devices that run on different operating systems and communicate with each other within an environment. The network connects servers, workstations, personal computers, and a variety of software and hardware devices like printers and fax machines. To work properly, all of the computers and devices in the network need to be maintained.

Advanced System Manager Pro (ASM Pro) is a network management software that allows you to spot errors or potential system malfunctions in network devices through a single management station. It also allows you to monitor all of the systems and devices on your network without sacrificing efficiency.

Advanced System Manager Pro consists of two elements: a manager console and system agents. The manager console monitors all of the agents in the network. The system agents are the software programs on each of the systems in the network that collect information about the systems and report the information to the manager console.

► Features

The major features of ASM Pro management system include the following:

- **ASM Pro Console**

ASM Pro Console is the manager console where all of the information that is gathered from the system agents is evaluated and assessed, using two protocols: SNMP (Simple Network Management Protocol) or DMI (Desktop Management Interface).

The SNMP and DMI protocols return the information from the system agents to the ASM Pro Console through the Management Information Base (MIB) Object ID get/set requests from the ASM Pro Console.

DMI is an API (Application Programming Interface) that allows system agents to collect information from the instrumentation code supporting MIF (Management Information Format) in the system.

- **System Alert Manager**

System Alert Manager is a utility that runs in the background of your ASM Pro Console system every time you bootup. It monitors network systems for faults and malfunctions and warns you if such an event occurs. This utility also includes an event viewer that allows you to view the event logs of network systems.

- **ASM Pro Server Agent Utilities**

The ASM Pro server agent utilities are configuration utilities that run under SCO OpenServer, SCO Unixware, Windows NT, and NetWare. These utilities allow you to enable or disable password protection, create and change passwords, change event handling options, and create, change or delete IP addresses.

- **ASM Pro MIB Browser (customized version only)**

ASM Pro MIB Browser is an MIB (Management Information Base) file browsing tool included with the ASM Pro package. This tool allows you to view and modify the OID (Object ID) values of the systems you are managing on your network. It also allows you to define and maintain a list of OIDs to view.

- **ASM Pro MIF Browser (customized version only)**

ASM Pro MIF Browser is an MIF (Management Information Format) file browsing tool included with the ASM Pro package. This tool is used to describe a hardware or software component of a system. MIF

files are used by DMI (Desktop Management Interface) to report system configuration information to the Console.

- **Asset Manager**

Asset Manager gathers information about the hardware and software configuration of each system being monitored by the ASM Pro Console, and saves this information in an asset log file for future reference.

Asset Manager consists of four parts:

- Asset Control - shows you the hardware and software configuration of the system currently being monitored.
- Asset Statistics Information - summarizes the hardware information contents of two or more systems.
- Asset Log - Displays the asset log and saves it to disk.
- Asset History - Shows a comparison of two or more asset log versions of a system.

- **Statistic Viewer (customized version only)**

Statistics Viewer records and displays system utilization information about monitored systems. This information can then be saved for future reference.

- **Alert via LAN**

The Alert via LAN (Land Area Network) function of ASM Pro enables administrators to easily monitor and reconfigure local systems via a network.

- **Remote Console**

The Remote Console function of ADM allows the administrator to remotely control the local systems connected to the LAN via the server, if access is granted.

- **CMOS Setup Manager**

CMOS Setup Manager is one of the ASM Pro utility programs used to change the CMOS settings remotely. With this remote capability, you do not need to visit the machine physically to change the CMOS settings for some abnormal system configuration. This program is not intended to replace the common CMOS setup function provided by all BIOS vendors, but for convenience under Windows environments, including Windows 9x and Windows NT systems. This feature requires proper hardware support.

- **BIOS Update Manager**

BIOS Update Manager updates the BIOS remotely. With such remote capability, administrators do not need to visit the machines physically to upgrade their system BIOS. Administrators can also schedule the upgrade in advance, and the BIOS Update Manager will perform the task at the scheduled time. This feature requires proper hardware support.

1 Getting started

Advanced System Manager Pro (ASM Pro) is a network system management tool designed to assist you in monitoring performance, managing assets, and detecting errors or potential system malfunctions in network systems.

► Welcome

The ASM Pro package consists of the following software components:

- ASM Pro Console

ASM Pro Console is installed on the monitoring station and collects the server information provided by the ASM Pro Server.

ASM Pro Console supports systems running on Windows 98, Windows NT, or Windows 2000.

- ASM Pro Server Agent

ASM Pro Server Agent is installed on the network servers that are monitored by the ASM Pro Console.

ASM Pro Server Agent supports systems running on Windows NT Server, Windows 2000, Novell Netware, SCO Openserver, SCO Unixware, or Red Hat Linux.

► Features

The basic features of ASM Pro are as follows:

- **System Information** - helps you locate the systems in your network and collects general information about your systems like operating system, protocols, addresses, etc.
- **Configuration Information** - shows the configuration of hardware devices (i.e. BIOS, I/O ports, hard disks, network interface cards, etc.) and software installed in each system in your network.
- **Performance Monitoring** - displays utilization information of system resources like read/write usage, network packets, memory, and the central processing unit, and shows whether these resources exceed their allowable threshold value.
- **Fault Management** - checks the systems for hardware errors and to see if a system resource has exceeded its threshold value. When the threshold is exceeded, the program notifies the system administrator. When a hardware error occurs, it can be set to shut down the system to protect it from further damage.

ASM Pro also provides a number of utilities to help you view information and manage your network systems:

- **System Alert Manager (SAM)** - runs in the background of your system and warns you immediately of any abnormal events. You can use it to trace system failures and malfunctions.
- **ASM Pro MIB Browser** - checks the network for all available MIB (Management Information Base) defined systems. It can also build a user-defined browsing object database to view the information for each system.
- **ASM Pro MIF Browser** - checks the network for all available MIF (Management Information Format) defined systems. It can also build a user-defined browsing object database to view the information for each system.
- **Asset Manager** - monitors systems for any hardware component changes and logs them into a database for future reference.
- **Statistic Viewer** - monitors systems use and logs them into a database for future reference. You can use it to identify and reduce bottlenecks occurring in your network and servers.

In addition to these features, ASM Pro also supports the following Add-on¹ and Snap-in* modules:

- Mylex GAM Agent -
- CA Unicenter - This module creates classes and objects in the repository of Unicenter TNG. The ASM Pro Agent object is created automatically when a new host is added into the repository (manually added or by auto discovery).
- HP OpenView -

For specific information about these add-on and snap-in module items, please refer to their user's guide.

¹ See Appendix D for further information.

► System requirements

ASM Pro Console

- Intel Pentium or higher processor
- 64MB of RAM (128MB recommended)
- 20MB free hard disk space
- Microsoft Windows 98, Windows NT, or Windows 2000 operating system
- Ethernet card
- Modem

ASM Pro Server Agent

- Intel Pentium or higher processor
- 64MB of RAM (128MB recommended)
- 20MB free hard disk space
- Novell NetWare, SCO OpenServer, SCO UnixWare, Linux RedHat, Microsoft Windows NT, or Windows 2000 operating system
- Ethernet card
- Modem (optional for RAS/OOB²)

² RAS (Remote Access Services) and OOB (Out-of-Band)

► System setup

Make sure that your computer meets the system requirements before proceeding. You may also want to change your screen to 800 x 600 resolution or higher for optimum viewing.

Installing ASM Pro Console

To install ASM Pro Console:

1. Insert the Management CD into the CD-ROM drive on your system.
2. Click **Applications** button.
3. In Applications lists, select **Advanced System Manager(ASM) Pro Console V4.5**.
4. Click **Setup** button.
5. Follow the installation wizard.
6. click **Finish** to complete the installation.



.....

Remember to remove all diskettes or CDs from the drives before rebooting the system.

Installing ASM Pro Server Agent

ASM Pro Server Agent can be installed on four different operating systems. The installation diskette contains the installation files for the following operating systems:

- Novell NetWare 5.x
- SCO OpenServer 5.0x
- SCO Unixware 7.x
- Microsoft Windows NT 4.0 Server
- Linux RedHat 6.2,7.1
- Microsoft Windows 2000 (Server and Advanced Server with SP1)

Installing the Novell NetWare Server Agent



Make sure the SNMP (Simple Network Management Protocol) is configured properly.

ASM Pro Server Agent requires SNMP.NLM running with *Control Community set to 'public'*, to allow ASM Pro Console to communicate with ASM Pro Server Agent.

ASMAGENT.NCF is the script file that loads all related modules of ASM Pro Server Agent. To load the SNMP use the following command:

```
load snmp control=public
```

If you load SNMP.NLM before ASM Pro Server Agent, make sure that the Control Community has been set up properly. For more information, please refer to related documents about the SNMP Agent for NetWare (NetWare SNMP).

Check AUTOEXEC.NCF to see if you have loaded SNMP. Notice that because of the auto loading feature of NLM, you can not directly find where SNMP is loaded. The most common module is TCPIP.NLM which auto loads SNMP.NLM. If you are using TCP/IP, load SNMP by using the command line *load snmp control=public* before loading TCPIP.

For NetWare 4.x and Netware 5.x users, if you are using INETCFG.NLM to configure the network, be sure to configure SNMP and make sure that the SNMP.NLM is running with *Control Community set to 'public'*.

To install the Novell NetWare Server Agent:

1. Insert the Management CD into the CD-ROM drive on your system.
2. At Netware server console, type:

```
load cdrom.
```
3. At Netware server console,type:

```
load EB450MgmtCD:\APP\ASM\Netware\setup.
```
4. You are asked if you want to install the ASM Pro Server Agent on your system. Select **Yes** to install.

The setup program detects the NetWare version and the model of the server. It copies related NLM files into the SYS: SYSTEM directory and C: of your NetWare server, and some needed command lines are added into AUTOEXEC.NCF in SYS: SYSTEM.

5. If the Mylex GAM driver and GAM service is installed in your NetWare system, the setup program asks you to install the Bbp agent.
6. Press any key to continue. The ASM Pro Server Agent Configuration Utility is launched.
7. The **Password** option is highlighted. Set up a password, and exit the utility.



.....

A password is required when using the ASM Pro Console to remotely change or set any values for the agent, such as threshold values and any trap handling method. If the password is disabled, there is no security protection for the agent when the Console tries to change or set these values.

8. Reboot the system to activate the ASM Pro drivers.



.....

ASM Pro Server Agent automatically starts after the server is restarted and running.

Installing the SCO OpenServer Agent



.....

Make sure the SNMP (Simple Network Management Protocol) is configured properly.

ASM Pro Server Agent requires SNMP running with *community set to 'public'*. The IP address of ASM Pro Console should be in */etc/snmpd.trap* so that ASM Pro Console can communicate with ASM Pro Server Agent.

Follow these steps to install the SCO Server Agent:

1. Insert the Management CD into the CD-ROM drive on your system.
2. Login SCO OpenServer as a super user.
3. In shell prompt, type following to mount CD-ROM:

 `mount /dev/cd0 /mnt/cd.`
4. In shell prompt, type:

 `ln -s /mnt/cd/APP/ASM/SCOPE~1/ASMIPMI.DD /tmp/OL.000.000.`
5. In shell prompt, type:

 `custom.`

6. Follows custom command UI, select **Software** -> **Install New** -> **From ...** -> **Media Images** -> **/tmp**.



.....

If the SCO Server Agent has been installed, the program asks if you want to preserve the existing config file. Choose Reinstall to overwrite the previously installed SCO Server Agent, or choose Upgrade if you know the existing password.

7. A password is required for a new installation. The system prompts you to enter a new password, and after you have entered it once, prompts you to reenter it.
8. After you set up the password, select the **SNMP_Config** option, and enter the IP address of the ASM Pro Console system. (You can run `asmconfig` at a later time to add or change the ASM Pro Console IP address. See the ASM Pro Server Agent Utilities chapter in the ASM Pro manual for information about running `asmconfig`.)



.....

If the SCO Server Agent has been installed, target IP addresses appear on this screen.

9. After installation complete, in shell prompt, type:

```
rm /tmp/VOL.000.000.
```

Configuring ASM Pro Server Agent for SCO OpenServer

You may disable the password if you are installing ASM Pro Server Agent to use only UPS (Uninterruptible Power Supply) or RDM functions.

You can use the `asmconfig` utility to set up a password for the agent. A password is required when you are using ASM Pro Console to remotely change or set any values for the agent.

Refer to the ASM Pro Server Agent Utilities chapter in the ASM Pro manual for instructions on how to use the `asmconfig` utility.

Installing the SCO UnixWare Server Agent



.....

All of the following procedures require root permission.

To install the SCO UnixWare Server Agent:

1. Make the ASM Pro installation diskette from the DD file on the ASM Pro package CD-ROM.
2. Mount the CD-ROM drive. For example, mount the CD-ROM to /mnt.
3. Insert an empty 1.44MB diskette into your floppy drive and execute the command:

```
# dd if={PATH}/asmuw.dd of=/dev/rdisk/f03ht
```

Here, {PATH} denotes the directory where asmuw.dd is located. For example, /mnt/UnixWare.

4. Insert the ASM Pro installation diskette into your floppy drive and, at the shell prompt, execute this command to begin ASM Pro installation:

```
# pkgadd -d diskette1 asm
```

The installation process copies the ASM Pro Server Agent package into the /usr/asm directory, and automatically makes changes to the following system configuration files:

```
/etc/netmgt/snmpd.comm
```

```
/etc/netmgt/snmpd.peers
```

```
/etc/inittab
```

After the installation is complete, ASM Pro Server Agent can be manually started by executing the command:

```
# /usr/asm/asmsmxd
```

or it will automatically be started on the next system reboot.



.....

Before starting ASM Pro SMUX Agent asmsmxd, execute the ASM Pro Agent Configuration Utility asmcfg to configure at least "SNMP", "ASM Pro_Password" and other parameters. Refer to "Chapter 5-ASM Pro Server Agent Utilities" in the ASM Pro manual for detailed instructions on using the ASM Pro Configuration Utility.

Installing the Microsoft Windows NT V4.0 Server or Windows 2000 Server/Advanced Server Agent



Before installing the ASM Pro software, make sure that the TCP/IP and its related SNMP service are installed on the server.

Follow these steps to install the Windows NT agent:

1. Insert the Management CD into the CD-ROM drive on your system, and the CD-ROM will be automatically run to the Management CD UI.
2. Click **Applications** button.
3. In Applications list, select "**Advanced System Manager(ASM) Pro Agent V4.50**".
4. Click **Setup** button.
5. Follow the following installation steps to complete the installation.
6. Verify the path (where the ASM Pro Agent will be installed to) and click **OK**. The Welcome screen appears.
7. Click **Next**. You are asked to stop SNMP service.
8. Click **Yes**. You are prompted to choose a destination directory. If you only want to install ASM Pro SNMP agent and Remote Console, you can choose **Typical**. If you want to choose more components, click **Custom**. There are five components in ASM Pro agent:
 - SNMP agent
 - DMI

ASM Pro agent defines a proprietary ASM Pro.MIF that supports the same items as the SNMP agent.
 - Server Mif

The server.mif that defined by DMTF will be installed.
 - Remote Console

The Remote Console Server is installed which can be remote control by Remote Console Client
 - MMC

This component is only supported on Windows 2000. And it is integrated with Microsoft Management Console.

9. Click **Next**, for the default directory, or click on **Browse** to find your own destination directory. Check any components you want to install, and click OK.

The asmcfg utility launches automatically.

You may skip steps 7 through 11 if you are installing ASM Pro Server Agent solely for the purpose of utilizing UPS and/or RDM functions.

10. Enter a password and click **OK**. A password is required when using the ASM Pro Console to remotely change or set any value for the NT Agent. If the password is disabled, there is no security protection for the agent when the ASM Pro Console tries to change or set these values.
11. Enter the IP address of the ASM Pro Console system, then click **ADD** to add trap destinations. Click **OK** to end the asmcfg utility. This IP address tells the Agent where to report (trap).
12. Click **Yes** to save your changes. The view readme file dialog box appears.
13. Click **Yes** to view, **No** to continue.
14. Click **Finish** to exit setup.

Installing the RedHat Linux Server Agent

Follow these steps to install the Red Hat Linux Agent:

1. Insert the Management CD into the CD-ROM drive on your system.
2. Login Linux server as a super user.
3. In shell prompt, type following to mount CD-ROM:
`mount /dev/hdX /mnt/cdrom.`
4. In shell prompt, type following to change to new directory:
`cd /mnt/cdrom/App/ASM/Linux.`
5. In shell prompt, type following to install ASM Pro SNMP agent:
`/bin/rpm -i asmpro-agent-4.5-4.rh62.i386.rpm.`
6. In shell prompt, type following to configure "SNMP_Config" to receive trap:
`/usr/local/share/asm/asmcfg.`
7. In shell prompt, type following to start ASM Pro agent:

`/usr/local/share/asm/asm-snmpd start.`

8. In shell prompt, type following to stop ASM Pro agent if necessary:

`/usr/local/share/asm/asm-snmpd stop.`

2 Quick tour

This quick tour is a step-by-step tutorial that helps you get started with setting up and customizing ASM Pro Console for your needs.

This tour shows you how to find network systems using the Auto Discovery function, manage them with the System Listing window, customized background graphics, printer fonts, and warning messages, and configure polling intervals.

For a complete reference to the commands and functions of ASM Pro Console, please refer to “Chapter 3 ASM Pro Console” on page 15.

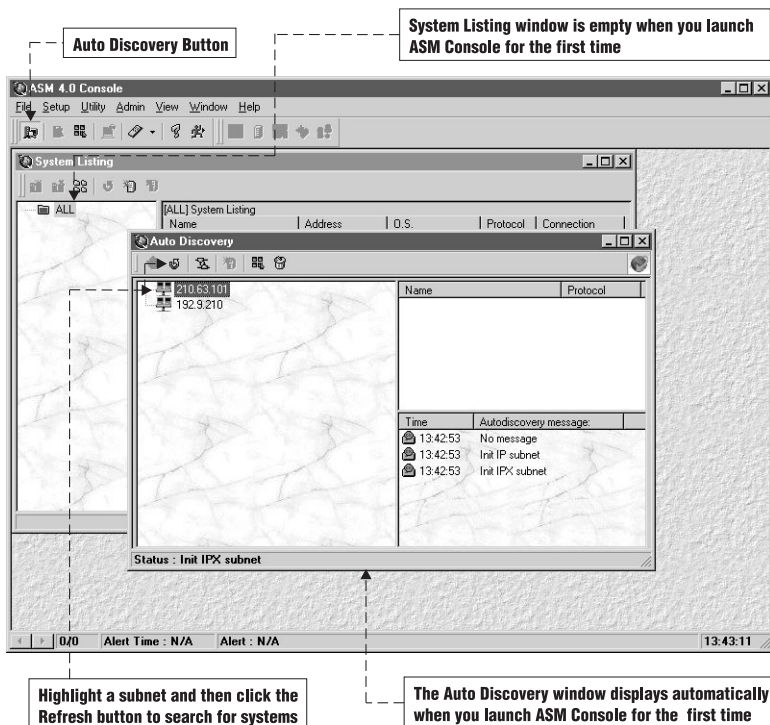
► ASM Pro console

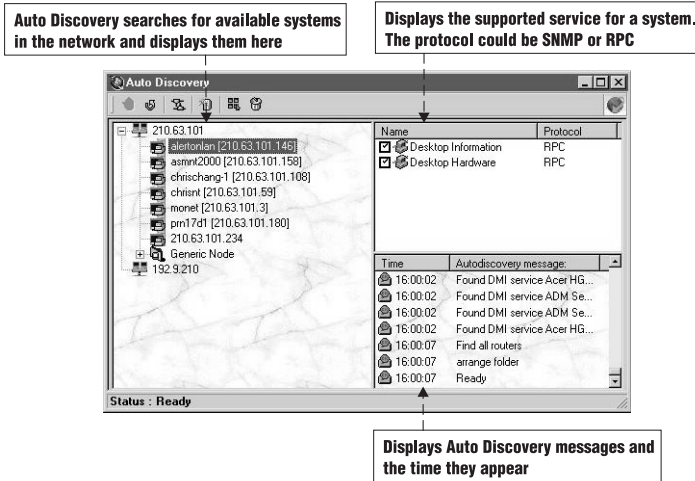
To launch ASM Pro Console, press the **Start** button and then select **Programs > ASM Pro > ASM Pro Console** or you can double-click on the **ASM Pro Console** shortcut icon.

If you are using ASM Pro Console for the first time, it will ask you to initialize a password before continuing.

To initialize a password, enter a password in the **New Password** field, re-type the password in the **Confirm** field, and then click **OK**. From now on, the Log In dialog box will prompt you to enter your password each time you access ASM Pro Console.

After initializing a password, the Auto Discovery window appears:





Understanding system listing

The System Listing window is the main interface of the ASM Pro Console. It is from this window that you will be doing all your work. The System Listing window consists of three panels: System Organizer, All System Listing, and Service panels.

This panel indicates the connection status of the system. It can be:

- connected
- disconnected

The screenshot shows a window titled 'System Listing'. It contains two main tables. The top table, '[ALL] System Listing', lists systems with columns: Name, Address, O.S., Protocol, and Connection. The bottom table lists services with columns: Service, Protocol, State, and Health. Arrows point from descriptive text boxes to specific cells in these tables.

Name	Address	O.S.	Protocol	Connection
V66LA_NTSTD	210.63.103.216	Windows NT	IP	Connected
V66LA	210.63.101.96	Windows 98	IP	Connected
NTSTD	210.63.103.65	Windows NT	IP	Connected
V66LA	210.63.101.253	Windows NT	IP	Disconnected

Service	Protocol	State	Health
Desktop Hardware	RPC	Alive	Normal
Desktop Information	RPC	Alive	Normal

The default services for server system are:

- System Hardware
- System Information

The default services for desktop system are:

- Desktop Hardware
- Desktop Information

This panel indicates the protocol of this service. It can be:

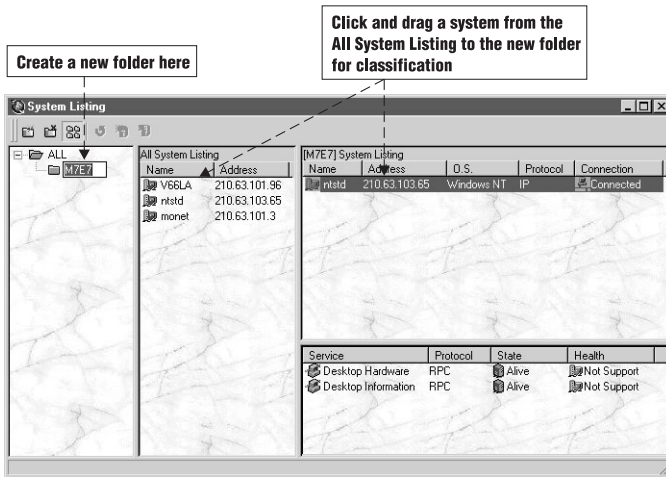
- SNMP for SNMP services
- RPC for DMI Instrumentation code

This panel indicates the health status of this service. It can be:

- Normal
- Abnormal
- Not Supported

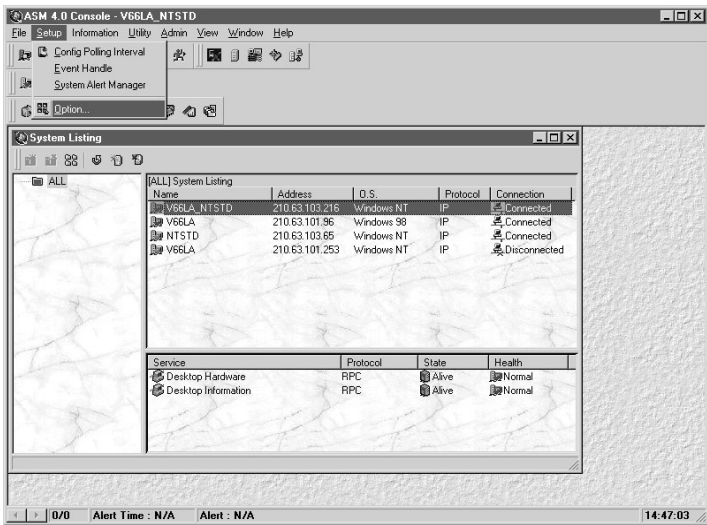
This panel indicates the state of this service. It can be:

- Alive
- Unstable
- Dead



Customizing system listing

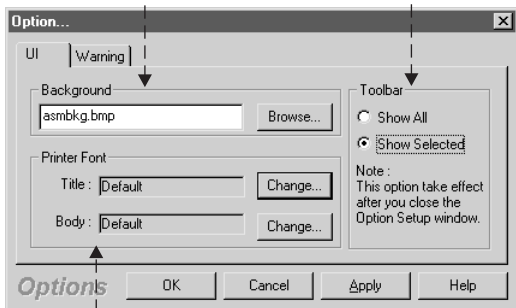
If you get bored looking at the same background graphic or if the fonts you are using now hurts your eyes, you can easily change them to fit your needs. Also, you can set the warning option to warn you before it executes a certain command. To display the Option dialog box, select **Setup > Option.....**



User interface (UI) tab

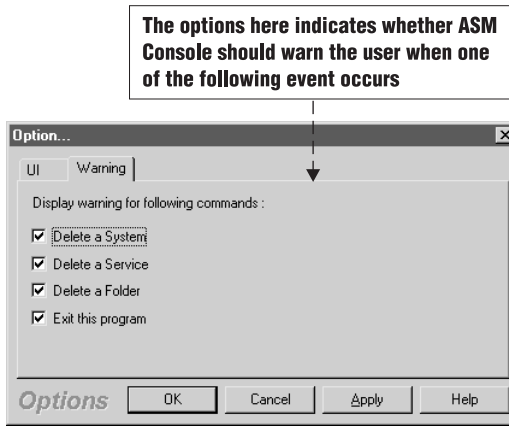
Choose a graphic to change the background display of ASM Console

Gives you an option to display all or selected toolbars for a system or service. The default setting is "Show Selected"



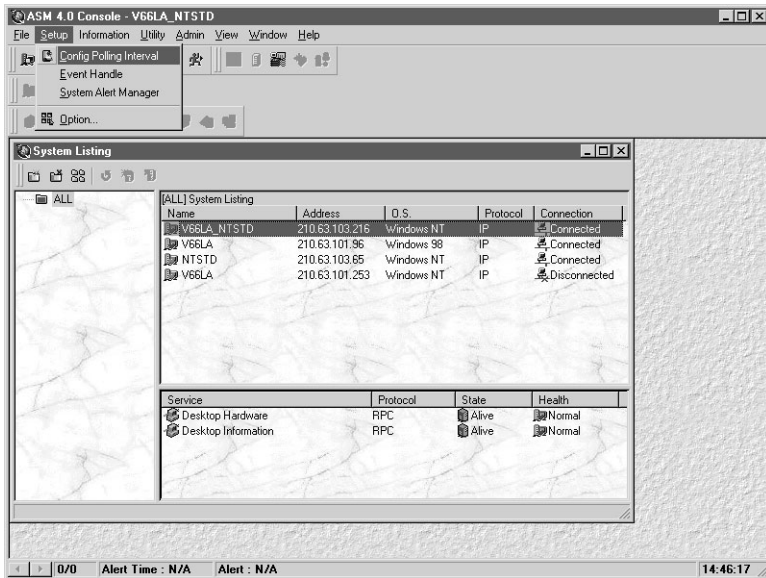
Choose a font for the title and body text of the printed material

Warning tab



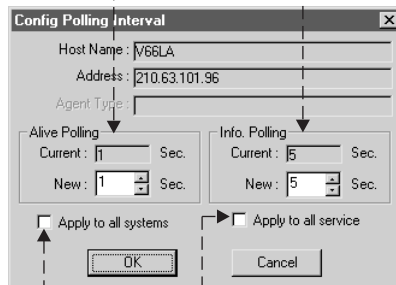
Configuring polling interval

ASM Pro Console polls each monitored system to get information and checks on the systems for faults and malfunctions. You can set the frequency by which the ASM Pro Console do this by stting up the polling interval of each system. To access the polling interval window, select **Setup > Config Polling Interval**.



Alive Polling indicates how often the connection status between the Console and the agent is checked. Polling interval must be from 01 to 60

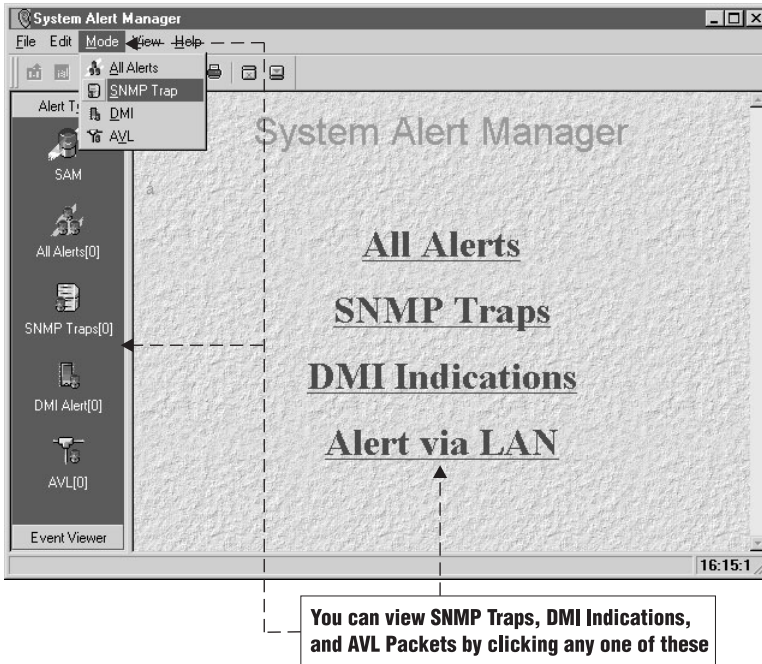
Information Polling determines how frequently the Console polls the Agent to update its data. Polling interval must be from 01 to 60

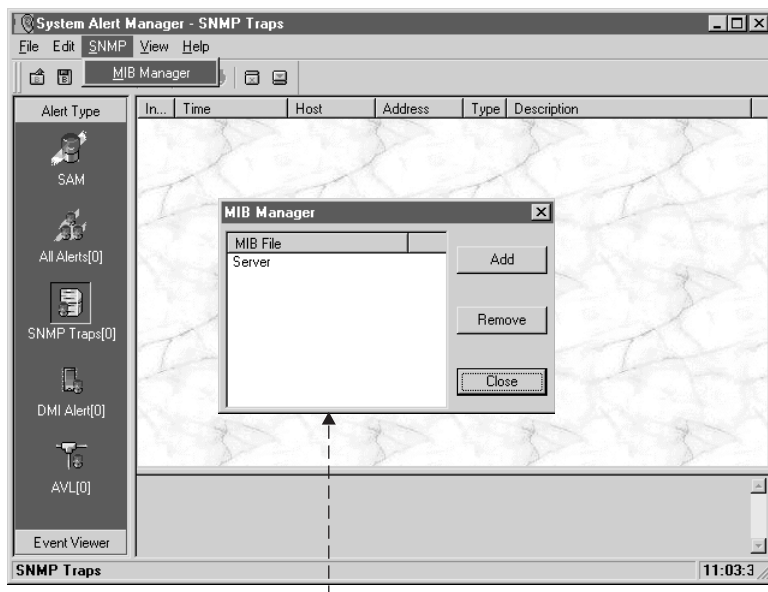


You can set the interval to all systems or to all services

► System alert manager

System Alert Manager is a utility that runs on the background of your Console system every time you bootup. It actively monitors network systems for faults and malfunctions and warns the administrator if such an event occurs. This utility also includes an event viewer that allows you to view event logs of network systems.





SNMP Traps also contains a MIB Manager that allows you to add or remove customized trap definition for SAM. If you have a third party device that supports MIB files, you can add this to the database and configure each trap type

To receive a DMI Indication, you have to register the source system to the service provider. ASM Console will register the machines in the System Listing automatically

Machine Manager

Machine	Address	Status
v66la	210.63.101.96	Registered
	210.63.101.253	Registered

Buttons: << Add, Delete >>, Refresh >>, Manual Add, Register, Unregister, Close

Subnet: 192.9.210

Right Panel Table:

Address	Host Name
192.9.210.27	TEDPANGNT
192.9.210.51	ASMMIT
192.9.210.31	N/A
192.9.210.88	GOLDENLIN
192.9.210.1	MONET
192.9.210.200	N/A

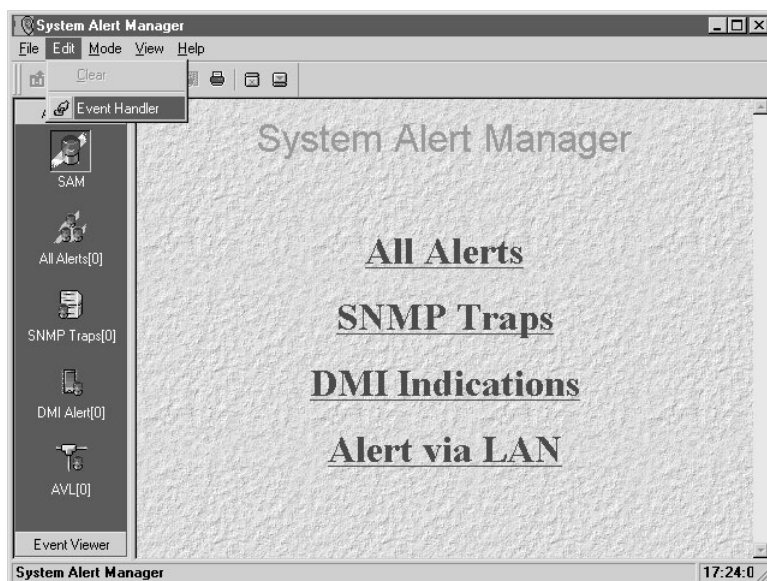
Subnet: 192.9.210 New

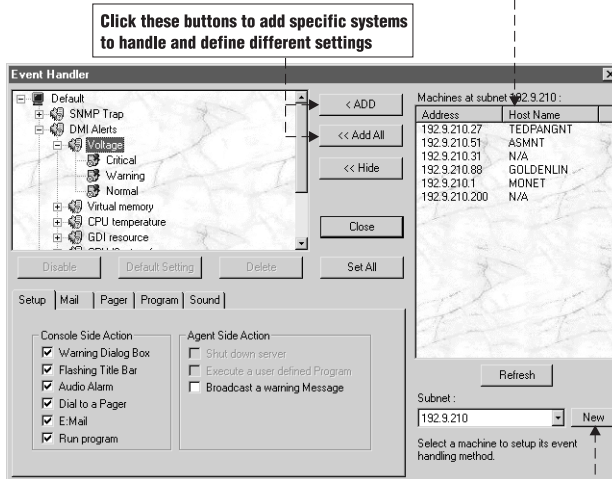
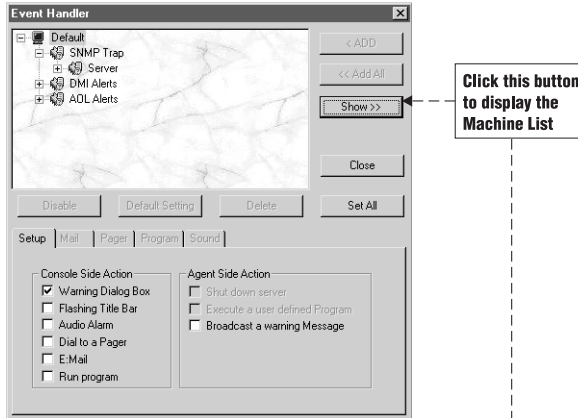
Callout Boxes:

- Click these buttons to Register and Unregister a system respectively
- Click this button to refresh the list and add a new system or click the Manual Add button to add a system
- Click this button to view a new subnet. The systems found in the new subnet will be displayed in the right panel

Assigning event handler

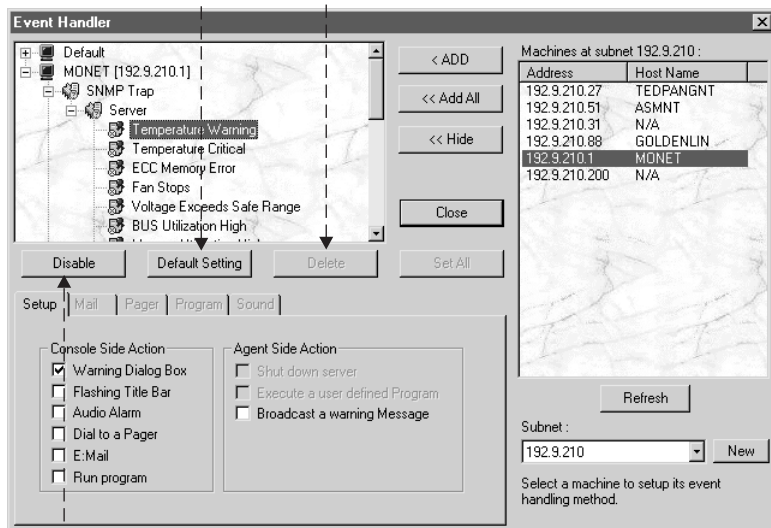
Select **Edit > Event Handler** or click the **Event Handler** button on the menu bar to access the Event Handler screen. Event notification applies to certain systems that you specify.





Click this button to reset the event notification function to the default setting

Click this button to remove the event notification function assignment to the system



Click this button to disable the event notification function assigned to this system forcing it to adopt the default event notification function setting

Event viewer

Event Viewer gathers information about events in the system being monitored by the ASM Pro Console. This information is then saved in the event log file for future reference.



Click here to switch to Event Viewer function

Click this button to view a single event log information

Click this button to view multiple event log information

The screenshot shows the 'System Alert Manager - v66la_ntstd' window. It features a menu bar (File, Edit, Operation, View, Help) and a toolbar. On the left is a sidebar with 'Alert Type' and 'Event Viewer' sections. The 'Event Viewer' section lists several 'v66la' systems, with 'v66la_ntstd [84]' selected. The main area displays a table of events for the selected system, including columns for Server Name, Type, Occuring Time, and Description. Below the event table is a 'Server Listing' table with columns for Server Name, Address, Count, and Percent. To the right of the server listing is a 'Event Statistics' section with a pie chart showing 100.0% for 'v66la_ntstd'. At the bottom left, a label 'v66la_ntstd' points to the selected system in the sidebar. At the bottom right, a label 'Lists the systems found in the System Listing of ASM Console' points to the 'Server Listing' table.

Server Na...	Type	Occuring Time	Description
v66la_ntstd	1006	Wed Jun 09 05:30:13 1999	Fan is not running properly. Please run ASM t...
v66la_ntstd	1006	Wed Jun 09 05:30:15 1999	Fan is running properly.
v66la_ntstd	1003	Fri Jun 11 02:11:32 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1009	Fri Jun 11 07:35:44 1999	Asset items changed. Please run Asset Mana...
v66la_ntstd	1009	Fri Jun 11 07:35:45 1999	Asset items changed. Please run Asset Mana...
v66la_ntstd	1003	Fri Jun 11 10:16:50 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:16:50 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:17:09 1999	Free drive size is in normal condition.
v66la_ntstd	1003	Fri Jun 11 10:17:09 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:17:40 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:17:40 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:17:40 1999	Free drive size is lower than Critical Threshold.
v66la_ntstd	1003	Fri Jun 11 10:17:40 1999	Free drive size is lower than Critical Threshold.
v66la_ntstd	1003	Fri Jun 11 10:18:18 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:18:18 1999	Free drive size is lower than Warning Thresho...
v66la_ntstd	1003	Fri Jun 11 10:18:36 1999	Free drive size is in normal condition.
v66la_ntstd	1003	Fri Jun 11 10:18:36 1999	Free drive size is in normal condition.

Server Name	Address	Count	Percent...
v66la_ntstd	210.63.103.2...	84	100.00

Event Statistics

100.0%

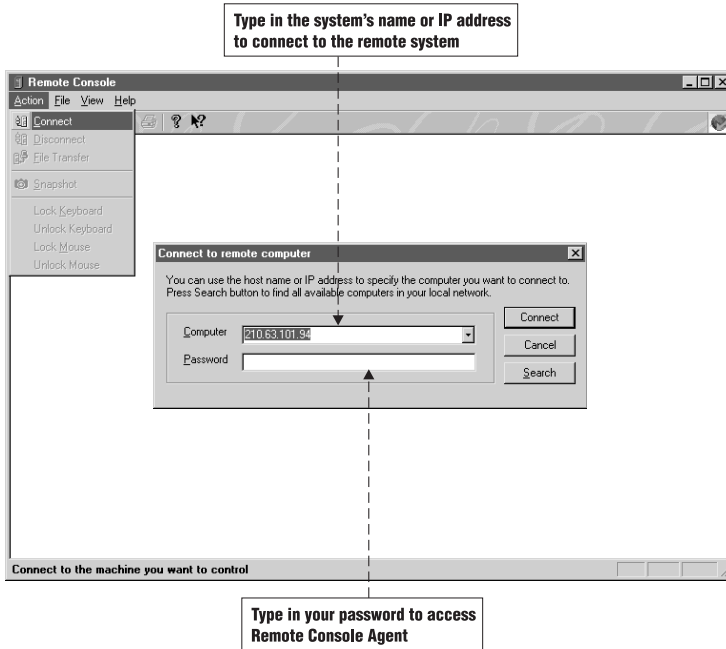
By Server By Type

Pie Bar 2D

11:16:5

► Remote console

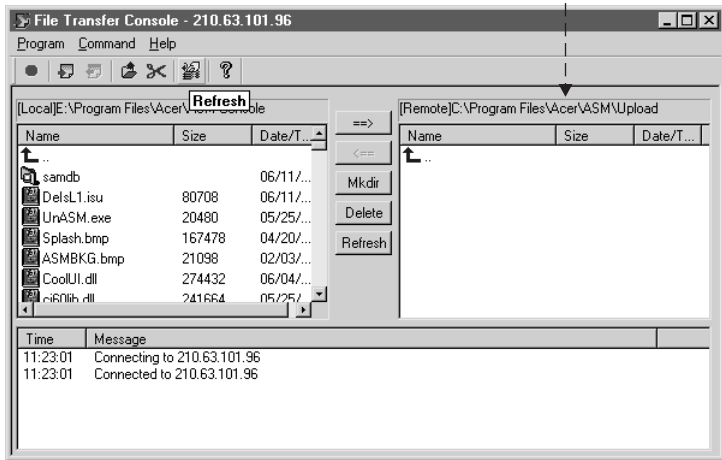
The Remote Console function allows the administrator to remotely control the local systems connected to the LAN via the server, if access is granted.



The File Transfer function allows you to get/put files into a remote system

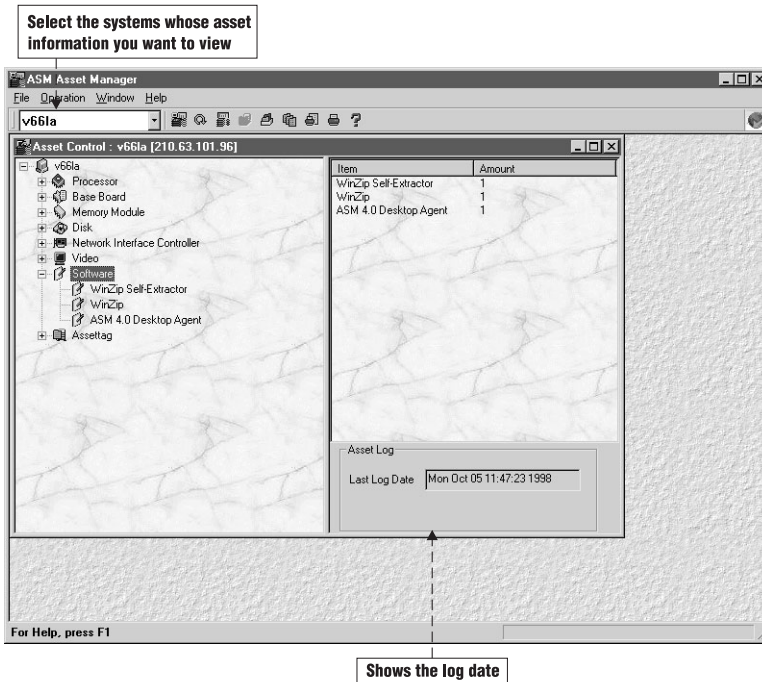


ASM Agent automatically creates a folder called "Upload" in the ASM program folder. You can only access this directory for security control

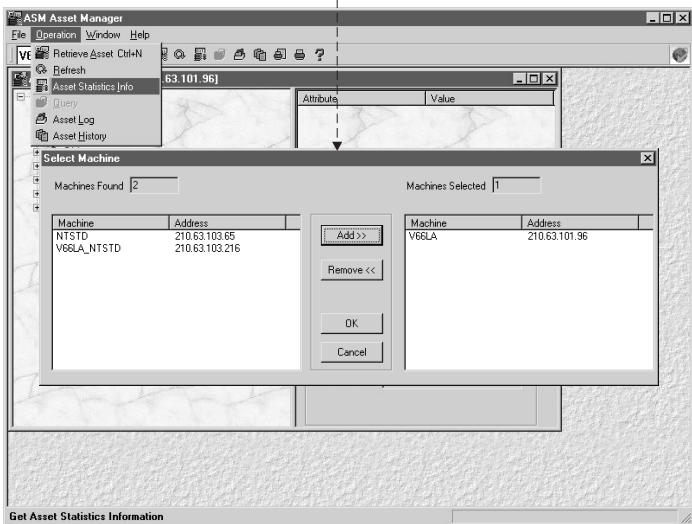


Asset manager

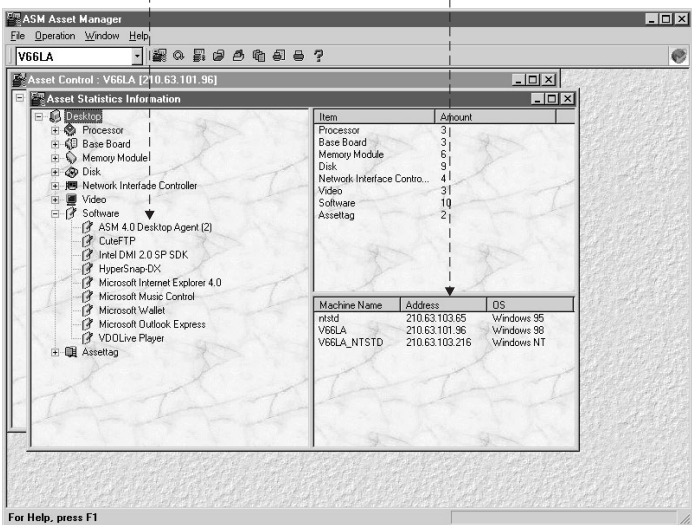
Asset Manager gathers information concerning the hardware and software configuration of each system being monitored by the ASM Pro Console. This information is then saved in an asset log file for future reference.



Select the Asset Statistics Info to collect and view multiple statistical information



This panel displays asset statistical information for three desktop systems displayed in the lower right panel



Systems found by the query is displayed here

Item	Amount
ASM 4.0 Desktop Agent	2
CuteFTP	1
Intel DMI 2.0 SP SDK	1

Item	Amount
Central Processor	1
Central Processor	1

Machine Name	Address	Amount
V68LA	210.63.101.96	1
V68LA_NTSTD	210.63.103.216	1

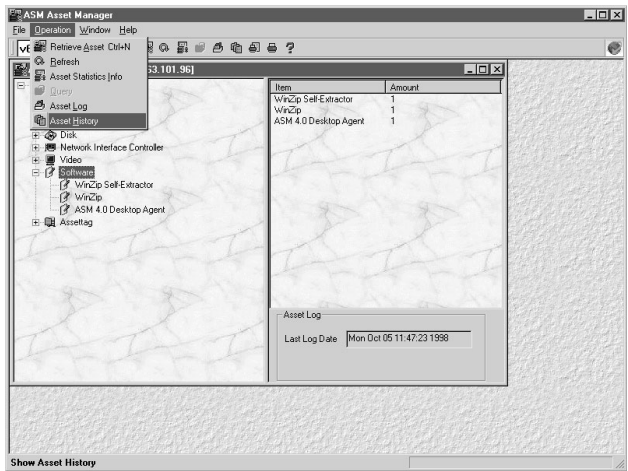
Select the item you want to query

Select any value in this field to find a system

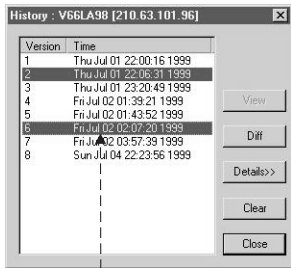
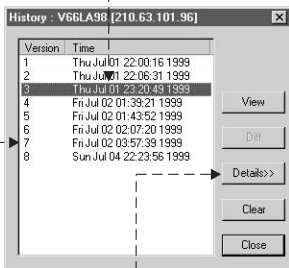
Machine	Item	Model	Description	Time
V68LA	Software	WinZip	0 -> 1	Thu Oct 08 13:44:00 1998
V68LA	Software	ASM Console ...	0 -> 1	Thu Oct 08 13:44:00 1998

Click here to save asset log to a text file

Click here to clear asset log

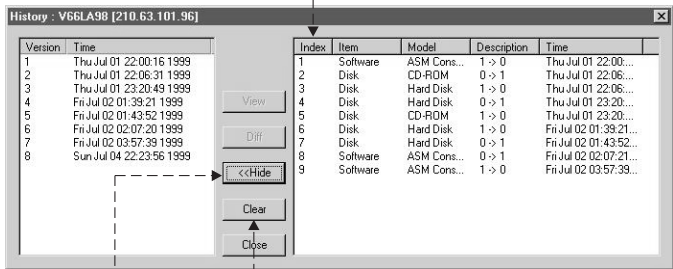


You can view old asset information



Click Details>> to view history log

Or compare the difference between two log versions

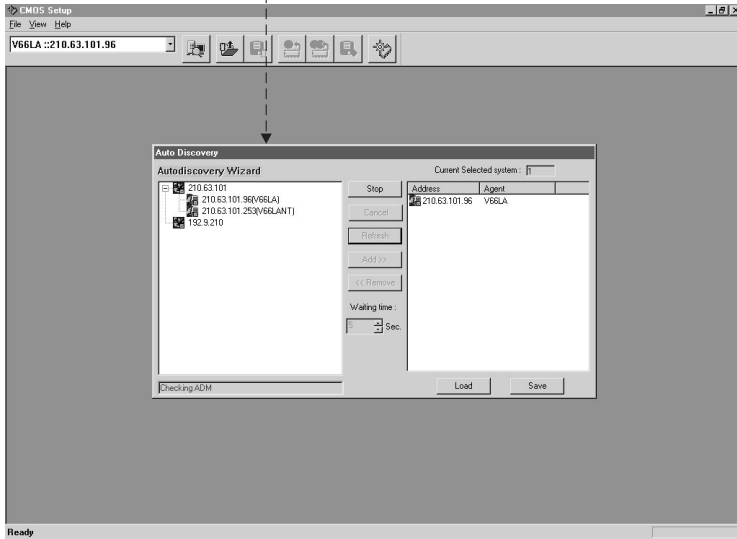


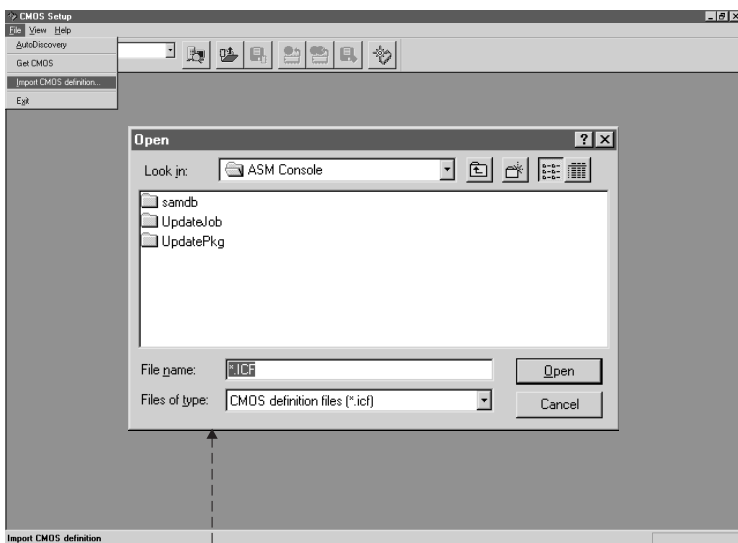
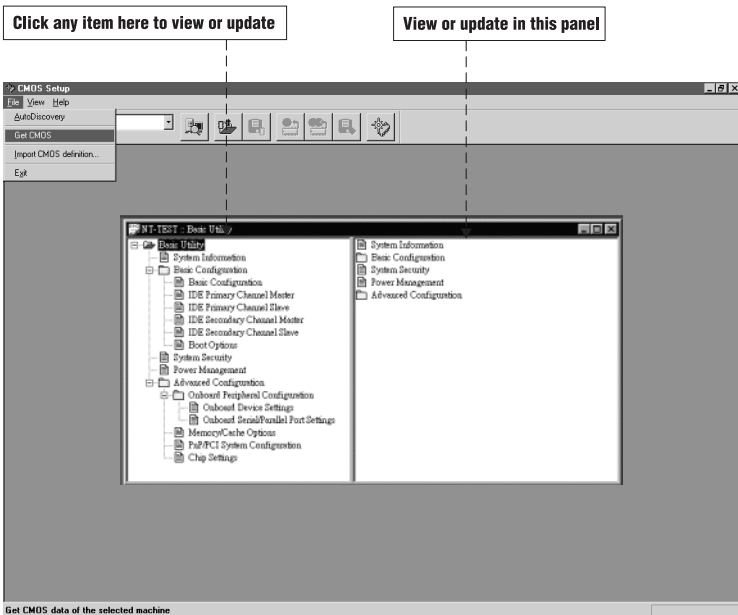
Click <<Hide to hide the history log

Clears all asset histories. This command should have a prior permission set in the agent system

► CMOS setup manager

The Auto Discovery function helps you locate systems in the network

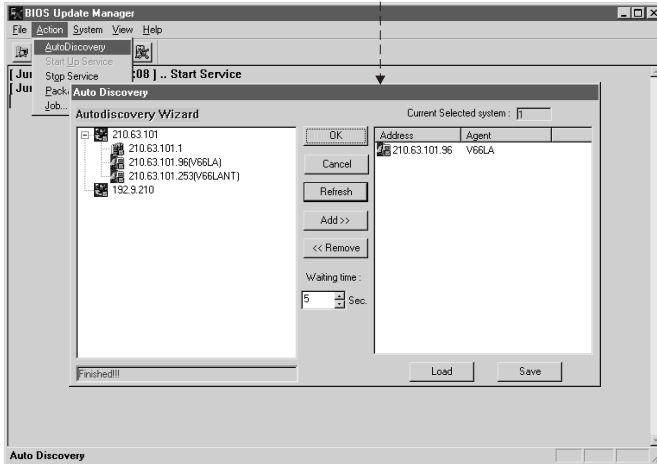




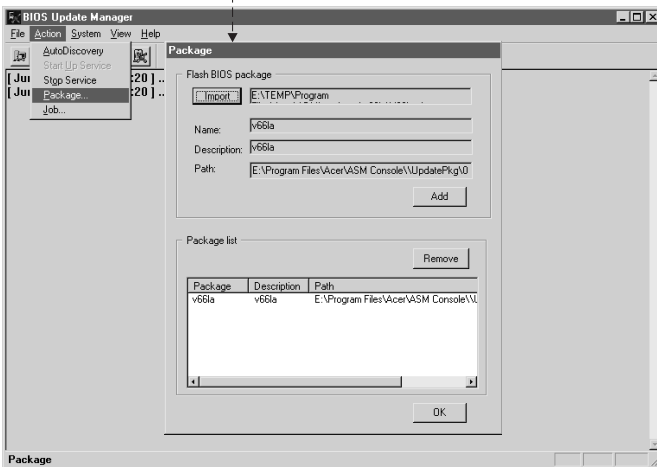
You can import CMOS definition file if the CMOS version of the target system does not match the current definition then you can setup CMOS remotely

BIOS flash manager

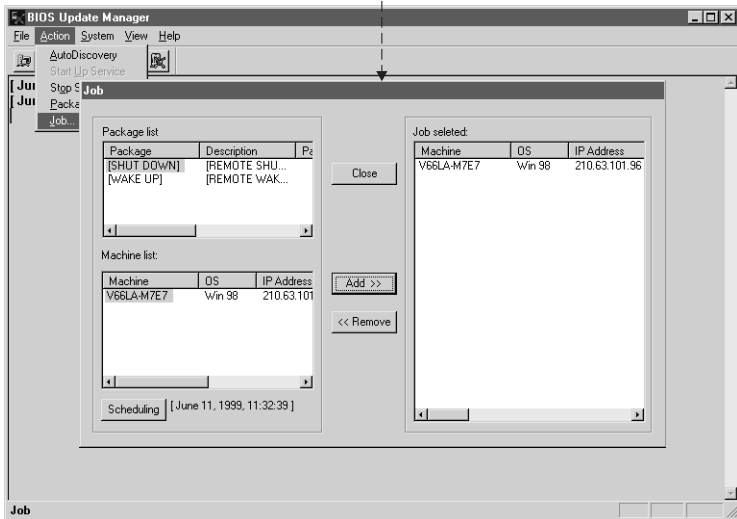
The Auto Discovery Wizard guides you to find systems in your network when you launch the BIOS Manager for the first time



To import a Flash BIOS Package into BIOS Update Manager:
 1. Click the Import button to open a package file
 2. Click the Add button to add it into the package list



After you have define a package list, you can define a job and schedule it to run



3 ASM Pro Console

ASM Pro Console is the central management station where the information gathered from the system agents is evaluated and assessed using either the SNMP (Simple Network Management Protocol) or RPC (Remote Procedural Call).

The SNMP protocol handles communication between the server and the ASM Pro system agent.

► Launching ASM Pro Console

To launch ASM Pro Console, press the **Start** button and select **Programs > ASM Pro > ASM Pro Console**, or double-click on the **ASM Pro Console** shortcut icon.

If you are using ASM Pro Console for the first time, you are asked to initialize a password before continuing.

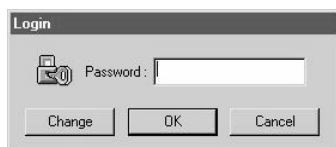
Initializing and changing the password

Access to the Console is controlled by a password. You are required to initialize a password when you access the Console for the first time.



To initialize a password, enter a password in the New Password field, then re-type the password in the Confirm field, and click on **OK**.

After setting up a password, the following dialog box appears each time you access ASM Pro Console:



To access ASM Pro Console, enter your password, then click on **OK**.

If you want to change your current password, click on the **Change** button to display the Change Password dialog box.

A screenshot of a 'Change Password' dialog box. It has a title bar with the text 'Change Password'. Inside, there are three text input fields labeled 'Old Password:', 'New Password:', and 'Confirm:'. Below the fields are two buttons: 'OK' and 'Cancel'.

To change your password, enter your current password, and then enter your new password. Retype your new password to confirm it, and then click **OK**.

ASM Pro Console confirms the password change by displaying a dialog box with the message "Password changed successfully."



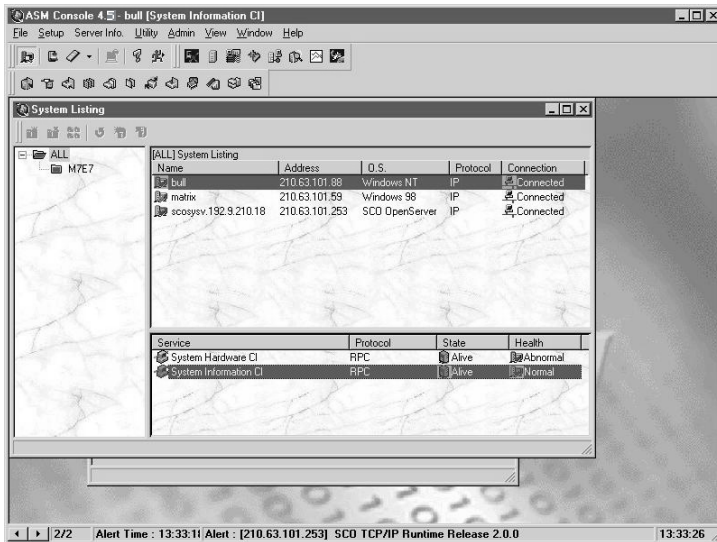
.....

Note: The security password mentioned here applies only to ASM Pro Console and not to its agents. See "ASM Pro Server Agent Utilities" on page 155 for more information on the ASM Pro Server Agent security password feature.

► ASM Pro Console user interface

The primary interface for ASM Pro Console is the System Listing window where you can view and check all of the systems being monitored. You can switch windows within the ASM Pro Console windows by pressing **Ctrl + Tab**. This allows you to compare the performance of various systems on your network by displaying the information about them simultaneously.




Before you view a system, you need to add it to the System Listing window.



Menu bar and toolbar

Toolbar buttons allow quick access to selected functions in ASM Pro Console through a single mouse click. The Menu Bar contains the following items and commands:











- The File Menu contains commands that allow you to print reports, to save information about a selected system, or to quit your ASM Pro Console session.







Command	Icon	Description
Auto Discovery		Displays the Auto Discovery screen.
Insert System		Manually adds a new system
Delete System/Service		Deletes an existing system or highlighted agent
Refresh Server		Reconnects to a selected agent or selected agent services
Exit		Exits ASM Pro Console

- The Setup Menu contains commands that allow you to specify the systems to be managed by ASM Pro Console and to set its initial value.


Command	Description
Config Polling Interval	Allows you to set polling intervals
Event Handler	Specifies event handling
System Alert Manager	Specifies the system alert manager
Option...	Displays the option window

- The Information Menu allows you to specify viewing commands for either server or desktop information. The list of commands displayed depends on which type of service you choose. Both types of information are described in the following tables.

Command	Icon	Description
Basic Information		Displays general information about the system and the system manager. For servers only.
O.S. Information		Displays the configuration of your operating system
DMI BIOS		Displays information about the processor, BIOS, and memory for the selected server
I/O Devices		Displays the configuration of I/O devices installed on the server
Storage		Displays the configuration of the server system's fixed disks
Network		Displays the configuration of the server's network interface cards. For servers only.
Resources		Displays information about IRQ addresses, DMA channels, I/O ports, and memory addresses
BIOS Event Log		Displays the event log stored in the NVRAM
Performance submenu		
Processor		Displays the CPU utilization
Memory		Displays the server's system memory utilization

Command	Icon	Description
Disk		Displays Disk Utilization of Windows NT and SCO OpenServer servers. For servers only.
File System		Displays the server's file system usage. For servers only.
NIC		Displays network card receive and transmit transactions
NIC Faults		Displays the number of instances of different faults in the server's network cards
Device submenu		
UPS		Displays information concerning UPS connection and configuration. For servers only.
Redundant Power Supply		Displays information about the redundant power supply installed in the system

If you want information about hardware components the following commands are displayed:


Command	Icon	Description
Health Monitor		Displays the current status of the CPU voltage, System voltage, Temperature, Fan status, Chassis status, Fuse status, SMART and RDM (Remote Diagnostic Management) status. For servers only.

If you want information about MIB-II components the following commands are displayed:


Command	Description
System	Implementation of the System group is mandatory for all systems. If an agent is not configured to have a value for any of these variables, a string of length 0 is returned
Interface	The Interfaces table contains information on the entity's interfaces. Each interface is thought of as being attached to a 'sub-network'. Note that this term should not be confused with 'subnet' which refers to an addressing and partitioning scheme used in the Internet suite of protocols.
AT	The Address Translation group contains one table which is the union across all interfaces of the translation tables for converting a NetworkAddress (e.g., an IP address) into a subnetwork-specific address. For lack of a better term, this document refers to such a subnetwork-specific address as a 'physical' address. For servers only.
IP	Implementation of the IP group is mandatory for all systems
ICMP	Implementation of the ICMP group is mandatory for all systems
TCP	Implementation of the TCP group is mandatory for all systems that implement the TCP. Note that instances of object types that represent information about a particular TCP connection are transient; they persist only as long as the connection in question

Command	Description
UDP	Implementation of the UDP group is mandatory for all systems which implement the UDP
SNMP	<p>Implementation of the SNMP group is mandatory for all systems which support an SNMP protocol entity. Some of the objects defined below are zero-valued in those SNMP implementations that are optimized to support only those functions specific to either a management agent or a management station. In particular, it should be observed that the objects below refer to an SNMP entity, and there may be several SNMP entities residing on a managed node (e.g., if the node is hosting on acting as a management station).</p> <p>This item is enabled only when the server supports the MIBII/SNMP group.</p>

- The Utility Menu contains commands to access special functions in ASM Pro Console.

Command	Icon	Description
Asset Manager		Loads and Views assets of monitored servers
Remote Flash BIOS		Remotely sets up Flash BIOS of systems connected to LAN via server.
Remote CMOS Setup		Remotely sets up CMOS of systems connected to LAN via server.
Remote Console		Allows the system administrator to remotely control the local systems connected to the LAN via a server, if access is granted.



- The View Menu allows you to display or hide certain components of your ASM Pro Console user interface.

Command	Icon	Description
Tool Bar		Displays the tool bar
Status Bar		Displays the status bar
System Overview		Displays an overview of the system.
System Listing		Displays systems currently monitored by ASM Pro Console
Auto Discovery		Displays the Auto Discovery screen.

- The Window Menu provides the following commands that allow you to arrange multiple views of multiple documents in the application window.

Command	Description
Cascade	Arranges windows in an overlapped fashion
Tile	Arranges windows in non-overlapped tiles
Arrange Icons	Arranges icons of minimized windows
System Listing	Goes to the specified window

- The Help Menu provides you with assistance for this application.

Command	Icon	Description
Help Topics		Provides general instructions on using Help and offers you an index to topics on which you can get help
About Console		Displays the version number of this application and license information

Using Auto Discovery to add a system to the System Listing

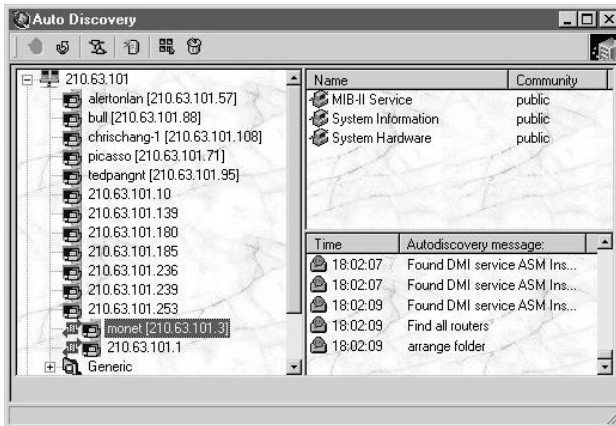
The Auto Discovery window displays when you run ASM Pro Console for the first time. It automatically detects all of the system agents in your subnet. It displays the names of these systems and their protocols and addresses in the left panel of the Auto Discovery window. The auto discovery process may take some time depending on the size of your network.

The upper right panel of the auto discovery window displays the services of the system highlighted in the left panel. This information includes the name and OID of the services, if any exist. These services typically include hardware, System, or Management Information Base-II (MIB-II) for server systems.







The lower right panel displays messages about the operations of Auto Discovery. The messages include the name of the operation and the time it was performed.

There are two types of agents shown in Auto Discovery:

- Agents provided by ASM Pro
- Industry standard agents.



Auto Discovery Commands

Command	Icon	Description
Stop		Cancels current search operation requested by user
Refresh		Updates the current list of systems by performing another search on the network
Insert Subnet		Activates the Subnet window which allows you to input the first three blocks of IP addresses and performs a search on the network
Add to System Listing		Adds the selected system to the System Listing window
Options		Activates the Options window. See "Specifying options" on page 63
Clear Messages		Clears the messages, if any, found in the lower right panel of the Auto Discovery window

After you have run ASM Pro for the first time, you can access the Auto Discovery window by clicking the **Auto Discovery** button on the toolbar, or by selecting **File > Auto Discovery** on the menu bar.

Adding a system from Auto Discovery to System Listing

ASM Pro Console uses two types of protocol to monitor server systems:

- IPX (Internetwork Packet Exchange) is usually used for Novell NetWare operating systems.
- IP (Internet Protocol) is used for Windows NT, Windows 2000 Server, RedHat Linux, SCO OpenServer, and SCO UnixWare operating systems.



.....

Note: IPX and IP protocols are automatically detected by ASM Pro.

ASM Pro Console detects RedHat Linux, NetWare, SCO OpenServer, SCO UnixWare, and Microsoft Windows systems on your network and displays them in the left panel of the Auto Discovery window.

ASM Pro Console displays each system according to the time a connection was made. The order of the systems listed may vary each time you open the Auto Discovery window.

To add an IP or IPX system to the System Listing:

1. Select **File > Auto Discovery**, or click on the **Auto Discovery** button on the toolbar to access the Auto Discovery window.
2. Click on the name of an agent in the left panel of the Auto Discovery window.
3. Click the **Add to System Listing** button. The system you just selected moves to the System Listing window.
4. Repeat steps 1 and 2 if you want to add more systems. When you finish adding systems, close the Auto Discovery window.

In the System Listing window, the color of the system symbol shown on the left of the system name appears red at first. This color changes to yellow during the initialization process, and finally changes to green when the system has finished initializing.

Adding a subnet

Subnets are smaller groups of servers and desktops within a local network. For example, a local network might contain separate subnets for different departments like purchasing, engineering, and manufacturing.

To add a subnet:

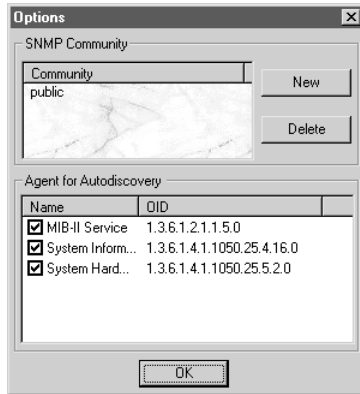
1. Click on the **Add Subnet** button. The Subnet window appears.
2. Enter the first three blocks of the IP address you want the Console to search.

ASM Pro Console searches all addresses in the specified with different protocols to find the agent. For all of the ASM Pro agent services, click on the Option button.

Specifying options

Click on the **Options** button in the Auto Discovery window to display the Options window as shown below. The Options window allows you to:

- Add or remove an SNMP community name
- Select the agents you want the Console to check.

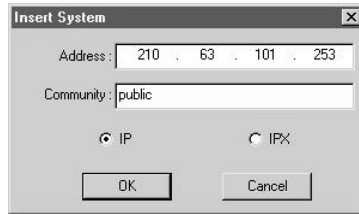


To add a new SNMP community, click on **New** and type in the community name. To remove a SNMP community name, highlight the community name and click **Remove**. The list of agents may vary depending on how you installed ASM Pro Console.

To specify which agents Console checks, click the square box next to each agent in the Discovery Agent Type box that you want checked to turn checking on for that agent.

Manually adding a system

To add a system to the System Listing manually, you type its IP or IPX address in the Insert System window.



To add an IP or IPX address manually:

1. Click **File > Insert a System** in the System Listing window.
2. Type the IP or IPX address of the system you want to monitor, and click on **OK**. If the address is available, it appears in the System Listing window.

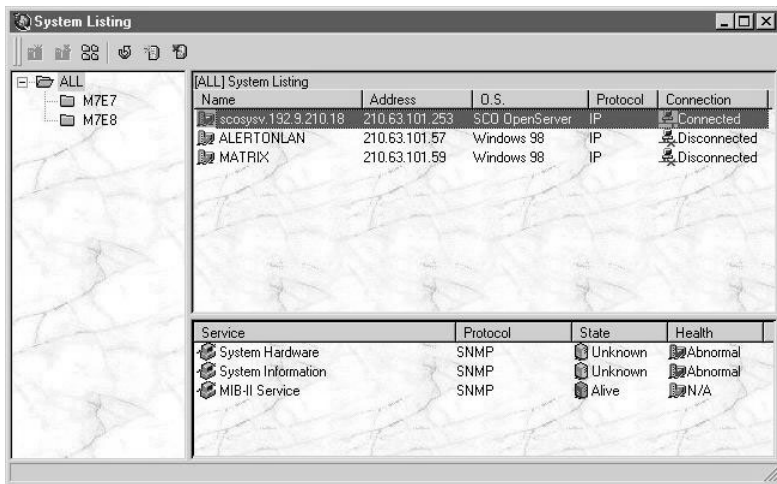
Removing a system from the list

To remove a system from the System Listing window, highlight the system that you want to delete and click the **Delete a System** toolbar button, or select **File > Delete a System**.

▶ Working with System Listing

The System Listing window displays the systems currently available to Console for management. If this window contains no system names, you need to add network systems to the System Listing. You can add a system by clicking **File > Insert a System**, or by using Auto Discovery. Refer to “Using Auto Discovery to add a system to the System Listing” on page 60 for these procedures.

The system listing screen contains three panels: the system organizer panel, the all system listing panel, and the system service panel.



The All System Listing panel displays the following information: System Name, Address, Operating System, Protocol, and Connection status. The address is the TCP/IP address or the IPX address (for Novell systems).

The Service panel displays the following information: Service Type, Service Protocol, State of the Service, and Health of the System.







The services for server systems are System Hardware and System Information. For desktop systems, Desktop hardware and Desktop Information.

The protocol for desktop systems is RPC. The protocol for server systems is Small Network Management Protocol (SNMP).

The health of a system is normal, abnormal, or a hardware feature not recognized by the ASM Pro product. The health is abnormal when the service is functioning but is not functioning as it should.

The System Listing can be sorted by clicking on the column bars. For example, if you click on System Name, the system names are displayed in alphabetical order.

A colored system symbol at the left of each system name indicates the status of the server. The color of these symbols may change based on the performance and condition of the server.

Command	Icon	Description
Create New Folder		Creates a new folder with a temporary name under the ALL folder directory
Delete Folder		Erases the folder you specified in the ALL folder directory
Show All Folder		Displays all the folders and their sub-folders
Refresh Server		Refreshes the System Listing
Add to System Listing		Manually adds a new system
Delete System/Service		Deletes an existing system or highlighted agent

System organizer

The System Organizer is a tree-structured directory on the left hand side of the System Listing window that allows you to organize network systems into folders.

For example, using folders in the system organizer, you can network systems by type (desktop or server), by location, or by building.

Once you have created folders, you can drag and drop systems from the All System Listing panel to one of the folders.

To create a new folder:

1. Click the **Create New Folder** icon, or click the right mouse button and choose **New Folder** from the menu. The new folder appears with a temporary name.
2. Type a title for the new folder and press **Enter**.

To delete an existing folder:

1. Select the folder you want to delete.
2. Click the **Delete Folder** icon, or click the right mouse button and choose **Delete Folder** from the menu.

To display all the lower level folders, click the **Show All Folder** icon or click the right mouse button and choose **Show All** from the menu.

System symbols

One of the symbols shown below (System Box or Service Box) appears to the left of each system name.



System Box - This means the system is connected in-band via an ethernet connection. The link is initiated automatically when the system is added to the System Listing.



Service Box - This means a service system. Each server in the System Listing has a Hardware, System, and MIB-II service. The link is initiated automatically when the server is added to the System Listing.

It can also be a combination of both boxes if the system agent is installed with both types of agent.

The system and service symbols appear in one of the following colors to indicate the current status of the system.

- Green means that the communication link between the agent and monitoring Console is up and running.
- Yellow means that ASM Pro Console did not receive a response from the system agent within a time period. This may be due to heavy network traffic, a network error, or the system being busy.
- Red means that the communication link between the Console and the System Agent is down or an error has occurred.



.....

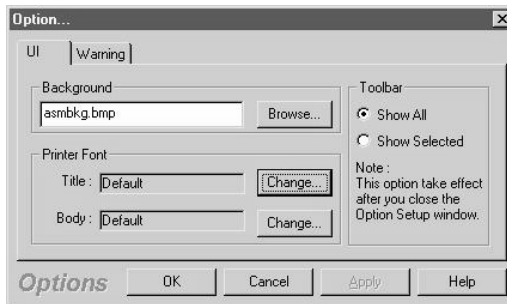
Note: If the status of the selected system is red (question mark), all toolbar buttons are disabled (grayed out). Only the Auto Discovery button is available.

Customizing System Listing

You can use the Option dialog box to customize the System Listing user interface. To display the Option dialog box, select **Setup > Option.....**

User interface (UI) tab

The U.I. tab allows you to change the settings of the background display and printer fonts.



To display all of the toolbars, regardless of the type of server you have selected, click on the **Show All** radio button in the toolbar box and then click **OK**.

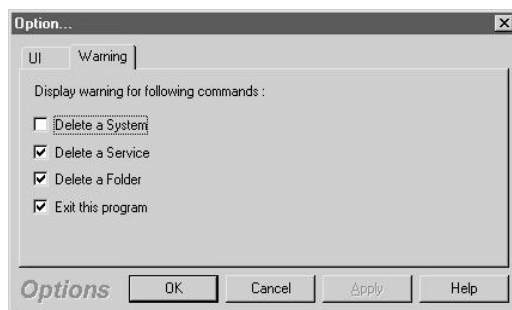
To personalize the wallpaper of the Console, click **Browse** and choose a graphic file, then click **OK**.

To change printer fonts, click the **Change** button. A listing of the fonts located in the Windows fonts folder appears. Choose one and click **OK**.

Warning tab

The options here specify whether ASM Pro Console should generate a warning message to alert the user when one of the following events occurs:

- Deleting a system
- Deleting a service
- Deleting a folder
- Exiting ASM Pro Console



To enable these functions, check the appropriate checkbox and click **OK**.

To disable these functions, uncheck the appropriate checkbox and click **OK**.

► System information and performance monitoring

From the System Listing window, you can select a system from the service panel to view agent information. To see the information, click the name of the service in the service panel (the bottom right panel) of the System Listing window: System, Hardware, or MIB-II, then select an option from the Information menu. The options in the Information menu vary, depending on which services are selected.

System information

The following sections describe the Information menu options that appear when a System Information service is selected in the System Listing window.

Basic information

Select **Information > Server Information > Basic Information** to display the Basic Information window. The window consists of three sections: System, Machine, and Modem.

System tab

Click on the **System** tab to view general information about the system. This tab also displays the system's network address and System Agent version.

MONET - Basic Information

System | Machine | Manager

Machine Name : MONET

Network Address : 210.63.101.3

Operation System : Windows NT 4.0 [build 1381] Service Pack 4

Server Agent Version : Server3.30

Computer Time : Thu Apr 29 09:34:42 1999

Up Time : 1 day 00 : 19 : 04

Machine Location : ASM console test Lab

Machine tab

Click on the **Machine** tab to view general information about the system's components, such as: Base Board, CPU, BIOS, and Physical Memory.

MONET - Basic Information

System | Machine | Manager

Base Board

Manufacture : ACER

Product Name : M11A

Version : 96105-1A

Serial No : 48.59101.011

BIOS

Vendor : ACER

Release Date : 06/05/96

Version : ACR2FE00408-961106-R01-B5

CPU

Manufacture : Intel

Family : Pentium Pro Family

Current Speed : 200 MHz

External Clock : 66 MHz

Physical Memory

Total Memory : 160 MB

Maximum Memory Capacity : 384 MB

Memory Slots No. : 3

Memory Slots Used No. : 3

Manager tab

Click on the **Manager** tab to view information about the person in charge of the system (for servers only). The manager information can be changed on the ASM Pro Server Agent system using the `asmcnfig` program.

MONET - Basic Information

System | Machine | Manager

Machine Location : ASM console test Lab

Manager : Manager

Office Address :

Office Phone :

Home Address :

Home Phone :

Pager :

E-mail :

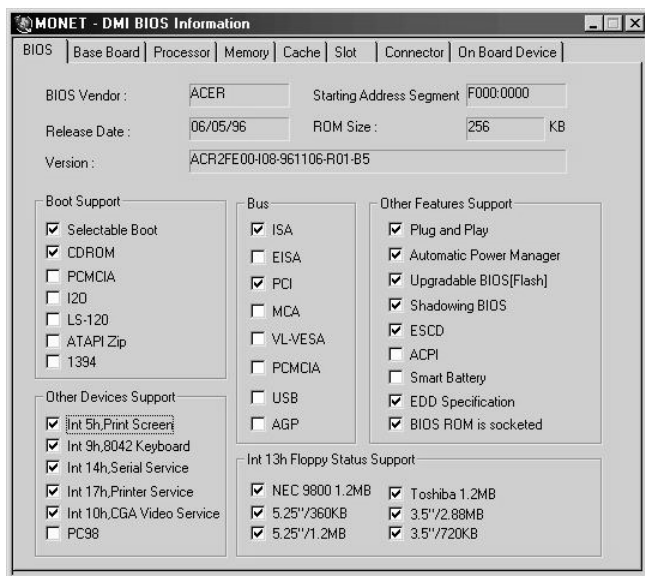
Refresh Undo Set

DMI BIOS information

Select **Information > Server Information > DMI BIOS** to display the System Configuration screen.

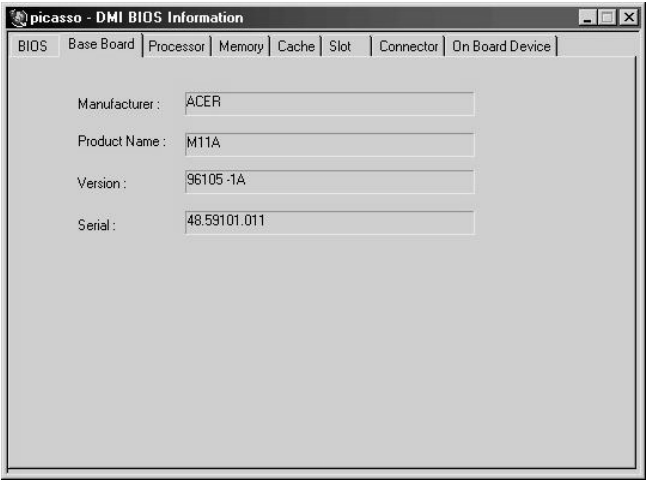
BIOS

The **BIOS** (Basic Input/Output System) tab displays general information about the BIOS version installed in the system. It also displays the type of hardware supported by the BIOS. The check marks show the supported bus, function, boot device, int13 floppy status, and other services based on the DMI specification used.



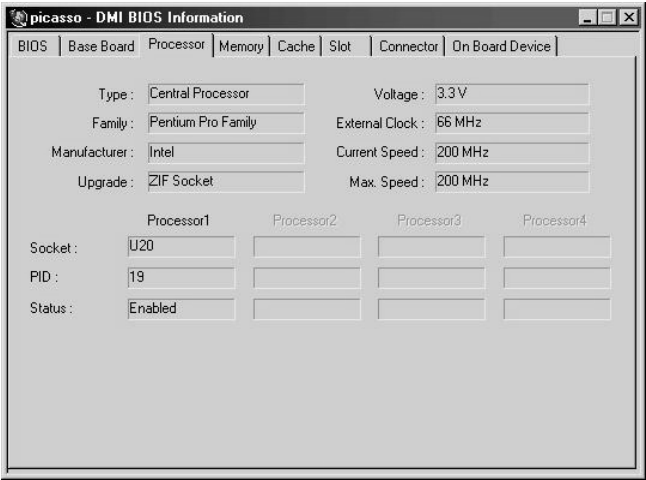
Base board

The **Basic Motheboard Information** tab displays the manufacturer, product name, version and serial number of the base board.



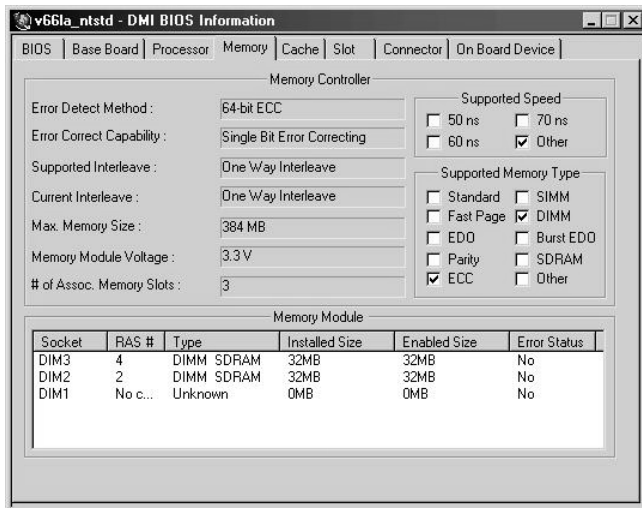
Processor

The **Processor** tab displays the type, speed, and other information about each CPU on the ASM Pro agent.



Memory

The **Memory** tab displays information about the memory controller and the memory module.



Memory controller

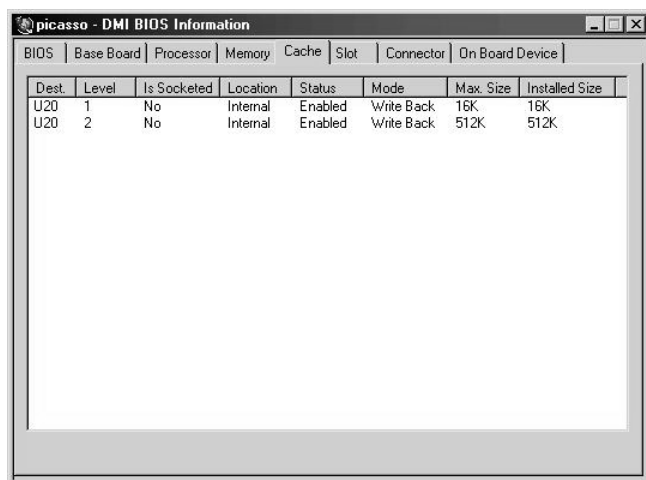
Memory Controller displays the attributes of all memory modules present in the controller's sockets.

Memory module

Memory Module displays detailed information about each socket, including the type, installed size, and error status.

Cache

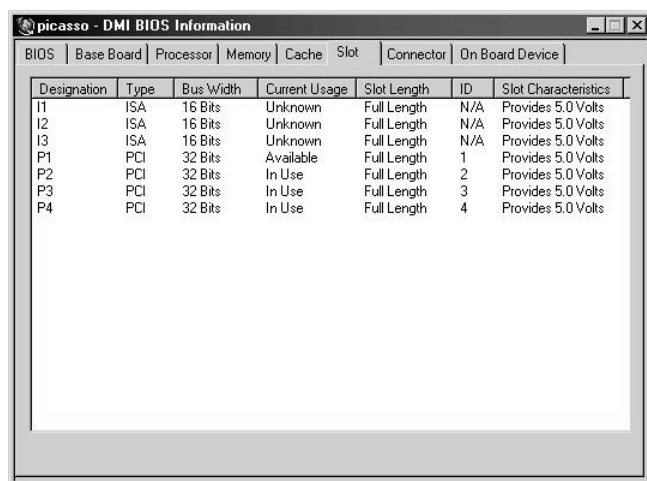
The **Cache** tab displays the attributes of CPU cache devices. The CPU cache is a chunk of fast memory. It stores data that the CPU can process quickly.



BIOS Base Board Processor Memory Cache Slot Connector On Board Device							
Dest.	Level	Is Socketed	Location	Status	Mode	Max. Size	Installed Size
U20	1	No	Internal	Enabled	Write Back	16K	16K
U20	2	No	Internal	Enabled	Write Back	512K	512K

Slot

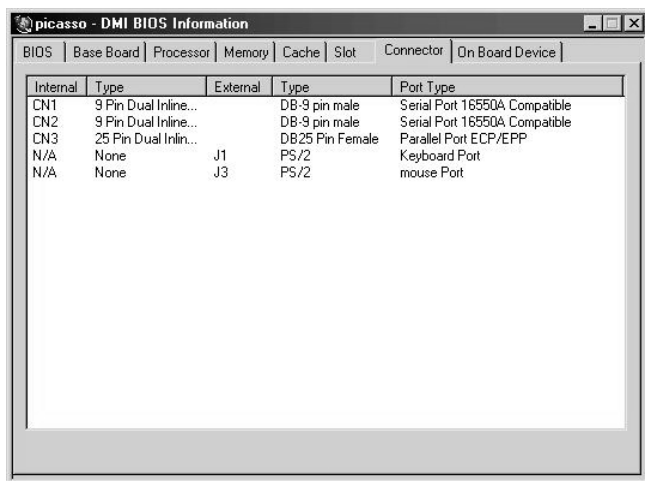
The **Slot** tab displays information about different slots on the system board, including the type and availability of each bus. Refer to the EISA (Extended Information System Architecture) or PCI (Peripheral Component Interface) specification for definitions of the slot IDs. The Designation field refers to the motherboard layout label.



BIOS Base Board Processor Memory Cache Slot Connector On Board Device						
Designation	Type	Bus Width	Current Usage	Slot Length	ID	Slot Characteristics
I1	ISA	16 Bits	Unknown	Full Length	N/A	Provides 5.0 Volts
I2	ISA	16 Bits	Unknown	Full Length	N/A	Provides 5.0 Volts
I3	ISA	16 Bits	Unknown	Full Length	N/A	Provides 5.0 Volts
P1	PCI	32 Bits	Available	Full Length	1	Provides 5.0 Volts
P2	PCI	32 Bits	In Use	Full Length	2	Provides 5.0 Volts
P3	PCI	32 Bits	In Use	Full Length	3	Provides 5.0 Volts
P4	PCI	32 Bits	In Use	Full Length	4	Provides 5.0 Volts

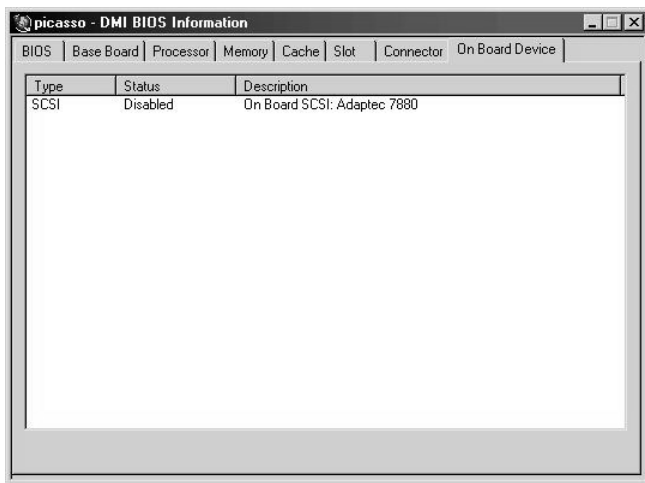
Connector

The **Connector** tab displays information about the motherboard connectors.



Onboard device

The **Onboard Device** tab displays information about devices found on the motherboard.

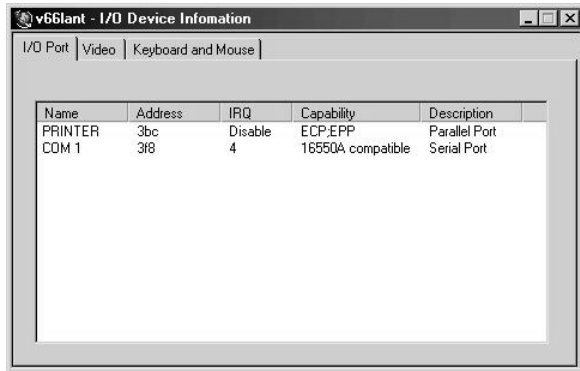


Input/Output device information

Select **Information > Server Information > Input/Output Device** or **Information > Desktop Information > Input/Output Device** to display Input/Output information for the keyboard, mouse, and video.

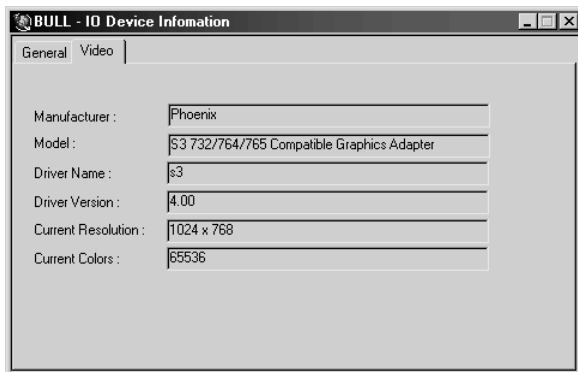
I/O port tab

The **I/O Port** tab displays information about the system's input/output devices and ports.



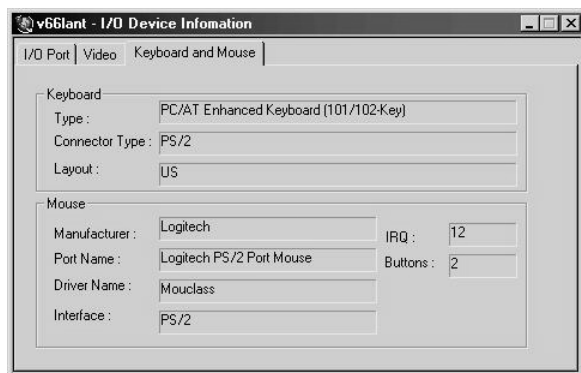
Video tab

The **Video** tab displays information about the system's video device and driver.



Keyboard and mouse tab

The **Keyboard and Mouse** tab displays general information about the keyboard and mouse type and configuration.



Storage information

Select **Information > Server Information > Storage** to display the Storage Information screen. This screen displays the size, type, and controller of all physical and logical hard disks that are configured on the system, as well as the floppy disk drive, Zip drive, or CD-ROM drive.

Physical disk

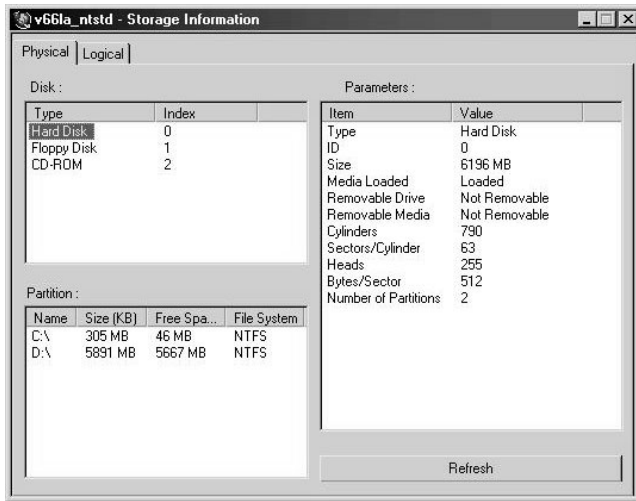
Physical disk indicates the number of actual hard disk drives installed in a system. Each hard disk drive is connected to an adapter that controls them.



Note: The physical disk screen for the desktop systems differ slightly from the screen shown here but the functions are the same.

To view storage drive information, click one of the items displayed in the upper left window. The storage device's logical partition (if the device you chose is a hard disk drive) and controller information displays on the lower left and right window.

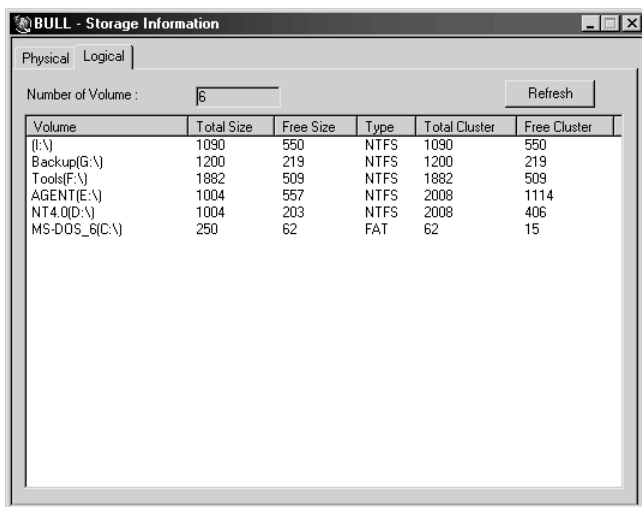
Click **Refresh** to update the information on the screen.



Logical disk

Logical disks are created when you separate a hard disk into several partitions and specify each of them as an independent logical drive. This window displays information about each of the logical drives created on the hard disk drives. The type of information shown depends on the type of agent selected: desktop or server.

Click **Refresh** to update the information on the screen.



Volume	Total Size	Free Size	Type	Total Cluster	Free Cluster
[I:\]	1090	550	NTFS	1090	550
Backup[G:\]	1200	219	NTFS	1200	219
Tools[F:\]	1882	509	NTFS	1882	509
AGENT[E:\]	1004	557	NTFS	2008	1114
NT4.0[D:\]	1004	203	NTFS	2008	406
MS-DOS_6[C:\]	250	62	FAT	62	15

Operating system information

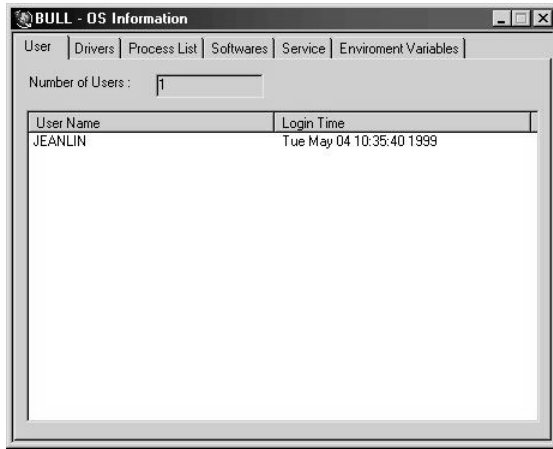
Select **Information > Server (or Desktop) Information > O.S. Information** to display the Operating System Information screen that displays information about the operating system. There are six screen tabs for server systems and three for desktop systems.

Server system

There are six screen tabs for server systems.

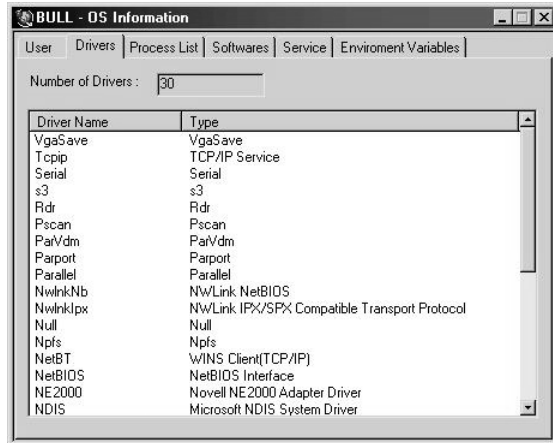
User tab

The **User** tab displays the number of users currently logged on to the server.



Drivers tab (only available for Windows NT and Windows 98 operating systems)

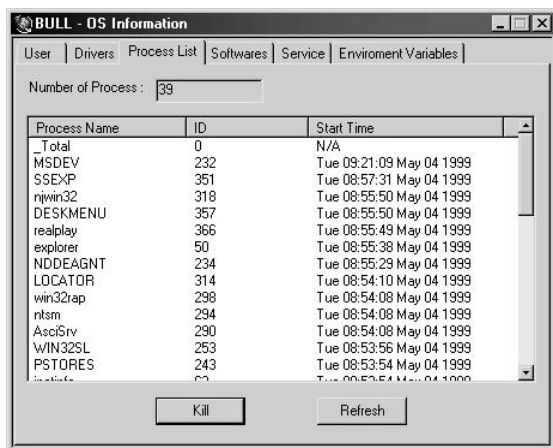
The **Drivers** tab displays all the device drivers installed in the ASM Pro Agent. It also displays the total number of drivers installed in the system.



Process list tab

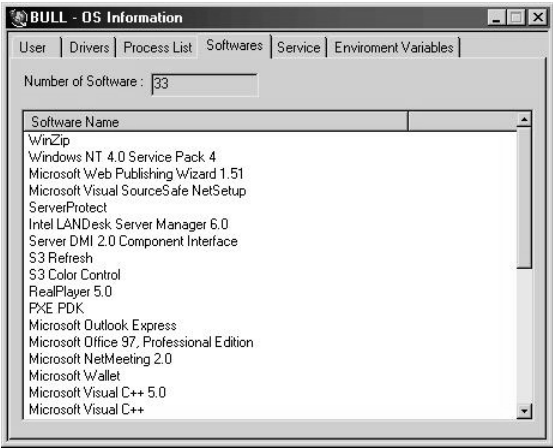
The **Process List** tab displays the programs and DLL libraries that are currently running on the system. For a server agent, it also displays the time that a process was executed.

To terminate a process in the list, select the process and click the **Kill** button.



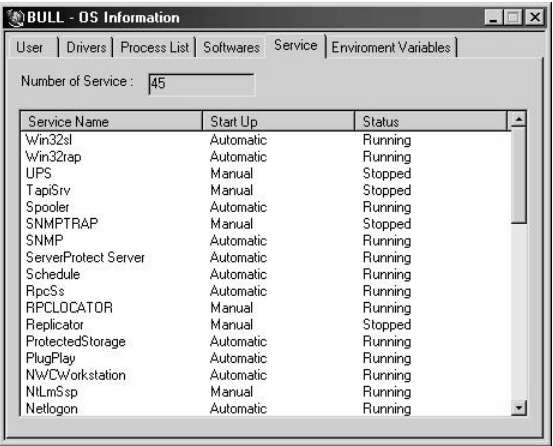
Software tab

The **Software** tab displays the software packages currently installed on the server.



Service tab (only available for Windows NT operating systems)

The **Service** tab displays the number of services currently active in the server.



Environmental variables tab (only available for Windows NT operating systems)

The **Environmental Variables** tab displays the contents of the initialization file of the operating system.



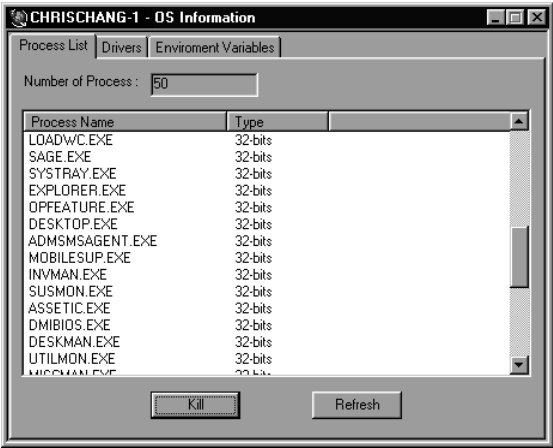
Desktop system

There are three screen tabs for desktop systems.

Process list tab

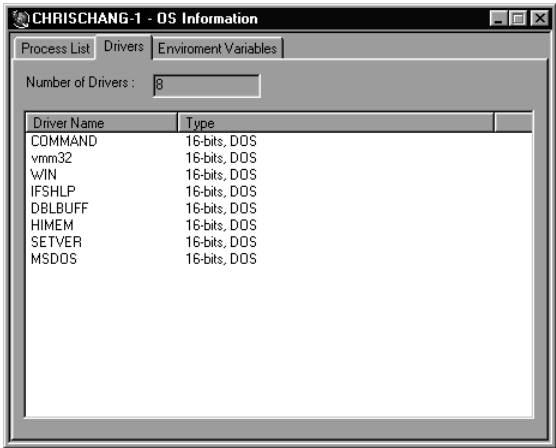
The **Process List** tab displays the number of processes the desktop has executed since it was turned on. It also shows the type (16-bit or 32-bit) of the program that was executed.

To terminate a process in the list, select the process and click the **Kill** button.



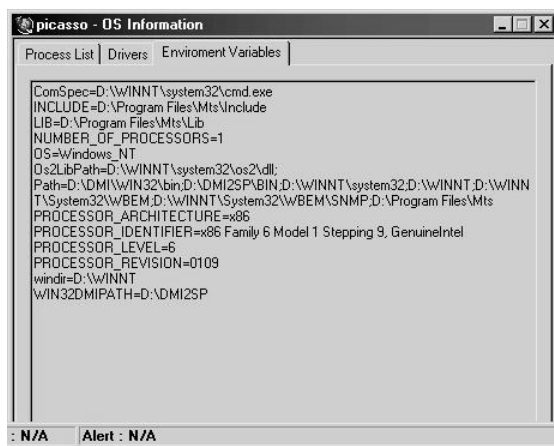
Drivers tab

The **Drivers** tab displays all the device drivers installed in the desktop. It also shows the total number of drivers installed in the system.



Environmental variables tab

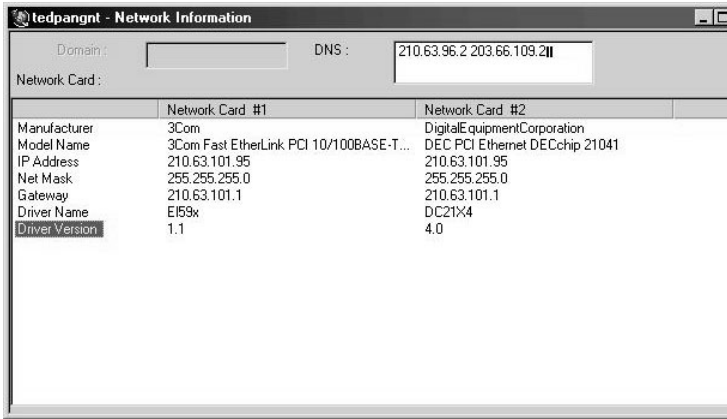
The **Environmental Variables** tab displays the contents of the initialization file of the operating system.



Network information

Select **Information > Network Information** to display the network Information screen. This screen displays information about some of the network interface cards. Not all network cards provide this type of information.

Details are provided for the type, model, slot number being used, IRQ, I/O port, base memory address, DMA address, IP address, gateway, NIC (Network Interface Card) speed, and NIC driver.



System resource information

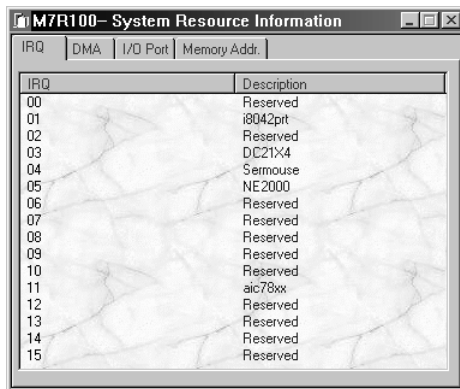
Select **Information > System Resource** to display the System Resource Information screen. System Resource Information consists of four tabs: IRQ, DMA, I/O Port, and Memory Address. The following sections briefly describe each of these tabs.

Server system

There are four tabs for server systems.

IRQ information

This screen displays a list of each IRQ and its assigned use in the system. It can be used to detect a hardware interrupt conflict.

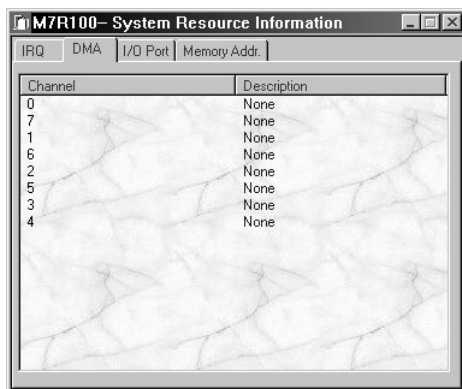


The screenshot shows a window titled "M7R100-System Resource Information" with four tabs: "IRQ", "DMA", "I/O Port", and "Memory Addr.". The "IRQ" tab is selected, displaying a table with two columns: "IRQ" and "Description".

IRQ	Description
00	Reserved
01	i8042prt
02	Reserved
03	DC21x4
04	Sermouse
05	NE2000
06	Reserved
07	Reserved
08	Reserved
09	Reserved
10	Reserved
11	aic78xx
12	Reserved
13	Reserved
14	Reserved
15	Reserved

DMA information

This screen displays all the DMA channels used by each device in the system.

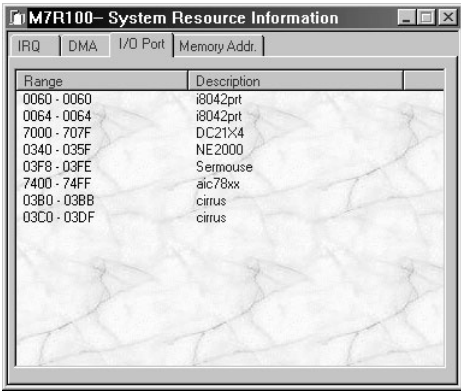


The screenshot shows the same window with the "DMA" tab selected. It displays a table with two columns: "Channel" and "Description".

Channel	Description
0	None
7	None
1	None
6	None
2	None
5	None
3	None
4	None

I/O port information

This displays the range of port addresses occupied by the system resources.

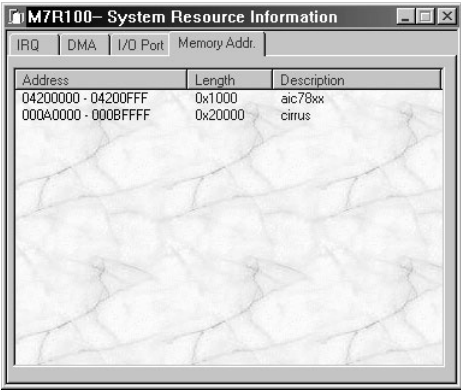


The screenshot shows a window titled "M7R100- System Resource Information". It has four tabs: "IRQ", "DMA", "I/O Port", and "Memory Addr.". The "Memory Addr." tab is selected. The table below lists memory ranges and their descriptions.

Range	Description
0060 - 0060	i8042prt
0064 - 0064	i8042prt
7000 - 707F	DC21x4
0340 - 035F	NE2000
03F8 - 03FE	Sermouse
7400 - 74FF	aic78xx
03B0 - 03BB	cirrus
03C0 - 03DF	cirrus

Memory address

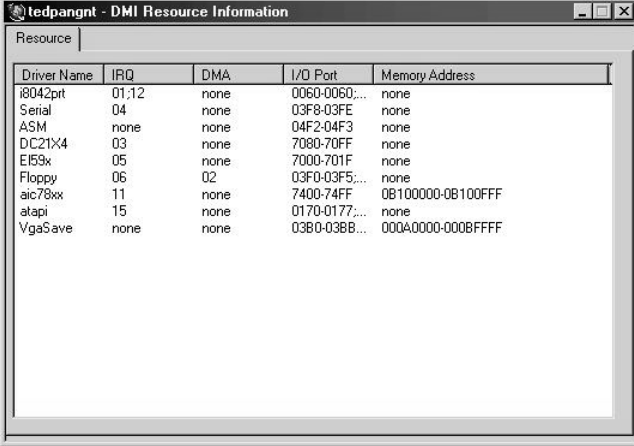
This displays the system's base memory usage, including the address, the length, and its description.



The screenshot shows the same window as above, but with a different table structure. It has columns for "Address", "Length", and "Description".

Address	Length	Description
04200000 - 04200FFF	0x1000	aic78xx
000A0000 - 000BFFFF	0x20000	cirrus

Desktop system



The screenshot shows a window titled "tedpangnt - DMI Resource Information" with a "Resource" tab selected. It contains a table with the following data:

Driver Name	IRQ	DMA	I/O Port	Memory Address
i8042prt	01,12	none	0060-0060...	none
Serial	04	none	03F8-03FE	none
ASM	none	none	04F2-04F3	none
DC21X4	03	none	7080-70FF	none
EISAx	05	none	7000-701F	none
Floppy	06	02	03F0-03F5...	none
aic78xx	11	none	7400-74FF	0B100000-0B100FFF
atapi	15	none	0170-0177...	none
VgaSave	none	none	03B0-03BB...	000A0000-000BFFFF

IRQ

The **IRQ** column displays a list of each IRQ and its assigned use in the system. It can be used to detect a hardware interrupt conflict.

DMA

The **DMA** column displays all the DMA channels used by each device in the system.

I/O port

The **I/O Port** column displays the range of port addresses occupied by the system resources.

Memory address

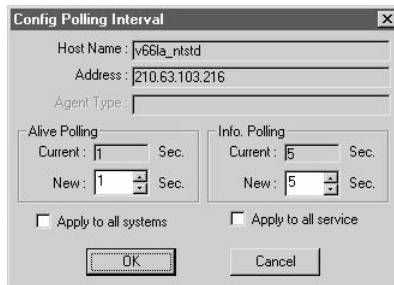
This displays the system's base memory usage, including the address, the length, and its description.

Performance monitoring

ASM Pro monitors the performance of each agent periodically and sends this information back to the ASM Pro Console. The polling interval of the Console can be configured to check the agents whenever the system administrator chooses.

Configuring polling interval

Select **Setup > Config Polling Interval** to display the Polling Interval Setup dialog box shown below.



The Alive Polling interval indicates how often the connection status between the Console and the Agent is checked. The Information Polling Interval determines how frequently the Console polls the Agents to update its data.

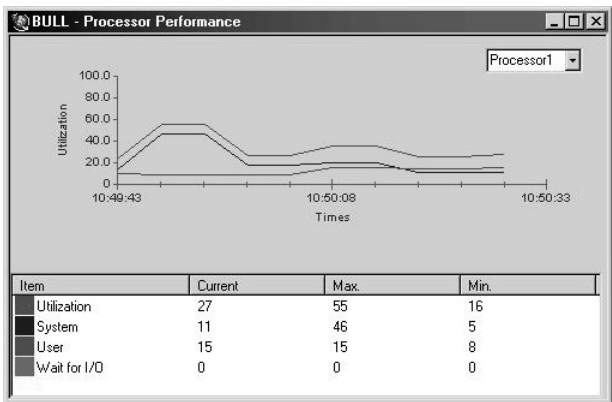
To change the polling interval, click the up and down button to increase or decrease the number of seconds, or type in the number of seconds, and click **OK**. The polling intervals must be from 1 to 60 seconds.

Processor performance (for server system)

Select **Information > Performance > Processor** to access the Processor Performance information screen.

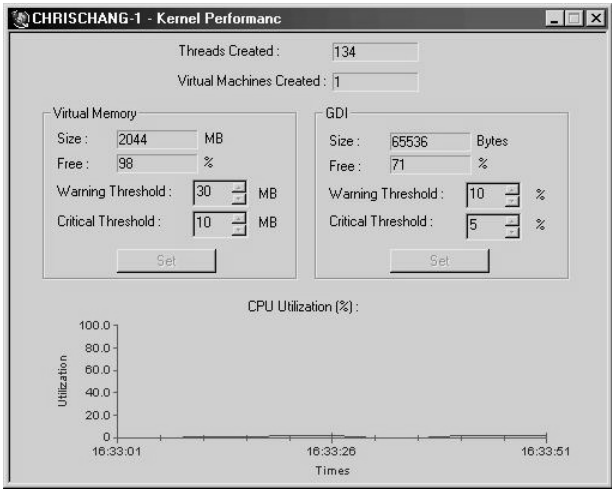
This window displays the current load and load limit of each CPU (Central Processing Unit) installed in the system. The higher the percentage, the more the CPU is being used. This indicates how much load the system has and how well the system's processing power is handling the load.

For multiple CPU systems, the multi-processor performance can be displayed only on the MP-Kernel OS.



Kernel performance (for desktop system)

Select **Information > Performance > Processor** to access the Kernel Performance information screen.



The Virtual Memory box indicates the size of virtual memory. It also shows the percentage of virtual memory available related to system virtual memory. The threshold settings allow ASM Pro to warn you if system operation exceeds capacity.

To adjust the warning and critical threshold value, click the Up/Down arrow key, or type the value in the text box and then click **Set**. The GDI (Graphical Device Interface) box also functions the same way.

Below the boxes, a graph of CPU use shows the current load and the load limit of the CPU installed in the system. The higher the percentage, the more the CPU is being used. This indicates how much load the system has and how well the system's processing power is handling the load.

Memory utilization

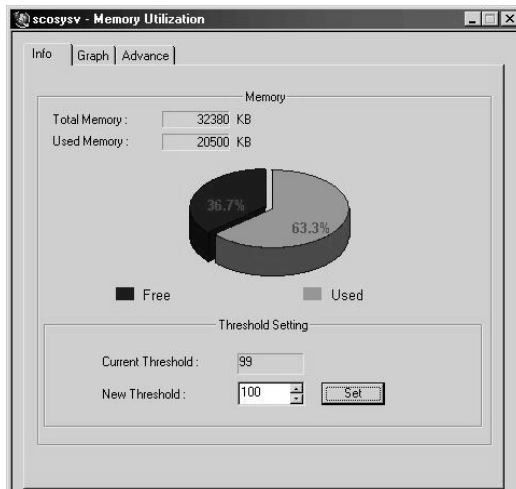
Select **Desktop (or Server) Information > Performance > Memory** to access the Memory Utilization information screen

The Memory Utilization window consist of three tabs: Info, Graph, and Advance. The following sections describe of each of these tabs.

Info

If the system being monitored is a server, the **Info** tab displays a graph showing the percentages of used and unused memory in the system. It also indicates the threshold value of memory use.

To change the threshold value of memory use in a server, click the up and down button to increase or decrease the percentage of use, or type in the desired value, and click **Set**. If the memory allocation in the server exceeds the threshold value, an alert is sent to the Console. For more information about alert handling, see Chapter 4 - System Alert Manager for more information.

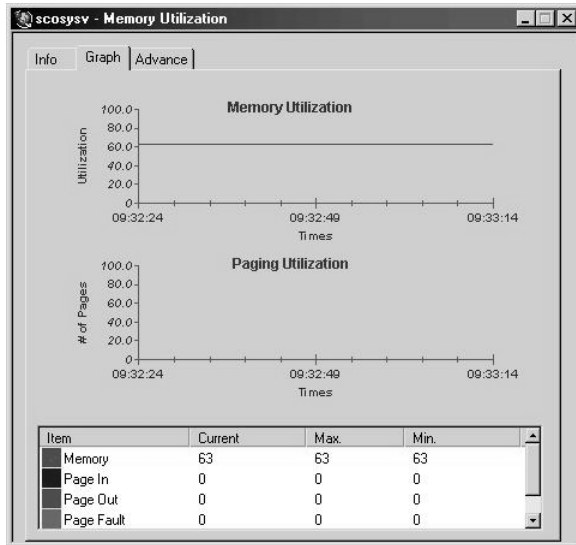




Note: If the password is enabled in the ASM Pro Server Agent, enter the password for the Agent when changing the threshold setting.

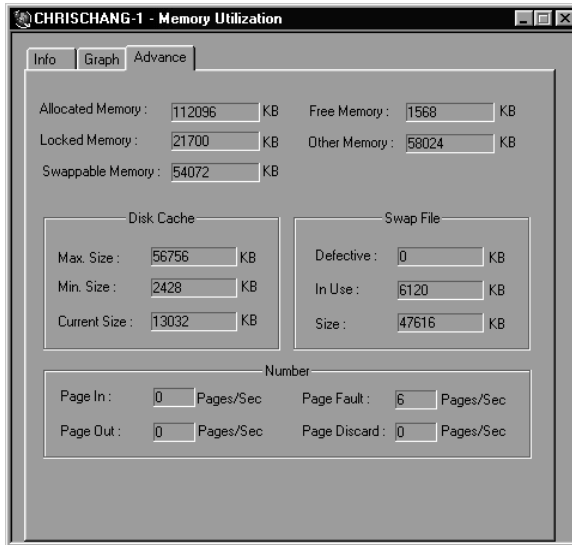
Graph

The **Graph** tab shows a graph that measures the use of system memory and memory paging along a time table.



Advance

The **Advance** tab shows more detailed information about memory use for different operating systems.



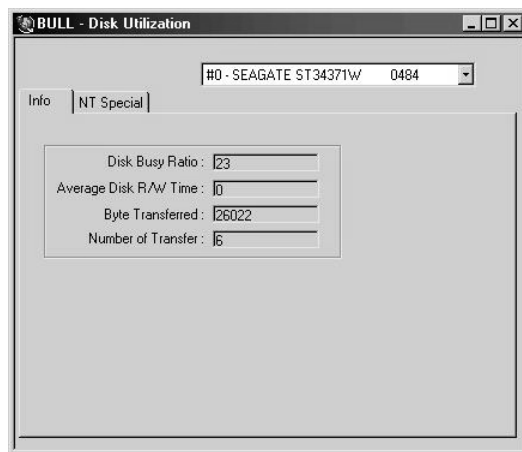
Note: This screen display may be different for different operating systems.

Disk utilization (for server systems only)

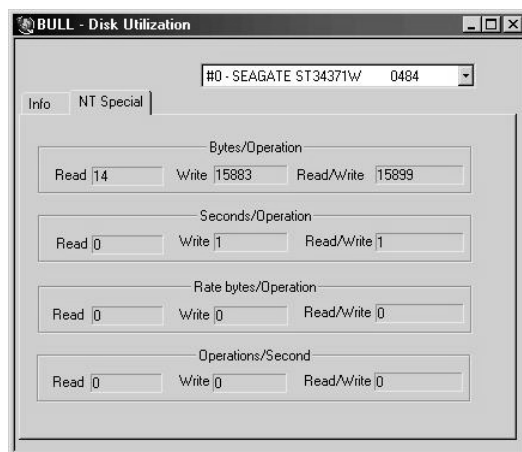
Select **Server Information > Performance > Disk** to access the Processor Performance information screen.

For NetWare, this command is enabled if a server is highlighted in the System Listing window, and is used to view the number of redirected blocks in the storage device.

For SCO OpenServer, SCO Unixware, and Windows NT, click the pulldown menu to choose the hard drive you want to view if the system have more than one hard drive. The screen shows the read/write access and over-all utilization of the hard disk.



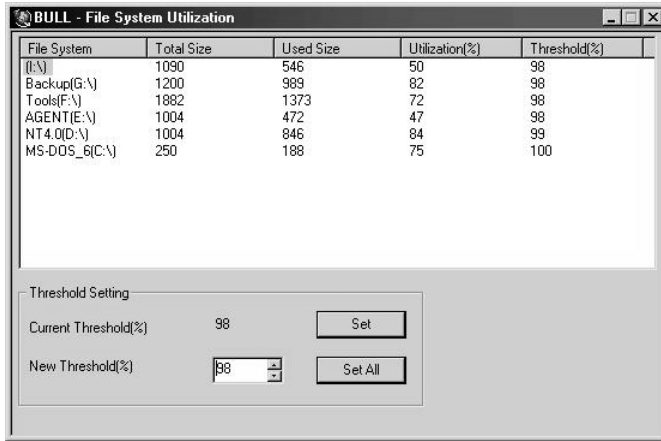
For Windows NT, you can click on the **NT Special** tab to display information about Read, Write, and Read/Write operation that is only supported in Windows NT. See the following example screen.



File system utilization

Select **Desktop (or Server) Information > Performance > File System** to access the File System Utilization information screen.

In the screen below, the utilization column indicates the percentage of space used for each file system. When file system use exceeds the threshold value, the Agent sends an alert to the Console. See Chapter 4 - System Alert Manager for more information.



File System	Total Size	Used Size	Utilization(%)	Threshold(%)
I:\	1090	546	50	98
Backup(G:\)	1200	989	82	98
Tools(F:\)	1882	1373	72	98
AGENT(E:\)	1004	472	47	98
NT4.0(D:\)	1004	846	84	99
MS-DOS_6(C:\)	250	188	75	100

Threshold Setting

Current Threshold(%) 98

New Threshold(%)

To change the threshold setting of the selected file system, click the up and down button to increase or decrease the percentage of utilization, or type the desired value, and click **Set**.

To set the threshold value for all of the file systems on the same server, type the threshold value, and click **Set All**.

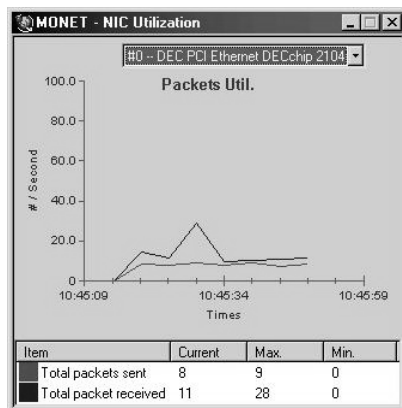


Note: If the password is enabled in the ASM Pro System Agent, enter the password for the Agent when changing the threshold setting.

NIC (Network Interface Card) utilization (for server system only)

Select **Server Information > Performance > NIC** to access the NIC Utilization information screen.

The NIC Utilization window shows the selected NIC card packet transactions on the selected system. The window below shows current receive and transmit transactions (bytes and packets) of NICs on selected servers.



This information is useful for determining the network traffic in the periods that the agent is at its peak.

NIC (Network Interface Card) fault

Select **Server Information > Performance > NIC Fault** to access the NIC card failure information screen.

This tab shows the number of instances of different faults in the selected Network Interface Card.

The screenshot shows a window titled "MONET - Storage Information". At the top, there is a dropdown menu showing "#0 -- DEC PCI Ethernet DECchip 21041". Below this, there is a tab labeled "Info". The main area of the window contains two columns of statistics, each with a label and a text input field showing a value.

Frame Transmit Error	275	Transmit heart beat	0
Frame receive error	157	CPS lost	0
Frame receive CRC error	0	Transmit late collision	1
Receive frame alignment error	0		
Transmit OK one collision	273748		
Transmit OK more collision	282488		
Transmit OK deferred	122793		
Transmit fail max collision	274		
Receive error overrun	2684768506		
Transmit error underrun	0		

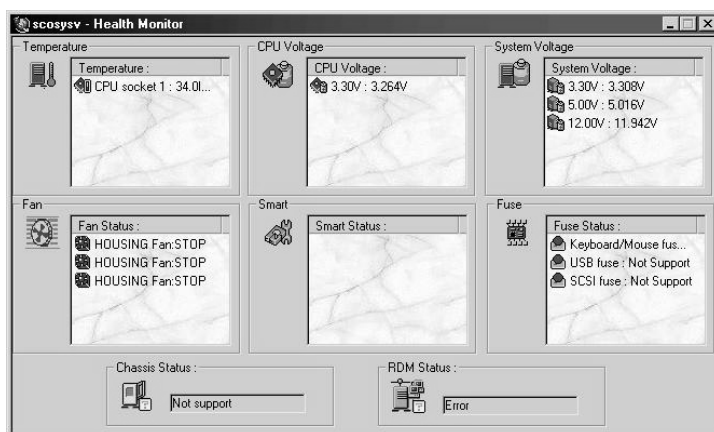
To view a particular network card, click the arrow button of the NIC# combo box and select a network card from the list.

Hardware status

The following sections describe the Information menu options that display when a desktop or server hardware service is selected in the System Listing window.

Health monitor

Select **Hardware Status > Health Monitor** to display the Health Monitor screen. This screen displays the current CPU voltage, CPU temperature, system voltage, fan status, SMART (Self-Monitoring, Analysis and Reporting Technology) status, RDM (Remote Diagnostic Management) status, and chassis status.



ASM Pro Console updates the values in the Health Monitor screen during each polling cycle. The polling intervals can be in the range of 1 to 60 seconds. Refer to “Configuring polling interval” on page 92 for more information.

Some of the threshold values for hardware components have been preset by the manufacturer and are not user configurable. When a threshold is exceeded, the action predefined by the system administrator is used to correct the problem. Refer to “Chapter 4 - System Alert Manager” for more information.



Caution: The events described in the following sections that generate alerts are critical. If any of them occur, correct the problem immediately. If the problem is not corrected, your system may be damaged.

CPU voltage

The voltage for each CPU's power source is shown here. The icon appears green when the voltage is within the normal range. The icon turns red when the voltage is not within this range. An alert is generated whenever the voltage is out of range. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.

CPU temperature

The CPU temperature is monitored in two stages. First, Console sends a warning when the temperature rises above a specified threshold. If the temperature continues to rise above a second, critical threshold, then a critical alert is issued. In some models, you can set the threshold values in the BIOS setup.

System voltage

The system power sources are shown here. The icon appears green when the voltage is within the proper range. The icon turns red when the voltage is not within this range. An alert is generated whenever the voltage is out of range. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.

Fan status

The fan status is monitored through the hardware module of the system. There is no user configurable setting.. If either the housing fan or the CPU fan stops, it will cause the temperature to rise, and could overheat the system.

Each fan is represented by a picture of a fan to the left of the fan name. The icon appears green when a fan is functioning properly. The icon turns red when the fan is not working. An alert is generated whenever a fan is not working. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.

SMART (Self-Monitoring, Analysis and Reporting Technology) status

SMART monitors a disk drive's health and reports potential problems to prevent impending disk crashes in your system. If this technology is available to the system, it can report disk error status to Console. If the system doesn't support this feature, the status is disabled. An alert is generated whenever a disk error occurs in the system. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.

Chassis status

The chassis status is monitored through the hardware module of the system. No user configurable setting exists. If the server can detect chassis status, the status is normal if the cover is closed or abnormal if the cover is open. If the system doesn't have chassis status detecting capability, the status indicates that it is "not supported." An alert is

generated whenever the chassis is opened and the system is not properly shut down. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.



.....

Note: The above events are critical. If any of the above events occurs, correct the problem right away. Damage to your system may result if the problem is left unattended.

Fuse (for server system only)

The fuse status is monitored through the hardware module of the system. No user configurable setting exists. Each fuse is represented by a picture of a fuse to the left of the fuse name. The icon appears green when the fuse is functioning properly. The icon turns red when the fuse is not working. An alert is generated whenever the fuse malfunctions. This alert is recorded in the alert log file. Refer to “Event viewer” on page 143 for more information.

RDM status (for server system only)

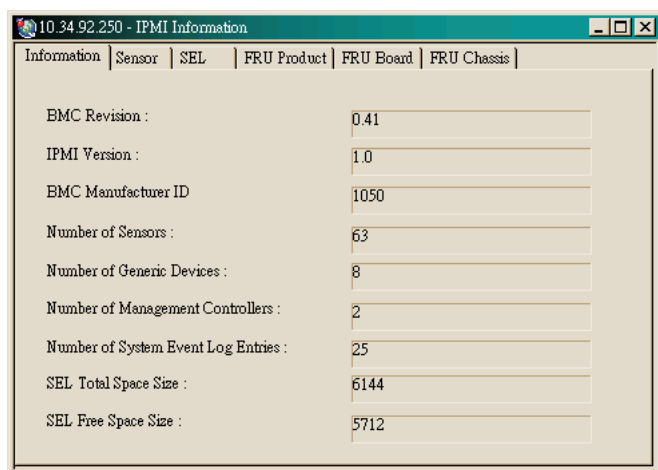
The RDM status is monitored through the hardware module of the server. If the server does not have RDM status detecting capability, the status is "Unknown." The status is "Active" if you have RDM installed in your systems. The status is "Not Exist" if your server does not have the RDM module installed.

IPMI (Intelligent Platform Management Interface)

Select **Information > Hardware Status > IPMI** to display the IPMI screen. The IPMI specifications define standardized, abstracted interfaces to platform management hardware. The IPMI screen consists of three tabs: Information, Sensor, and SEL (System Event Log).

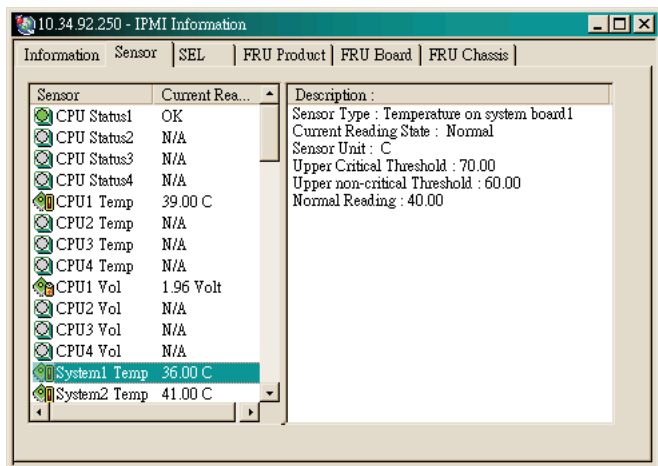
Information

The **Information** tab displays the IPMI version and other information concerning the sensors installed in the system and the system event log for these installations.



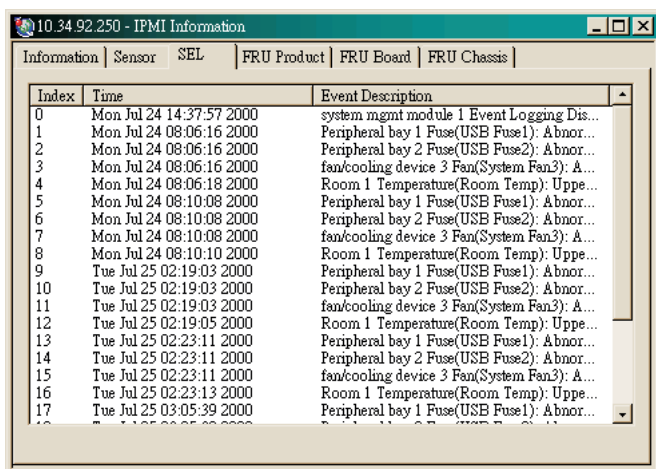
SensorFRU

The **Sensor** tab Shows sensor information in the system.



SEL (System Event Log)

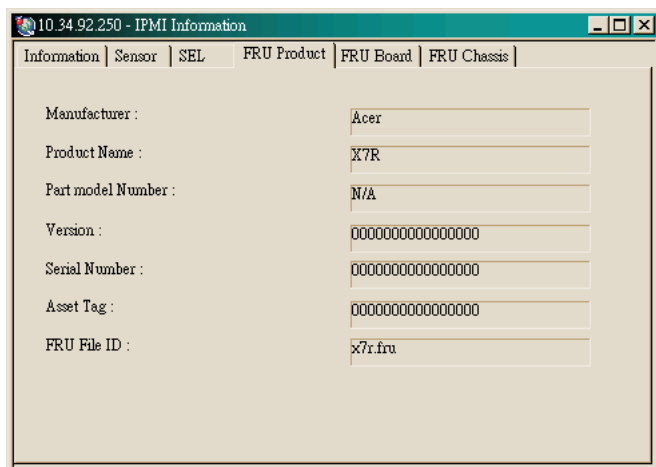
The **SEL** tab displays system event logs by time and event descriptions.



Index	Time	Event Description
0	Mon Jul 24 14:37:57 2000	system mgmt module 1 Event Logging Dis...
1	Mon Jul 24 08:06:16 2000	Peripheral bay 1 Fuse(USB Fuse1): Abnor...
2	Mon Jul 24 08:06:16 2000	Peripheral bay 2 Fuse(USB Fuse2): Abnor...
3	Mon Jul 24 08:06:16 2000	fan/cooling device 3 Fan(System Fan3): A...
4	Mon Jul 24 08:06:18 2000	Room 1 Temperature(Room Temp): Uppe...
5	Mon Jul 24 08:10:08 2000	Peripheral bay 1 Fuse(USB Fuse1): Abnor...
6	Mon Jul 24 08:10:08 2000	Peripheral bay 2 Fuse(USB Fuse2): Abnor...
7	Mon Jul 24 08:10:08 2000	fan/cooling device 3 Fan(System Fan3): A...
8	Mon Jul 24 08:10:10 2000	Room 1 Temperature(Room Temp): Uppe...
9	Tue Jul 25 02:19:03 2000	Peripheral bay 1 Fuse(USB Fuse1): Abnor...
10	Tue Jul 25 02:19:03 2000	Peripheral bay 2 Fuse(USB Fuse2): Abnor...
11	Tue Jul 25 02:19:03 2000	fan/cooling device 3 Fan(System Fan3): A...
12	Tue Jul 25 02:19:05 2000	Room 1 Temperature(Room Temp): Uppe...
13	Tue Jul 25 02:23:11 2000	Peripheral bay 1 Fuse(USB Fuse1): Abnor...
14	Tue Jul 25 02:23:11 2000	Peripheral bay 2 Fuse(USB Fuse2): Abnor...
15	Tue Jul 25 02:23:11 2000	fan/cooling device 3 Fan(System Fan3): A...
16	Tue Jul 25 02:23:13 2000	Room 1 Temperature(Room Temp): Uppe...
17	Tue Jul 25 03:05:39 2000	Peripheral bay 1 Fuse(USB Fuse1): Abnor...

FRU product

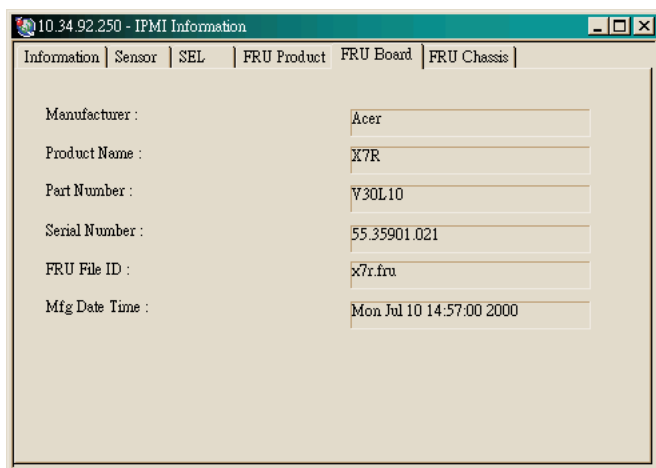
Field replaceable unit product displays product information.



Manufacturer :	Acer
Product Name :	X7R
Part model Number :	N/A
Version :	000000000000000000
Serial Number :	000000000000000000
Asset Tag :	000000000000000000
FRU File ID :	x7r.fru

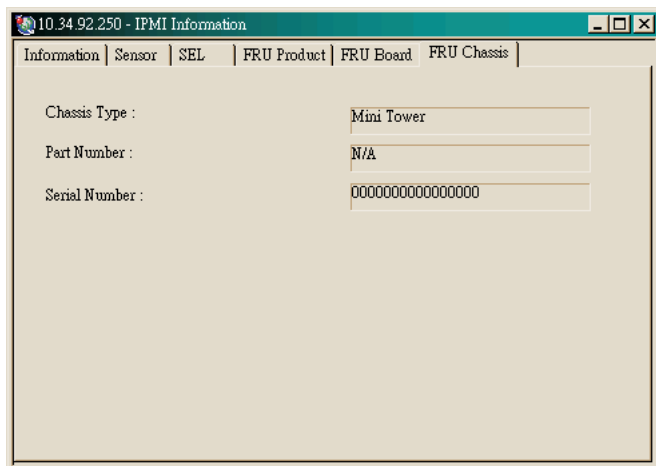
FRU board

Field replaceable unit board displays motherboard information.



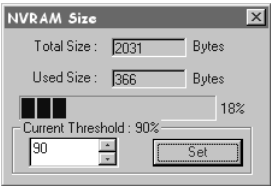
FRU chassis

Field replaceable unit chassis displays chassis information.



NVRAM

This button shows you the total amount of memory allocated for storing BIOS events in the RAM.



You can adjust the threshold setting by entering the percentage in the input box, and then click the **Set** button to accept the setting.

MIB-II information

This section describe MIB-II (Management Information Base) information. MIB-II is a database of objects that can be monitored by a network management system. If you have installed the MIB-II Agent software, you can view the information from ASM Pro Console.

The following sections describe the Information menu options that display when an MIB-II service is selected in the System Listing window.

System

Implementation of the system group is mandatory for all systems. If an agent is not configured to have a value for any of these variables, a string of length 0 is returned.

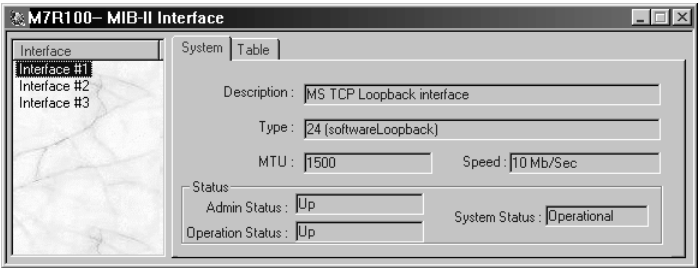


Parameter	Description
Description	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software
Object ID	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Jayson, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Ann Router'
Up Time	The time (in hundredths of a second) since the network management portion of the system was last re-initialized
Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person
Name	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name
Location	The physical location of this node (e.g., 'telephone closet, 3rd floor')
Services	The set of services that this entity primarily offers.

Interface

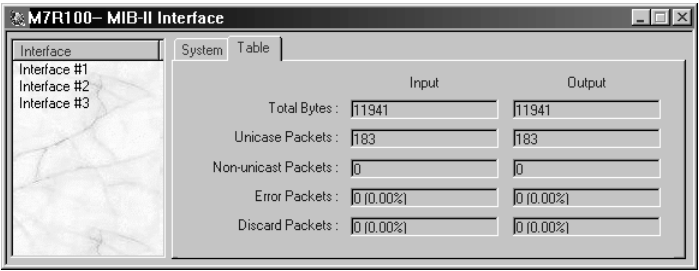
Implementation of the Interface group is mandatory for all systems.

System Tab



Parameter	Description
Description	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface
Type	The type of interface, distinguished according to the physical/link protocol(s) immediately 'below' the network layer in the protocol stack
MTU	The size of the largest datagram which can be sent/ received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface
Speed	The desired state of the interface. The testing (3) state indicates that no operational packets can be passed
Admin Status	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name
Operation Status	The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed
System Status	Indicates if the system is operational or not

Table tab

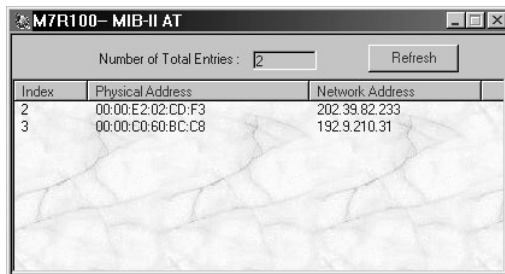


Parameter	Description
Input Total Bytes	The total number of octets received on the interface, including framing characters
Input Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol
Input Non-Unicast Packets	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol
Input Discard Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space
Input Error Packets	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Output Total Bytes	The total number of octets transmitted out of the interface, including framing characters
Output Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent

Parameter	Description
Output Non-Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent
Output Discard Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space
Output Error Packets	The number of outbound packets that could not be transmitted because of errors

AT (Address Translation)

Implementation of the Address Translation group is mandatory for all systems.



The screenshot shows a window titled "M7R100-MIB-II AT". Inside, there is a label "Number of Total Entries : 2" and a "Refresh" button. Below this is a table with three columns: "Index", "Physical Address", and "Network Address". The table contains two rows of data.

Index	Physical Address	Network Address
2	00:00:E2:02:CD:F3	202.39.82.233
3	00:00:C0:60:8C:C8	192.9.210.31

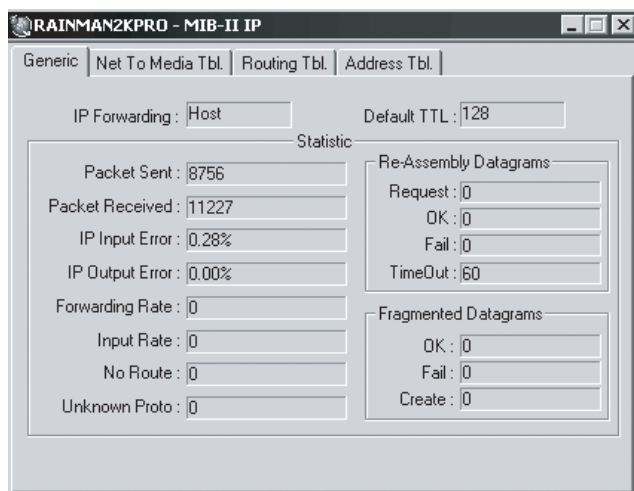
The Address Translation group contains one table which is the union across all interfaces of the translation tables for converting a NetworkAddress (e.g., an IP address) into a subnetwork-specific address. This document refers to such a subnetwork-specific address as a 'physical' address.

Parameter	Description
Physical Address	The media-dependent 'physical' address. This is usually an ethernet address that has been hardwired on the ethernet chip.
Network Address	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent 'physical' address

IP (Internet Protocol)

Implementation of the IP group is mandatory for all systems.

Generic tab



RAINMAN2KPRO - MIB-II IP

Generic | Net To Media Tbl. | Routing Tbl. | Address Tbl.

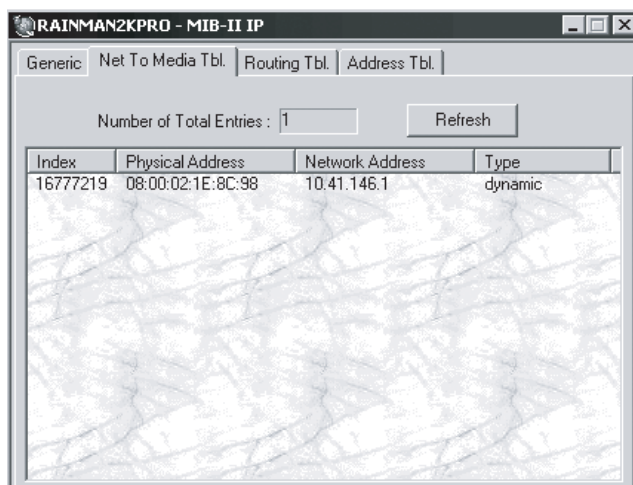
IP Forwarding : Host Default TTL : 128

Statistic

Packet Sent : 8756	Re-Assembly Datagrams
Packet Received : 11227	Request : 0
IP Input Error : 0.28%	OK : 0
IP Output Error : 0.00%	Fail : 0
Forwarding Rate : 0	TimeOut : 60
Input Rate : 0	Fragmented Datagrams
No Route : 0	OK : 0
Unknown Proto : 0	Fail : 0
	Create : 0

Net to media table tab

The IP address translation table contains the IP address and 'physical' address equivalents. Some interfaces do not use translation tables for address equivalents. DDN-X.25, for example, uses an algorithmic method. If all interfaces are of this type, then the Address Translation table is empty, i.e., has zero entries.



RAINMAN2KPRO - MIB-II IP

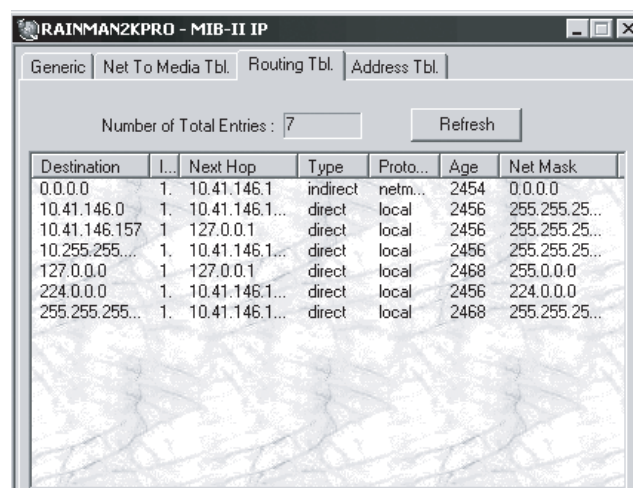
Generic | Net To Media Tbl. | Routing Tbl. | Address Tbl.

Number of Total Entries : 1

Index	Physical Address	Network Address	Type
16777219	08:00:02:1E:8C:98	10.41.146.1	dynamic

Routing table tab

The IP routing table contains an entry for each route presently known to this entity.



RAINMAN2KPRO - MIB-II IP

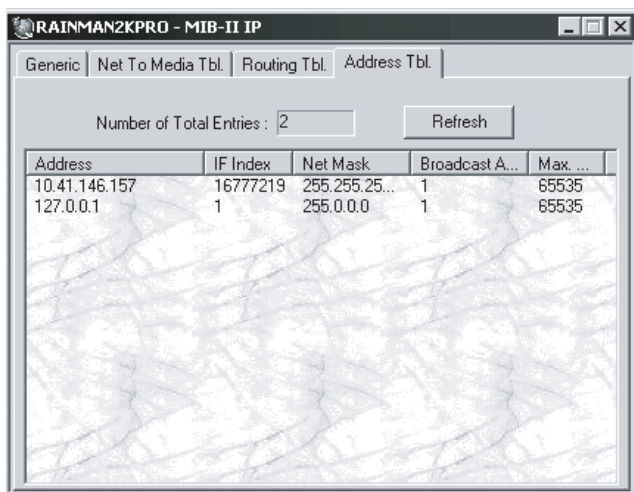
Generic | Net To Media Tbl. | Routing Tbl. | Address Tbl.

Number of Total Entries : 7

Destination	I...	Next Hop	Type	Proto...	Age	Net Mask
0.0.0.0	1.	10.41.146.1	indirect	netm...	2454	0.0.0.0
10.41.146.0	1.	10.41.146.1...	direct	local	2456	255.255.25...
10.41.146.157	1	127.0.0.1	direct	local	2456	255.255.25...
10.255.255...	1.	10.41.146.1...	direct	local	2456	255.255.25...
127.0.0.0	1	127.0.0.1	direct	local	2468	255.0.0.0
224.0.0.0	1.	10.41.146.1...	direct	local	2456	224.0.0.0
255.255.255...	1.	10.41.146.1...	direct	local	2468	255.255.25...

IP address table tab

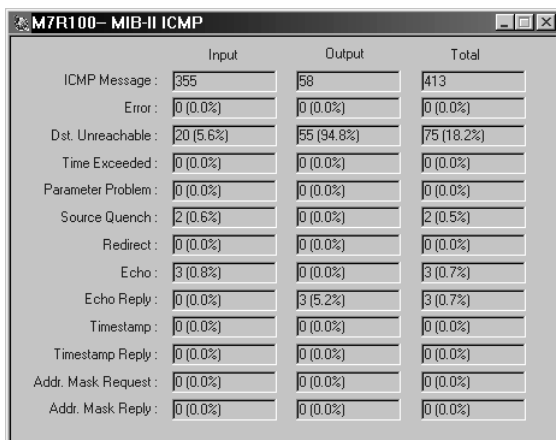
The IP address table contains this entity's IP addressing information.



Address	IF Index	Net Mask	Broadcast A...	Max. ...
10.41.146.157	16777219	255.255.255...	1	65535
127.0.0.1	1	255.0.0.0	1	65535

ICMP (Internet Control Message Protocol)

Implementation of the ICMP group is mandatory for all systems.



	Input	Output	Total
ICMP Message :	355	58	413
Error :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Dst. Unreachable :	20 (5.6%)	55 (94.8%)	75 (18.2%)
Time Exceeded :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Parameter Problem :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Source Quench :	2 (0.6%)	0 (0.0%)	2 (0.5%)
Redirect :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Echo :	3 (0.8%)	0 (0.0%)	3 (0.7%)
Echo Reply :	0 (0.0%)	3 (5.2%)	3 (0.7%)
Timestamp :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Timestamp Reply :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Addr. Mask Request :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Addr. Mask Reply :	0 (0.0%)	0 (0.0%)	0 (0.0%)

Parameter	Description
Input/Output Messages	The total number of messages which the entity received/sent. Note that this counter includes all those counted by InErrors.
Input/Output Errors	The number of messages which the entity received/sent but determined as having -specific errors (bad checksums, bad length, etc.).
Input/Output Dest Unreachables	The number of Destination Unreachable messages received/sent.
Input/Output Time Exceeds	The number of Time Exceeded messages received/sent.
Input/Output Parameter Problems	The number of Parameter Problem messages received/sent.
Input/Output Source Quenches	The number of Source Quench messages received/sent.
Input/Output Redirects	The number of Redirect messages received/sent.
Input/Output Echos	The number of Echo (request) messages received/sent.
Input/Output Echo Replies	The number of Echo Reply messages received/sent.
Input/Output Timestamps	The number of Timestamp (request) messages received/sent.
Input/Output Timestamp Replies	The number of Timestamp Reply messages received/sent.
Input/Output Addr Masks Requests	The number of Address Mask Request messages received/sent.
Input/Output Addr Mask Replies	The number of Address Mask Reply messages received/sent.

TCP (Transmission Control Protocol)

The TCP connection table contains information about the entity's existing TCP connections. TCP connection information lasts only as long as the connection.

Generic tab

The screenshot shows a configuration window titled "RAINMAN2KPRO - MIB-II TCP". It has two tabs: "Generic" and "Table", with "Generic" selected. The window contains several labeled input fields:

- Retrans. Alg.: vanj
- Retrans. timeout: 300 ms. < timeout < 240000 ms.
- Max. Conn.: Dynamic
- Current Conn.: 0
- Active Open: 28
- Passive Open: 27
- Received Seg.: 270
- Sent Seg.: 282

Parameter	Description
Retrans Alg	The algorithm used to determine the timeout value used for re-transmitting unacknowledged octets.
Retrans Timeout	Retrans Min - the minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. Retrans Max - the maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
Max Conn	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1

Parameter	Description
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state
Received Segments	The total number of segments received, including those received in error. This count includes segments received on currently established connections
Sent Segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets

Table tab

The TCP connection table contains information about this entity's existing TCP connections.

Status	Local Addr.	Local Port	Remote Addr.	Remote...
listen	0.0.0.0	111	0.0.0.0	10381
listen	0.0.0.0	135	0.0.0.0	43083
listen	0.0.0.0	445	0.0.0.0	59610
listen	0.0.0.0	1029	0.0.0.0	10298
listen	0.0.0.0	1032	0.0.0.0	26788
listen	0.0.0.0	1036	0.0.0.0	10283
listen	0.0.0.0	1047	0.0.0.0	2253
listen	0.0.0.0	1048	0.0.0.0	34867
listen	10.41.146.157	139	0.0.0.0	2144
timeWait	10.41.146.157	1065	10.41.146.193	139

Parameter	Description
Status	The state of this TCP connection
Remote Address	The remote IP address for this TCP connection
Remote port	The remote port number for this TCP connection
Local Address	The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used
Local Port	The local port number for this TCP connection

UDP (User Datagram Protocol)

The UDP listener table contains information about the entity's UDP end-points on which a local application is currently accepting datagrams.

Generic tab

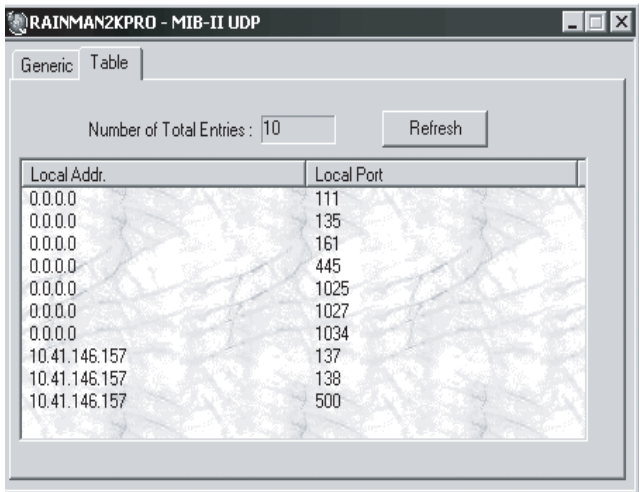
The screenshot shows a window titled "RAINMAN2KPRO - MIB-II UDP" with two tabs: "Generic" and "Table". The "Generic" tab is active and displays four statistics in a list box:

- Input Datagrams : 7196
- Output Datagrams : 5385
- Invalid Port : 1606
- Received Error : 0

Parameter	Description
Input Datagrams	The total number of UDP datagrams delivered to UDP users
Output Datagrams	The total number of UDP datagrams sent from this entity
Invalid Ports	The total number of received UDP datagrams for which there was no application at the destination port
Received Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port

Table tab

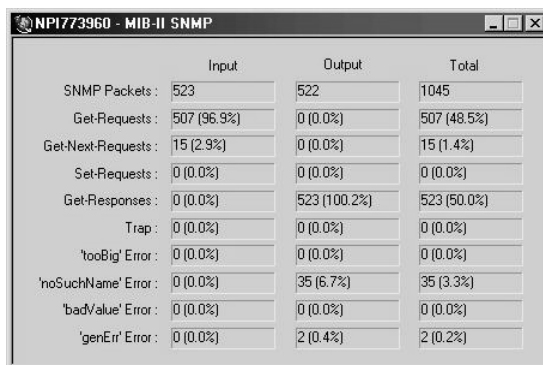
The UDP listener table contains information about this entity's UDP end-points on which a local application is currently accepting datagrams.



Parameter	Description
Local Address	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used
Local Port	The local port number for this UDP listener

SNMP (Simple Network Management Protocol)

Implementation of the SNMP group is mandatory for all systems that support a SNMP protocol entity. Some of the objects defined below are zero-valued in SNMP implementations that are optimized to support only those functions specific to either a management agent or a management station. The objects below refer to the SNMP entity, and there may be several SNMP entities residing on a managed node.



	Input	Output	Total
SNMP Packets :	523	522	1045
Get-Requests :	507 (96.9%)	0 (0.0%)	507 (48.5%)
Get-Next-Requests :	15 (2.9%)	0 (0.0%)	15 (1.4%)
Set-Requests :	0 (0.0%)	0 (0.0%)	0 (0.0%)
Get-Responses :	0 (0.0%)	523 (100.2%)	523 (50.0%)
Trap :	0 (0.0%)	0 (0.0%)	0 (0.0%)
'tooBig' Error :	0 (0.0%)	0 (0.0%)	0 (0.0%)
'noSuchName' Error :	0 (0.0%)	35 (6.7%)	35 (3.3%)
'badValue' Error :	0 (0.0%)	0 (0.0%)	0 (0.0%)
'genErr' Error :	0 (0.0%)	2 (0.4%)	2 (0.2%)

Parameter	Description
Input/Output packets	The total number of Messages delivered to the SNMP entity from the transport service
Input/Output Get-Requests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity
Input/Output Get-Next-Requests	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity
Input/Output Set-Requests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity
Input/Output Get-Responses	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity
Input/Output Traps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity
Input/Output TooBig Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'tooBig'

Parameter	Description
Input/Output NoSuchNames Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'noSuchName'
Input/Output BadValues Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'badValue'
Input/Output GenErr Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'genErr'

► Redundant power supply

This section describes the redundant power supply features are displayed when you select **Information > Hardware Status > Redundant Power Supply**.



.....

Important! Redundant power supplies are not available on all server models. If the devices are not present in the server, their options in the Information menu are grayed out.

The Redundant Power Supply window shows the current working condition of the redundant power supplies and their respective fans. When redundancy between power supplies has been interrupted, such as when one or both power supplies fail, or a fan stops working, a Fail status displays. If this happens, refer to this window to determine the cause of failure.

The color of each icon in the window indicates its status, as follows:

- Green means Normal
- Red means Fail
- Gray means Does Not Exist or Unknown



.....

Note: On Windows NT and NetWare systems that contain a redundant power supply, you can monitor and control the redundant power supply remotely via Console.

► Fault management

One of the most important functions of ASM Pro is fault management. This is done through the use of threshold settings and hardware error detection methods.

The ASM Pro System Agent performs two tasks when it encounters an error:

1. It sends an alert to SAM (System Alert Manager). See “SAM (System Alert Manager)” on page 131.
2. It handles the error condition based on the event handling method setup for the server. The event handling method is setup using the `asmconfig` utility.



.....

Note: The Broadcast Message checkbox must be checked before the Agent can broadcast error messages. Refer to “Event handling method” on page 149 for more information.

After the Console receives an alert from the Agent, the Console performs two tasks:

1. It logs the alert information into a log file. This log file may then be reviewed at a later time.
2. It bases the event handling on the method defined in System Alert Manager.

An event is something out of the ordinary that occurs on an agent, which, if left unattended, might cause data loss or hardware damage. An event occurs when a predefined threshold setting is exceeded, or when a hardware error occurs.

Threshold settings

All threshold settings are preset to the factory-recommended values. The following threshold values are user-configurable:

- PCI Bus Utilization (for some models only)
- Memory Utilization
- File System Utilization
- BIOS Event Log Utilization

All other threshold values are internally preset and cannot be changed. In some models, you can set the threshold values in the BIOS setup screen.

The threshold values are:

- Temperature warning
- Temperature critical
- Voltage exceeds safe range

See “Event types” on page 144 for the definition of each threshold.

An example of non-configurable threshold values is the internally-preset temperature warning and temperature critical. For example, the manufacturer-suggested threshold value for some types of Pentium processors is between 131°F - 167°F (55°C - 75°C). (131°F (55°C) is the temperature warning threshold; 167°F (75°C) is the temperature critical threshold. ASM Pro reads and checks the manufacturer's preset temperature warning and temperature critical range whenever this type of Pentium processor is detected.

Hardware errors

The following hardware errors are preset by the manufacturer and cannot be changed:

- ECC memory error
- Fan stoppage
- UPS related errors (power supply, AC power, power supply fan) (applies only to certain systems)
- Redundant Power Supply related errors (power supply, power supply fan) (applies only to certain systems)
- Fuse fail (applies only to certain systems)
- Chassis open (applies only to certain systems)
- SMART error (for systems that have a SMART drive installed)

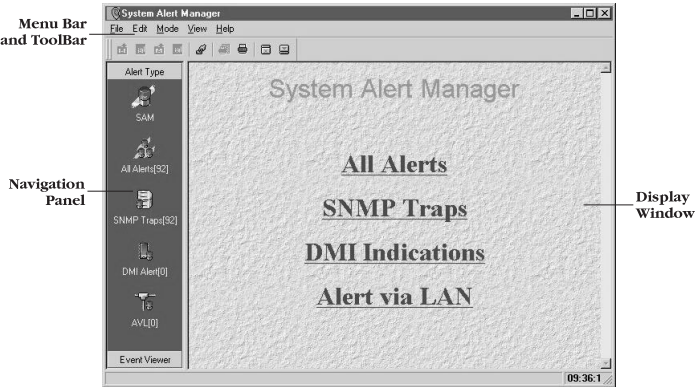
See “Hardware status” on page 100 for more information about system health monitoring.

4 System Alert Manager (SAM)

System Alert Manager is a utility that runs in the background of your Console system every time you bootup. It actively monitors the systems in a network for faults and malfunctions and warns you if they occur. It also includes an event viewer that allows you to view the event logs of networked systems.






► SAM user interface

The following figure illustrates the SAM user interface window.



The toolbar, located at the top of the SAM window, contains the toolbar buttons. The toolbar buttons allow quick access to selected SAM functions via a single mouse click. You can also access these functions from the menu bar.

Icon	Description
	Load Alert. Displays the previously saved alert file
	Save Alert. Saves alert log information to disk
	Import File. Allows you to view other alert files (ASCII type only) created by other programs
	Export File. Allows you to save alert files in a text format that other programs can read

Icon	Description
	Event Handler. Accesses the Event Handler screen
	Print Preview. Shows the format display before printing
	Print. Prints event log lists
	Shutdown. Unloads SAM from the system
	Close Window. Minimizes the SAM window to the Windows taskbar

The navigation panel has two parts: Alert Type and Event Viewer. The Alert Type panel shows the alert type icons. The Event Viewer panel shows the monitored system's host name and addresses. Click the title bar to switch between these panels.

► Viewing system alert

When a hardware error occurs or a threshold setting is exceeded, the ASM Pro Agent detects the condition and sends an alert to inform the Console. When the Console receives the alert, it logs the event in the Alert Log file.

There are three types of alerts associated with the Console:

- SNMP Traps
- DMI Indications
- Alert via LAN

To view the alert log of a specific type, click its respective icon on the navigation panel.

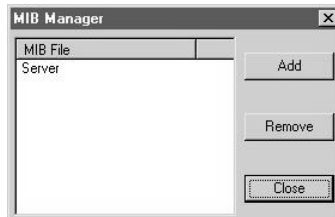
SNMP traps

SNMP traps are generated by systems that use the SNMP (Simple Network Management Protocol) to report devices that are not working properly. To view SNMP traps, select **View > SNMP** or click the **SNMP** icon in the navigation panel. The SNMP trap log displays.

Alert Type	Index	Time	Host	Address	Type	Description
SNMP Traps[11]	11	04/27/1999 13:32:50	210.63.101.253	210.63.101.253	0	SCD TCP/IP Runtime Release 2.0.0
	12	04/27/1999 13:33:18	210.63.101.253	210.63.101.253	0	SCD TCP/IP Runtime Release 2.0.0
	13	04/27/1999 15:01:33	210.63.101.253	210.63.101.253	0	SCD TCP/IP Runtime Release 2.0.0
	14	04/27/1999 15:01:34	210.63.101.253	210.63.101.253	5	Fan Stops
	15	04/27/1999 15:01:34	210.63.101.253	210.63.101.253	5	Fan Stops
	16	04/27/1999 15:01:34	210.63.101.253	210.63.101.253	5	Fan Stops
	17	04/27/1999 15:01:34	210.63.101.253	210.63.101.253	5	Fan Stops
	18	04/27/1999 15:01:34	210.63.101.253	210.63.101.253	8	BUS Utilization High
	19	04/27/1999 15:01:36	210.63.101.253	210.63.101.253	5	Fan Stops
	20	04/27/1999 15:01:38	210.63.101.253	210.63.101.253	5	Fan Stops
	21	04/27/1999 15:01:40	210.63.101.253	210.63.101.253	5	Fan Stops

Item	Description
Index	Index number that is assigned to the event
Time	Actual time when the error occurred
Host	Name of the system where the error occurred
Address	Network address of the system
Type	Type of error that occurred
Description	Description of the error

SNMP Traps also contains a MIB Manager that allows you to add or remove customized trap definitions for SAM. To access the MIB Manager, select **SNMP > MIB Manager** on the menu bar. The MIB Manager window appears.



SAM supports server SNMP trap definitions. If you have a third party device that supports MIB files, you can add this to the database and configure the action for each trap type.

To add a new trap definition file to SAM, click the **Add** button and select the file you want to include in the list.

To remove a trap definition file, select the file and click the **Remove** button.



.....

Note: Add the trap definition to SAM, using the procedures above, to receive some traps for the specific devices you use.

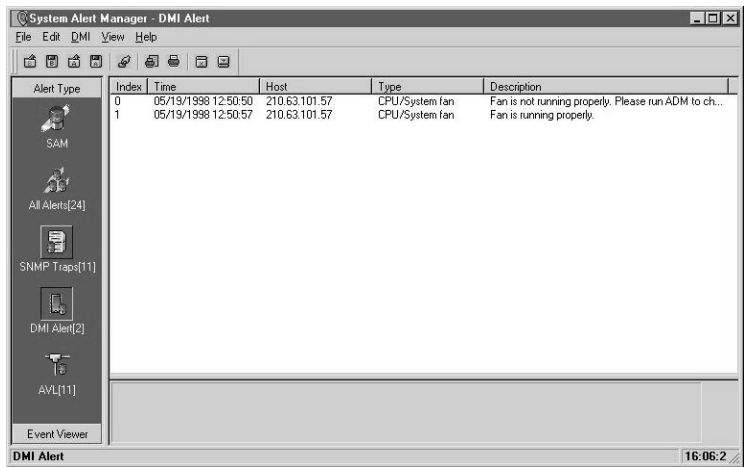
Trap types for server systems

The following event types are listed in the Event Handler window.

Type.	Description
0	Trap Other than ASM Pro
1	Temperature Warning
2	Temperature Critical
3	1-Bit ECC Memory Error
4	M-Bit ECC Memory Error
5	Fan Stops
6	Voltage Exceeds Safe Range
8	Bus Utilization High (applies only to certain systems)
9	Memory Utilization High
10	File System Utilization High
11	NIC Counter Threshold Exceeded
The following traps apply only to certain system models	
16	Chassis Intrusion
17	Fuse Fail
18	Redundant Power Supply Fail
19	Redundant Power Supply Fan Fail
20	BIOS Event Log
21	BIOS Event Log Utilization High
22	CPU Abnormal
23	Asset Change

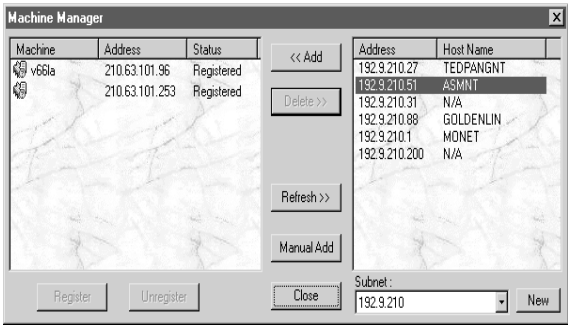
DMI indications

DMI indications are generated by systems that use DMI (Desktop Management Interface) to report devices that are not working properly. To view DMI alerts, select **View > DMI** or click the **DMI** icon in the navigation panel. The DMI indication log displays.



Item	Description
Index	Index number that is assigned to the event
Time	Actual time when the error occurred
Host	Name of the host system where the error occurred
Type	Network address of the system
Description	Description of the error

DMI Alert also includes a Machine Manager that allows you to choose which systems to view. To access the Machine Manager, select **DMI > Machine Manager** on the menu bar. The Machine Manager window appears.



The systems that you can view are listed in the Machine Manager window. However, they must be registered to the service provider before you can access the log files.



.....

Note: SAM registers the system automatically if it is added to the System Listing window in Console. If the system is removed from the System Listing, it becomes unregistered.

To add a system, select a system on the right panel and click the **<<Add** button. The system you selected appears in the left panel.

The subnet drop-down menu lists all the available subnets in the System Listing. If you want to view a new subnet, click the **New** button and type the subnet you want. If the subnet is valid, the systems located in that subnet are displayed on the right panel.

To register a system, select a system on the left panel and click **Register**. The default status of the system is Not Registered. SAM register the systems automatically.



.....

Note: You can register and unregister the systems any time.

To unregister a system, select the system you want to unregister and click the **Unregister** button.

To remove a system from the Machine Manager, select the system you want to remove and then click the **Delete>>** button. The system you deleted appears on the right panel.

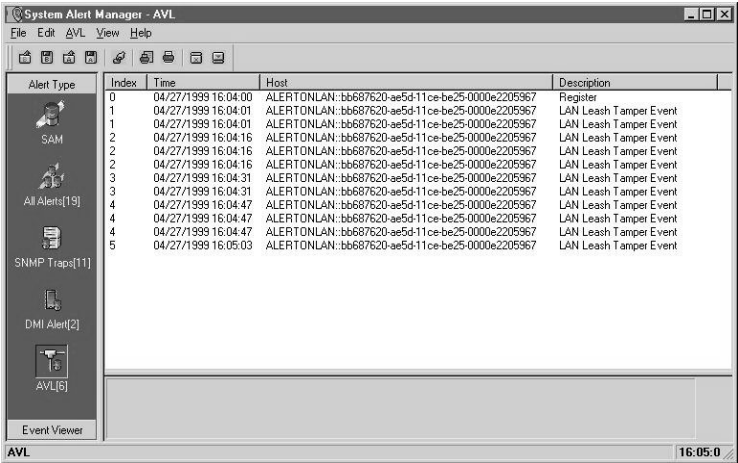
DMI indication types

The following indication types are listed in the Event Handler window. Each of these indications have three states: normal, warning, and critical.

Indication	Alerts when..
Voltage	Voltage exceeds safety range
Virtual Memory	Virtual memory utilization exceeds the intended value
CPU Temperature	CPU temperature exceeds the threshold setting
GDI Resources	Graphical Device Interface utilization exceeds resource limit
CPU/System Fan	CPU stops working or the system fan stops rotating
Logical Drive	Occurs when file system utilization exceeds warning or critical threshold
SMART Drive	Disk error occurs in the system
Asset	System device has been added, removed, or changed

Alert via LAN (Local Area Network)

The Alert via LAN (Local Area Network) function allows administrators to monitor and reconfigure local systems through a network. Even if a system is turned off, it can still report its status to the administrator.



Item	Description
Index	Index number assigned to the event
Time	Actual time when an error occurred
Host	Name of the host system where the error occurred
Description	Description of the error

AVL alert types

The following alert types are listed in the Event Handler window.

Alert Type	Alerts when..
Cover Tamper	System chassis is open
Voltage Event/Fan/Temp	System voltage exceeds safety range
LAN Leash Tamper	Network cable is disconnected from the system
Processor Missing	No CPU is available in the system

Alert Type	Alerts when..
Watchdog Event	A software hang occurred
Software Event	Software failure to the system

Saving and loading system alert log files

You can save the log for future reference by clicking the **Save Alert** button. SAM saves the file to the local hard drive. Click the **Load Alert** button to view these files in the future.

You can also save the log to a plain text file or binary file by selecting **File > Export File** or by clicking the **Export File** button and saving it as text or binary.

You can view previously saved log files from other programs by selecting **File > Import File** or by clicking the **Import File** button. You can only import ASCII type files.

► Event viewer

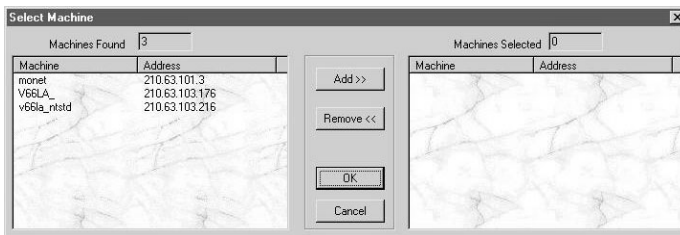
Event Viewer gathers information about events in the system being monitored by the ASM Pro Console. This information is saved in the event log file for future reference.

Saving and loading event log file

You can save the event log for future reference by clicking the **Save Event Log** button. Event Viewer saves the file with a .evt extension. Click the **Load Event Log** button to view these files. You can also save the event log to a plain text file by selecting the command from the File menu.

Retrieving multiple event log information

To retrieve multiple events, click the **Retrieve Multiple Events** button. The Select System window displays:



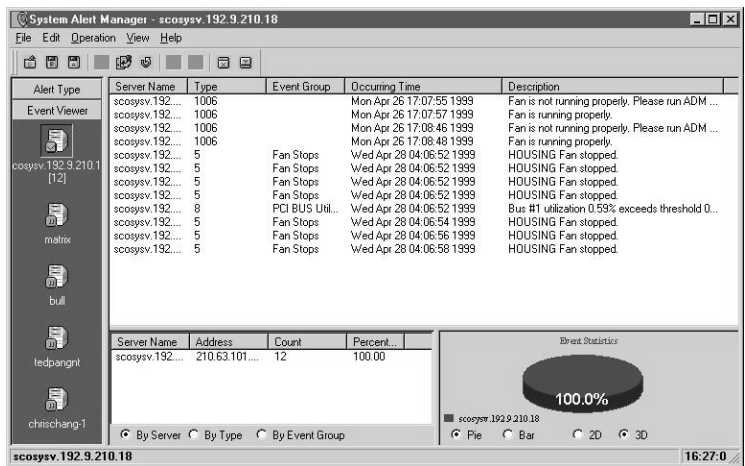
Event Viewer searches for available systems and lists them in the Systems Found category. Click on the systems you want to view and then click **Add>>** to collect event information about the systems you have selected.

To remove a system from the Systems Selected category:

1. Click on the system you want to remove and click the **Remove<<** button.
2. Click **OK** to verify and exit the Select System window. Event Viewer starts retrieving data from the systems.

Displaying single event log information

In the Event Viewer navigation panel, click on a system to display the Event List window. The Event List window displays events from the system being monitored. The upper window shows the system name, type of event group, event group name, time occurred, and a brief description of the event.



The lower window shows a summary of events by event group type and a graphic presentation of those events. You can change these displays by clicking on the radio buttons below them.

Event types

When an event occurs in a system agent, the Agent sends a trap (interrupt signal) to the Console. An exceeded threshold value, whether user-configurable or internally preset, will cause Agent to send a trap. It also sends a trap when it detects a hardware error.

The following table describes the types of events that are trapped by Agent, and lists the actions taken by Agent and Console. Possible solutions to the problems are also offered.

The first part of the table lists the types of events that can be trapped and managed on all server models. The second part lists those that are only available on certain models.

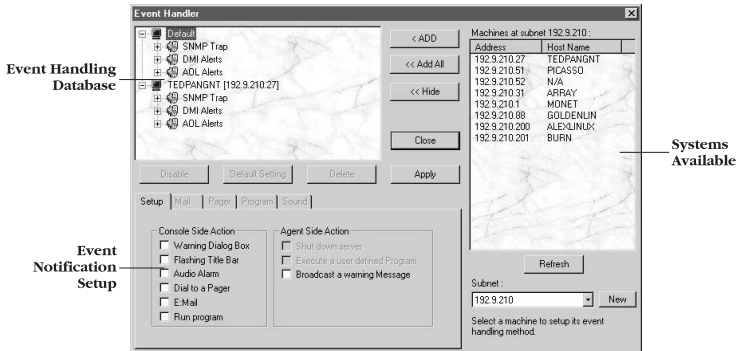
Event Type	Description
Trap Other Than ASM Pro	When trap that is not listed in the ASM Pro event-type listing occurs, ASM Pro Agent sends a trap to Console
System Up/Down	<p>The server has been booted or shut down. Agent sends a trap to Console every time this occurs. Console notifies the system administrator by the method selected in the Console Side Action section of the Event Notification Setup screen</p>
Temperature Warning	<p>The processor temperature has exceeded the first threshold setting. A typical default threshold setting is 131°F (55°C).</p> <p>Agent broadcasts a “Temperature Warning” message to all users on the server.</p> <p>Agent also sends a “Temperature Warning” event trap signal to Console, who handles the event by the method selected in the Console Side Action section of the Event Notification Setup screen.</p> <p>Agent sends a trap every minute thereafter as long as the temperature remains above the threshold. Console records each of these traps in the event log file.</p> <p>Note: You can check the processor temperature by clicking the Hardware Environment toolbar button in Console</p>
Temperature Critical	<p>The processor temperature has exceeded the second threshold setting. A typical default threshold setting is 167°F (75°C). This value is not user-configurable.</p> <p>Agent sends a broadcast and a trap, after which it shuts down the server to prevent loss of data and possible damage to the hardware. Although not recommended, Agent can be configured to disable the auto-shutdown feature. Refer to “Chapter 5 - ASM Pro Server Agent Utilities” for more information.</p> <p>Note: You can check the processor temperature by clicking the Hardware Environment toolbar button in Console</p>

Event Type	Description
ECC Memory Error	<p>A single-bit or multi-bit ECC memory error has been detected.</p> <p>Agent sends a broadcast and a trap.</p> <p>Users should immediately back up their data files.</p> <p>Caution: The faulty memory module(s) should be replaced immediately to protect data integrity. Refer to your system's service guide for memory module recommendations</p>
Fan Stops	<p>A system fan has stopped rotating.</p> <p>Agent sends a broadcast and a trap.</p> <p>Replace the defective fan to ensure that the server stays within its heat tolerances.</p> <p>Note: You can verify whether the fan is functioning by clicking the Hardware Environment toolbar button in Console</p>
Voltage Exceeds Safe Range	<p>The voltage reading has exceeded the safe operating range.</p> <p>Agent sends a broadcast and a trap.</p> <p>Note: You can check the voltage by clicking the Hardware Environment toolbar button in Console</p>
Memory Utilization High	<p>Memory utilization has exceeded the threshold setting.</p> <p>Agent sends a trap.</p> <p>Add more memory to the server if possible. Refer to your system's service guide for memory module recommendations</p>
File System/Volume Utilization High	<p>File system utilization has exceeded the threshold setting.</p> <p>Agent sends a broadcast and a trap.</p> <p>Perform maintenance on the disk(s). Add another hard drive if the threshold is still exceeded after performing disk maintenance</p>

Event Type	Description
The following are event types that apply only to certain server models	
Bus Utilization High	<p>PCI bus utilization has exceeded the threshold setting.</p> <p>Agent sends a trap.</p> <p>Rearrange your PCI add-in components to even out bandwidth distribution, if possible</p>
AC Power Fails	<p>AC power to the server has failed.</p> <p>Agent sends a broadcast and a trap, then shuts down the server</p>
Chassis Intrusion	<p>The server cover is open.</p> <p>Agent sends a broadcast and a trap</p>
Fuse Fail	<p>The keyboard/mouse, USB, or SCSI fuse has failed.</p> <p>Agent sends a broadcast and a trap</p>
Redundant Power Supply Fail	<p>The server's redundant power supply has failed.</p> <p>Agent sends a broadcast and a trap</p>
Redundant Power Supply Fan Fail	<p>The server's redundant power supply fan has failed.</p> <p>Agent sends a trap.</p> <p>How Console handles the trap is determined by the event notification method selected by the system administrator in the Event Notification Setup screen</p>
BIOS Event Log	<p>The BIOS has detected hardware and has saved the information to its event log in NVRAM.</p> <p>Agent sends a trap</p>
BIOS Event Log High	<p>BIOS Event Log utilization has exceeded the threshold setting.</p> <p>Agent sends a trap</p>
CPU Abnormal	<p>The BIOS has detected an internal CPU error.</p> <p>Agent sends a trap</p>
Asset Change	<p>An asset has changed, for example, a disk has been added, removed, or replaced.</p> <p>Agent sends a trap</p>

► Event handler setup

Select **View > Event Handler** or click the **Event Handler** button on the menu bar to access the Event Handler screen. Event notification applies to certain systems that you specify.



The default alert definitions consist of three types: SNMP traps, DMI indication, and AVL alerts. The default event handling actions are defined for all alerts received by SAM, but you can set some specific event handling actions for some systems by creating a new database for that system.

To create a new database entry:

1. Click the **Show>>** to open the System Select view located on the right side of the window.
2. Choose an existing subnet, or create a new subnet by clicking the **New** button.
3. Click the **Refresh** button to show all the systems in this subnet.
4. Select a system in the systems available window and then click **<Add**. If you want to add all the systems in the window click **<<Add All**. The systems you specified appear in the database list.

To assign event notification to a specific trap or alert:

1. Select a trap or alert under the alert definition in the database list.
2. Use your mouse pointer to check the various boxes in the event notification setup tabs. Refer to the next section for more information about these functions.

To assign event notification to the alert definitions (whole subnode):

1. Select an alert definition in the database list.
2. Check the various boxes in the event notification setup tabs. Refer to the next section for more information about these functions.

This action automatically activates the event notification you selected to all the traps defined under that alert definition.

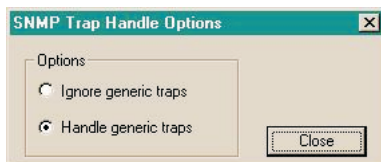
3. Click **Close** to save the changes.

To remove a system from the database list, select the system you want to remove and click the **Delete** button.

To disable the event notification function for a system, select the system you want to disable, and click the **Disable** button. Disabling the assigned event notification function of a system forces it to adopt the default setting.

To reset the default value of the system's notification, select the system you want to reset and then click the **Default Setting** button.

For SNMP traps, users can decide to receive the traps which are defined in SAM or not. If the user choose to handle generic traps, SAM will interpret the message according to the varbind list of SNMP trap packet.



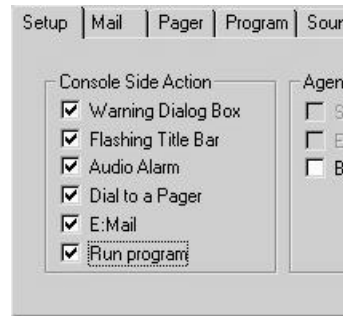
.....

Note: When the checkbox in the Agent Side Action frame is grayed out it indicates that you can only enable this action at the agent side.

Event handling method

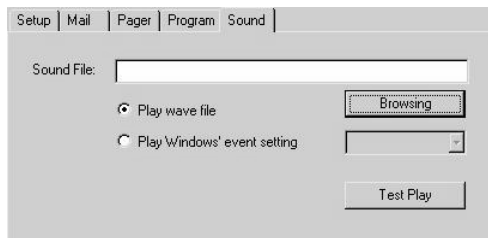
The following list describes the event handling methods and the function of each method. You can check and uncheck as many of these boxes as desired. A check in the box enables the function; removing a check disables the function. Use your mouse pointer to check and uncheck these boxes.

When you open the Event Handler window, you see a list of event notification methods in the Console Side Action box. Checking an event notification method causes the ASM Pro Console to take the action indicated in the checkbox.



Console side action

- The Warning Dialog Box appears on the ASM Pro Console screen when the ASM Pro System Agent sends a trap to the Console.
- The Flash Title Bar flashes on and off when the ASM Pro System Console receives a trap.
- The Audio Alarm makes a sound whenever a trap is received from the ASM Pro System Agent. You need to set up the sound file before you select “Audio Alarm”. You can change the sound the system makes by changing the sound file in the Sound File edit box. Select the **Sound** tab. The following display appears:



When you click on the **Browse** button, you see the Open Sound File screen. You can choose a specified sound file to edit. The sound can be tested by clicking on the **Test Play** button.

If you choose to play a windows event setting, click the bullet button and choose a theme from the pull-down menu.



Note: Select the sound file tab to set up a sound file before marking the "audio alarm" trap action. You must have a sound card for the sound file to work.

- The Dial to a Pager sends a call to a pager when the ASM Pro System Agent sends a trap to the Console. Select the **Pager** tab from the Event Handler screen. The following display appears:



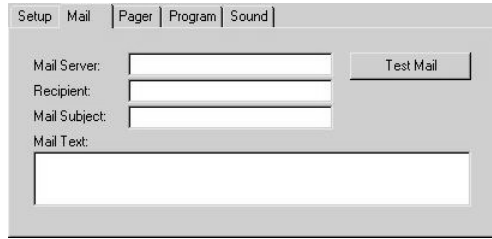
Note: Select the pager tab to set up a pager before marking the "Dial to a pager" trap action.

Enter the pager number in the Pager Number box and a message in the Message box. Enter the modem port in the COM Port box for dialing out from the Console. The pager can be tested by clicking on the **Test Pager** button.



Note: Set up and configure Microsoft Exchange before you use the Mail function. For more information on Microsoft Exchange, refer to your Microsoft Exchange User's Manual.

- E:Mail - the ASM Pro Console sends an email when the ASM Pro System Agent sends a trap to the Console. Select the **E:Mail** tab from the Event Handler screen. Fill out the information in the display. Email can be tested by clicking on the **Test Mail** button.



The screenshot shows the 'Mail' tab selected in the 'Setup' window. The window has tabs for 'Setup', 'Mail', 'Pager', 'Program', and 'Sound'. The 'Mail' tab contains the following fields and buttons:

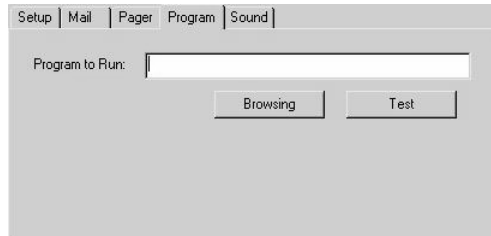
- Mail Server: [Text Field]
- Recipient: [Text Field]
- Mail Subject: [Text Field]
- Mail Text: [Text Area]
- Test Mail: [Button]



.....

Note: Select the **E:Mail** tab to set up email information, before marking the "E:Mail" action.

- Run Program - executes the program when an event occurs. To enter the Program to Run display, select the **Program** tab from the Event Handler screen.



The screenshot shows the 'Program' tab selected in the 'Setup' window. The window has tabs for 'Setup', 'Mail', 'Pager', 'Program', and 'Sound'. The 'Program' tab contains the following fields and buttons:

- Program to Run: [Text Field]
- Browsing: [Button]
- Test: [Button]

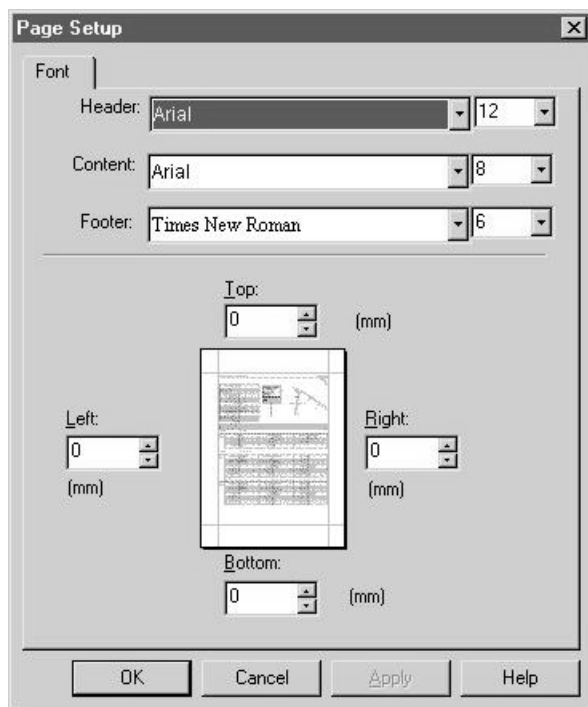


.....

Note: Set up and configure Microsoft Exchange before you use the Fax and Mail function. For more information on Microsoft Exchange, refer to your Microsoft Exchange User's Manual.

► Page setup for printing

Select **File > Page Setup** to access the Page Setup window. This allows you to change the header, contents, and footer fonts and font size when printing out information. You can also adjust the top, bottom, left, and right margins on the paper.



5 ASM Pro Server Agent utilities

This chapter describes the ASM Pro configuration utilities for Agents that run under SCO OpenServer, SCO UnixWare, Windows NT, NetWare and Linux.

The configuration utility for each operating system allows you to:

- Enable, disable, or change the ASM Pro Agent password.
- Change Agent event-handling action.
- Add, change, and delete the ASM Pro Console name or IP addresses.



.....
Warning! To report events, the ASM Pro Agent must know the IP address of the ASM Pro Console. Be sure to use the correct agent configuration utility to enter the Console IP address.

ASM Pro requires a password for the ASM Pro Console and for each server agent. To launch the ASM Pro console program, you need an ASM Pro console password. To protect the server agent data, you need a separate password for each agent.

► asmconfig for SCO OpenServer

asmconfig is invoked during ASM Pro Server Agent installation to set up the agent password. It may be invoked at any time by typing asmconfig from a UNIX shell prompt. The executable file is found in the /usr/bin directory.

```
SNMP_Config Manager_info Event_Action Password Threshold Event_Log Quit
```

Password:****

```
Configure /etc/snmpd.trap for SNMP/SMUX
```

Working in asmconfig:

- Use the right and left arrow keys to select a menu item.
- Use the up and down arrow keys to highlight the item and press the return key to execute or select the highlighted item.
- Use the left and right arrow keys to switch control between the main window and confirm selection window shown at the bottom of the screen.
- To quit, select Quit from the main menu and press Enter.

SNMP config

This function allows you to add, change, or delete any IP address in /etc/snmpd.trap. When you want the ASM Pro Console to monitor the ASM Pro Server Agent, the Console's IP address must be included in /etc/snmpd.trap on the server site.

In the following screen example, ASM Pro agent sent event traps for three monitoring systems: 192.9.210.27, 192.9.210.99, and 202.39.85.64.

SNMP_Config Manager_info Event_Action Password Threshold Event_Log Quit

public	192.9.210.27	162
public	192.9.210.99	162
public	202.39.85.64	162

[Add]

[Modify]

[Delete]

[Cancel]

Manager information

Modify Manager Contact Information and Server Location by selecting this function. You can also view and change manager information from the ASM Pro Console by entering **Server Information > Basic Information** window.

Instructions about editing data appear on the status line at the bottom of the screen. Press the **Enter** key to move the cursor to the next line. When you finish typing, press **Enter** and the arrow key to return to the menu item.

SNMP_Config **Manager_info** Event_Action Password Threshold Event_Log Quit

Manager Name :
Office Phone :
Office Location :
Home Phone :
Home Location :
Pager Number :
E-mail Address :
Server Location :

Use arrow key and edit.....

Event action

One of the most important functions performed by ASM Pro is event trapping and handling. This is done through the use of threshold settings, hardware error-detection methods, and fault management. When an “event” occurs, Agent performs the event action and sends a trap to Console. It uses the IP address specified in SNMP Config to send the trap to the ASM Pro Console.

This function allows you to specify the type of action that ASM Pro Agent takes when an event occurs. The ASM Pro events that Agent traps are predefined in the ASM Pro software. You can use the Event_Action function to define agent actions performed on the agent system. After ASM Pro Console receives the trap it takes the action defined by the System Alert Manager or ASM Pro Console Setup event handler. You can also use the related Threshold function, described later, to change some of the threshold settings. For more information on threshold settings and event types, refer to “System Alert Manager” on page 131. A typical Event_Action screen is shown below. The types of events this screen displays are dependent on the specific server hardware configuration. For example, not all server models have a UPS or a redundant power supply.

SNMP_Config Manager_info **Event_Action** Password Threshold Event_Log Quit

Event	Agent Action	Execution Program
Warning Temperature	Broadcast	
Critical Temperature	Broadcast	Shutdown
ECC Memory Error	Broadcast	
Fan Stops	Broadcast	
Voltage Exceeds Safe Range	Broadcast	
PCI Bus Utilization		
Memory Utilization High		
File System Utilization High	Broadcast	
XPower Supply Fail		
XUPS Battery Fail		
XPower Fan Stop		
XAC Power Fail		
Chassis Intrusion	Broadcast	
Fuse Fail	Broadcast	
Redundant Power Supply Fail	Broadcast	
Redundant Power Supply Fan Fail	Broadcast	
[Broadcast]	[Execution]	[Cancel]

To specify the desired event action, use the up and down arrow keys to select the event, then press **Enter** or **Tab** to move the cursor to the bottom of the screen. Use the left and right arrow keys to move between the **Broadcast**, **Execution**, and **Cancel** options. You can also specify the name of an **Execution Program** to run when the event occurs.

To exit the Event_Action screen, press **Tab** and the left/right arrow key.

Password

This item allows you to change or enable or disable the agent password. A password must have a minimum of 3 characters and a maximum of 16 characters. If you disable the password, the ASM Pro Server Agent does not execute password checking when the threshold is set from the Console.



Caution: If the password feature is disabled, the server has NO SECURITY protection.

ASM Pro has password protection for setting values. This means that if you want to change threshold values, manager contact information or server location, the Console asks you to enter the ASM Pro Server Agent's password.

SNMP_Config Manager_info Event_Action **Password** Threshold Event_Log Quit

Change Password

Disable Password

You can change into a new password which is from 3 to 16 letters...

Threshold

The four threshold items that can be set at the server site are: PCI Bus Utilization (for systems equipped with PCI Bus hardware), Memory Utilization, BIOS Event Log Utilization, and global File System Utilization (for all file systems).

Setting a PCI or memory threshold is the same as setting these thresholds from the Console side. However, the File System Utilization threshold is a global value that applies to all of the file systems on the agent system.

When the agent uses a resource up to its threshold value, it generates a trap. You use this to ensure that resources are used within reasonable limits.



Note: All threshold settings are preset to factory-recommended values. Some are user-configurable, others are not. For more information on threshold settings and event types, refer to “System Alert Manager (SAM)” on page 131.

SNMP_Config	Manager_info	Event_Action	Password	Threshold	Event_Log	Quit
				PCI Bus Utilization		
				Memory Utilization		
				File System Utilization		
				BIOS Eventlog Utilization		

Event log

This item allows you to view or clear the Trap Log. When any event occurs, the ASM Pro Server Agent sends a trap and save this event to the Trap Log.

When the **View Event Log** option is selected, it allows you to view the Event Log file (/etc/eventlog.dat) by invoking the vi editor.

When you finish viewing the Event Log file, type: **q !** and press **Enter** to end the viewing session.

SNMP_Config Manager_info Event_Action Password Threshold **Event_Log** Quit

View Event Log
Clear Event Log

View Event log file by vi

Quit

To exit the configuration utility, select **Quit** and press **Enter**.

If you change any data, the asmconfig program asks you to update the data before exiting from the program. Select **Update** to update the files.



.....

Note: If you select **Cancel**, your changes are not saved.

SNMP_Config Manager_info Event_Action Password Threshold Event_Log **Quit**

Do you want to update?

[Update] [Cancel]



.....

Note: If you select **Update**, and change the SNMP_config information, the utility displays the following screen prompting you to restart Agent so that the changes can take effect. This happens

whenever you change SNMP Config information utility. If you select **Restart** (recommended), and have changed an IP address in /etc/snmpd.trap, the SNMP daemon (snmpd) is also stopped and restarted.

SNMP_Config Manager_info Event_Action Password Threshold Event_Log **Quit**

Do you want to restart ASM Server Agent?

Note: If you want ASM Server Agent to execute correctly,
please choose [Restart] after you finish all
modifications.

[Restart]

[Cancel]

► asmcfg for SCO UnixWare

Follow these steps to configure the SCO UnixWare agent:

1. At the shell prompt, execute the command to start the ASM Pro Agent Configuration Utility.

/usr/asm/asmcfg
2. Use the **Esc** key to move the cursor between the menu and form regions. When the cursor is located in the form region, use the **PageUp/PageDown** key to switch to different form pages. (Each form page contains a group of related configuration parameters.) Use the **Tab** key or Arrow keys to move the cursor around fields in a form page and then set up the values in them.
3. When the cursor is located in the menu region, select items from the **Config** pulldown menu to directly jump into the corresponding form pages.
4. From the menu, select **File > Save** to update the modified configuration parameters back into the ASM Pro configuration file */usr/asm/asmsmxd.conf*.
5. In the menu select **File > Exit** to quit from the ASM Pro Configuration Utility.



.....

Note: The changed parameters will not become effective until ASM Pro Server Agent is restarted. Therefore, if any configuration is modified and saved, the ASM Pro Configuration Utility will ask whether to restart ASM Pro Server Agent.

Config > SNMP

In this pop-up form, the user can enter the IP addresses of SNMP trap destinations (i.e., those for which ASM Pro Console expected to receive SNMP traps). The list of IP addresses will be saved to the SNMP configuration file */etc/netmgt/snmpd.trap* after choosing the **OK** button. Notice that each IP address entered should be in decimal dot notation, and be typed on one line.

```

ASM Agent Configuration Utility (asmcfg)

File      Config      View
-----
[ASM Password]
Password Protection:
Password: [Change .

Add/Modify/Delete IPs of SNMP
Trap Destinations below:

127.0.0.1

[ OK ]   [ Cancel ]

--- KEY: <Arrow Key>/<PgUp>/<PgDn>/<Tab>/<Enter>/<ESC>----- (Page 1)-----

```

Config > ASM Pro_Password

In this form page the user can:

- Enable or disable the ASM Pro password protection by selecting or unselecting the check mark in the square bracket. If the ASM Pro password protection is enabled, the ASM Pro Console will request the user to enter the ASM Pro password each time when issuing an SNMP set command. (The default setting is Disabled.)
- Change the ASM Pro password. A valid password must have a minimum of 3 characters and a maximum of 16 characters. (The default password is a null string.)

```

ASM Agent Configuration Utility (asmcfg)

File      Config      View
-----
[ASM Password]
Password Protection: [ ]
Password: [ Change... ]

--- KEY: <Arrow Key>/<PgUp>/<PgDn>/<Tab>/<Enter>/<ESC>----- (Page 1)-----

```




Caution: If the password feature is disabled, the server will have NO SECURITY protection.

ASM Pro has password protection for setting values. This means that if the user wants to modify threshold values, manager contact information or server location, the Console will request the user to input the password of the ASM Pro Server Agent.

Config > Manager_Info

This form page contains the information related to the server manager.

```

ASM Agent Configuration Utility (asmcfg)

File      Config      View

[Server Manager Info]
Manager Name:
Office Phone:
Office Address:
Home Phone:
Home Address:
Pager Number:
Email Address:

Server Location:

--- KEY: <Arrow Key>/<PgUp>/<PgDn>/<Tab>/<Enter>/<ESC>----- (Page 2)---
```

Config > Threshold

The Threshold form page allows you to set/change three thresholds: PCI Bus Utilization (for certain server models only), Memory Utilization, and File System Utilization. It also allows you to specify the interval that elapses between polling.



Note: All threshold settings are preset to factory-recommended values; some are user-configurable, others are not. For more information on threshold settings and event types, refer to "System Alert Manager (SAM)" on page 131.

```

ASM Agent Configuration Utility (asmcfg)

File      Config      View
-----
[Threshold Values]
PCI Bus Util. (%):      100
Memory Util. (%):      100
File System Util. (%):  100

Polling Interval (sec.): 1

-- KEY: <Arrow Key>/<PgUp>/<PgDn>/<Tab>/<Enter>/<ESC>----- (Page 3)-----

```

Config > Event_Actions

The events that Agent traps are predefined in the ASM Pro software. However, you can use the Event_Actions form pages to define the agent action that is taken when an event occurs. You can also use the related Threshold form page, described previously, to modify some of the threshold settings. For more information on threshold settings and event types, refer to “Chapter 3 - System Alert Manager”.

```

ASM Agent Configuration Utility (asmcfg)

File      Config      View
-----
<<Event Handling (1)>>
Broadcast  Shutdown  Execute
=====
[Warning Temperature Event]
Event Action:      [V]          [ ]          [ ]
Execute Program:
Pager Number:

[Critical Temperature Event]
Event Action:      [V]          [V]          [ ]
Execute Program:
Pager Number:

[ECC Memory Error Event]
Event Action:      [V]          [ ]          [ ]
Execute Program:
Pager Number:

-- KEY: <Arrow Key>/<PgUp>/<PgDn>/<Tab>/<Enter>/<ESC>----- (Page 3)-----

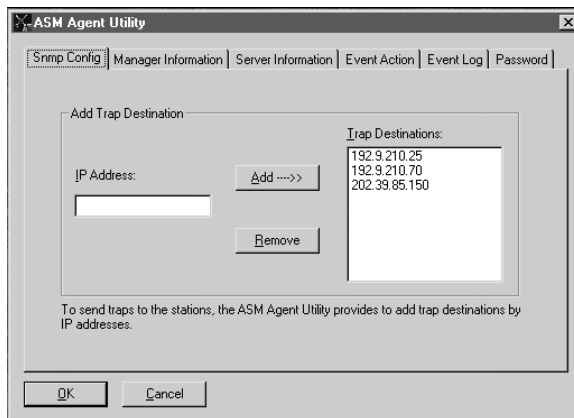
```

► asmcfg for Windows NT

The ASM Pro configuration utility for Windows NT (asmcfg) is found in the ASM Pro Server Agent target directory. The features are similar to asmconfig features for the SCO OpenServer utility described earlier in this chapter.

To Run the Program:

1. In Windows NT, click **Start > Program**. Click ASM Pro Server Agent and ASM Pro Server Agent Utility. The password window appears.



2. Type in the correct agent password and click **OK**. The utility has the following functions that can be accessed by clicking on their tabs.

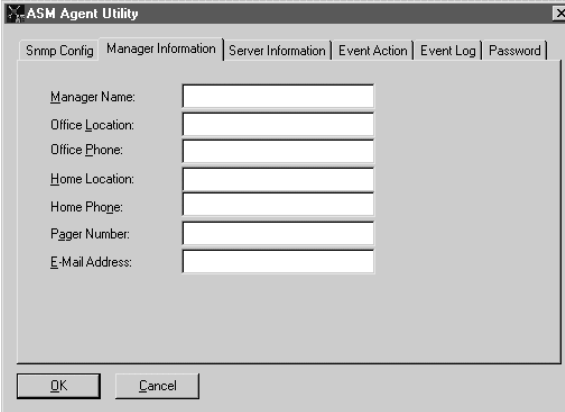
SNMP Config

This section allows you to add, change, or delete any address in the SNMP service trap destinations. If you want the ASM Pro Console to receive event traps from the ASM Pro Server Agent, the Console's IP address or the ASM Pro Console name must be included in the SNMP service trap destinations with the community name "public" on the agent site. The ASM Pro Console name is found in **System > Control Panel > Network > Information** on the ASM Pro Console system.

To add an IP address to the trap list, type in the IP address or ASM Pro Console name and click on the **Add** button. To remove IP address(es) from the trap list, select the IP address or ASM Pro Console name and click on the **Remove** button.

Manager information

Click on the **Manager Information** tab to change server manager or owner information.

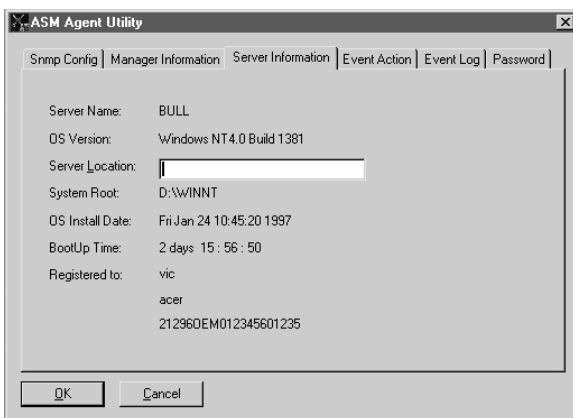


The screenshot shows a window titled "ASM Agent Utility" with a tabbed interface. The "Manager Information" tab is selected. It contains several text input fields for the following labels: "Manager Name:", "Office Location:", "Office Phone:", "Home Location:", "Home Phone:", "Pager Number:", and "E-Mail Address:". At the bottom of the window are "OK" and "Cancel" buttons.

The maximum number of characters allowed is 48 per field.

Server information

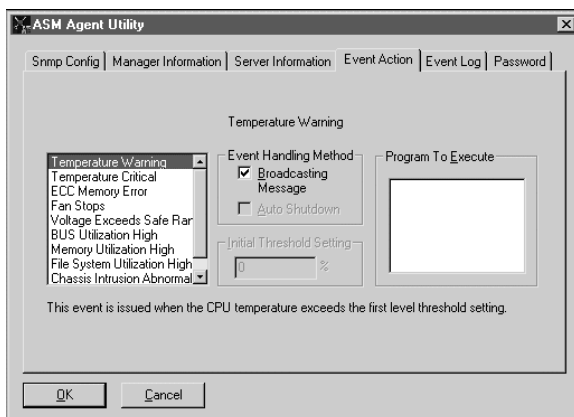
Click on the **Server Information** tab to change the server location. This tab describes basic server data. You can also view this tab through **ASM Pro Console > Server Information > Basic Information**. This screen also allows you to specify the ASM Pro server agent location so that you can track it when you need it.



The maximum number of characters allowed is 48.

Event action

This function allows you to specify the action that ASM Pro Agent takes when an event occurs. Click on the **Event Action** tab to display the following screen.



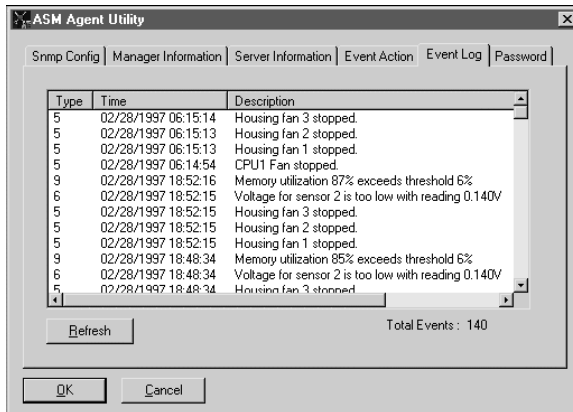
A number of events are defined in ASM Pro. You can define the agent action (broadcast message or shutdown), the threshold setting, and the user-defined program to be executed by the server agent when the trap occurs.

ASM Pro Agent sends a warning message to all users that are logged in at the time the event occurs.

To specify the event action, highlight the event, and use the mouse to check the Event Handling Method checkbox. You can type in the name of the user-defined program you want to execute when the event occurs. You can also set the threshold value for certain events.

Event log

The ASM Pro Event Log is stored in the Windows NT application log area. You can save or delete this information using the Windows NT Eventview program. Click on the **Event Log** tab to display the following screen:

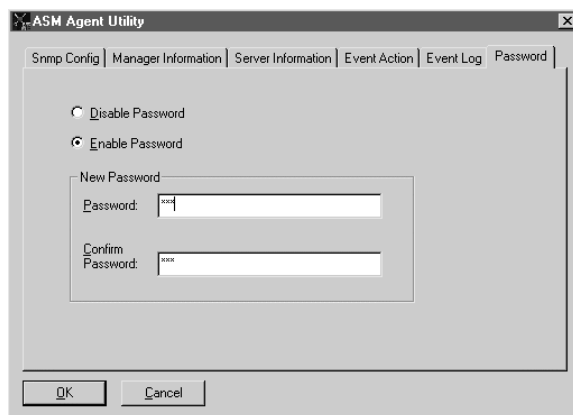


This screen shows the Event Log list. It contains all of the traps generated in the server system. You can view all of the ASM Pro events from the day you installed the ASM Pro server agent.

To refresh the Event Log list, click on the **Refresh** button.

Password

Click on the **Password** tab to display the following screen:



This screen allows you to change, enable, or disable the agent password. A password should have a minimum of 3 characters and a maximum of 16 characters. If you disable the password, the ASM Pro Server Agent does not execute password checking when the threshold is set by the ASM Pro Console.

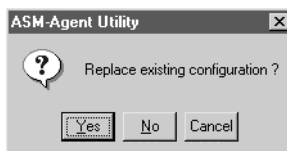


Caution: If the password feature is disabled, the server has NO SECURITY protection.

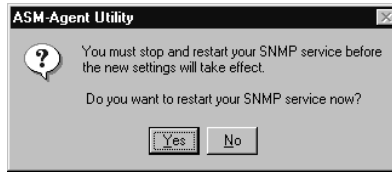
ASM Pro server agent has password protection for setting values. If you want to change threshold values, manager contact information or server location, the ASM Pro Console asks you to enter the ASM Pro Server Agent's password.

Saving changes in asmcfg

After you have finished making changes, click on **OK**. The following dialog box appears:



To save your changes, click on **Yes**. If you have changed the SNMP_config data, the following dialog box appears:



This dialog box prompts you to restart the SNMP services for the changes that you made to take effect. Click on **Yes** to restart these services.

► asmcfg for NetWare

The ASM Pro configuration utility for NetWare (asmcfg) is similar in function to the asmcfg utility used for Windows NT and the asmconfig utility for SCO OpenServer.

At the system console prompt on your NetWare server, enter the command “load asmcfg”. A window similar to the following appears:



The utility includes the following functions: (For each function, follow the instructions at the bottom of the screen.)

Password

ASM Pro has password protection for setting threshold values. When changing a threshold value from the ASM Pro Console, it asks you to enter the password for the ASM Pro Server Agent. If you disable the password, the ASM Pro Server Agent no longer executes password checking when any values are changed.



.....

Caution: If the password feature is disabled, the server has NO SECURITY protection.

To enable or disable the password option:

1. Select the **Password** option. A password must have a minimum of 3 characters and a maximum of 16 characters.
2. Use the left and right arrow keys to switch between **Yes** or **No** and then press **Enter**.



To change the password:

1. Highlight the **Change password** option and press **Enter**. The Set Agent Password window appears.
2. Type the new password and press **Enter**.



Out of band

When you use a modem to connect the agent and the ASM Pro Console, select the **OOB** button (Out of Band connection between the agent and the Console via modem) to configure and to change the out of band modem settings. The modem settings control the out of band connection between the ASM Pro Server Agent and the ASM Pro Console, including the COM port settings. Refer to your modem manual for the proper values.



Manager information

Select **Manager Information** to change manager contact information, such as the manager's name, address, and phone number.

ASM Agent Configuration Utility V4.0 NetWare Loadable Module

Server Manager's Information

Name: _____

Office Phone Number: _____

Office Address: _____

Home Phone Number: _____

Home Address: _____

Pager Number: _____

EMail Address: _____

ENTER=Select ESC=Exit Menu

Server location

Select **Server Location** to specify the physical location of the server.

ASM Agent Configuration Utility V4.0 NetWare Loadable Module

Configuration Item

Password

OOB

Manager Information

Server Location

ENTER=Select ESC=Exit Menu

Event handling

This function allows you to specify the action that ASM Pro Agent takes when an event occurs. Select **Event Handling** to display the Event Handling screen. (A typical Event Handling screen is shown below.)

ASM Agent Configuration Utility V4.0		NetWare Loadable Module	
Event	Broadcast	Shutdown	Execute Program
Temperature Warning	Yes		
Temperature Critical	Yes	Yes	
ECC Memory Error	Yes		
Fan Stops	Yes		
Voltage Exceeds Safe Range	Yes		
UPS - Power Supply Fail	Yes		
UPS - AC Power Fail	Yes		
UPS - Power Supply Fan Fail	Yes		
UPS - Battery Fail	Yes		
Chassis Intrusion	Yes		
Fuse Fail	Yes		
Redundant Power Supply Fail	Yes		
Redundant Power Supply Fan Fail	Yes		
New BIOS Event Log	Yes		
CpuDisabled	Yes		
AssetChanged	Yes		
		Threshold	

ENTER>Select ESC=Exit Menu

See "Event types" on page 144 for a description of the important events.

There are three ways that events are handled:

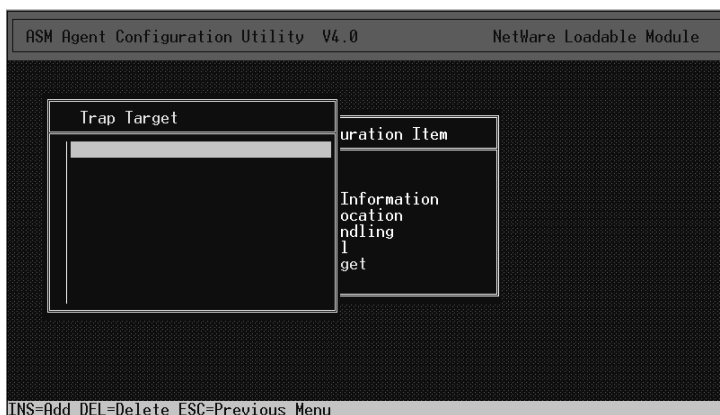
Broadcast - sends a messages to all users logged in to the network.

Shutdown - Shuts down the network operating system.

Execute Program - Executes a specified program when an event occurs.

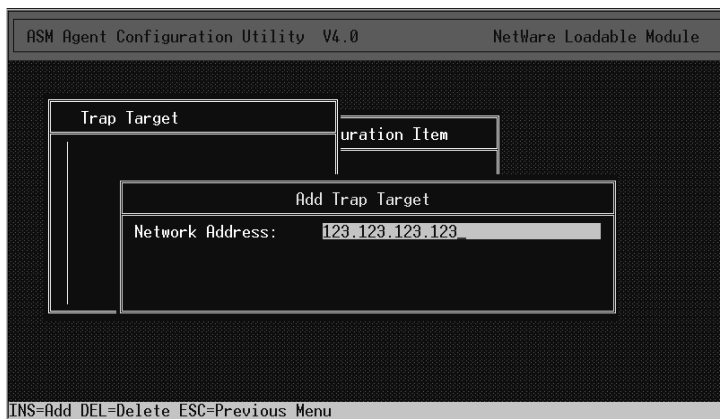
Trap target

Select **Trap Target** to add, change, or delete any IP address in the trap target destinations. If you want the ASM Pro Console to receive the trap from the ASM Pro Agent, the Console's IP address must be included in the trap target destinations with the community name "public" on the system site.



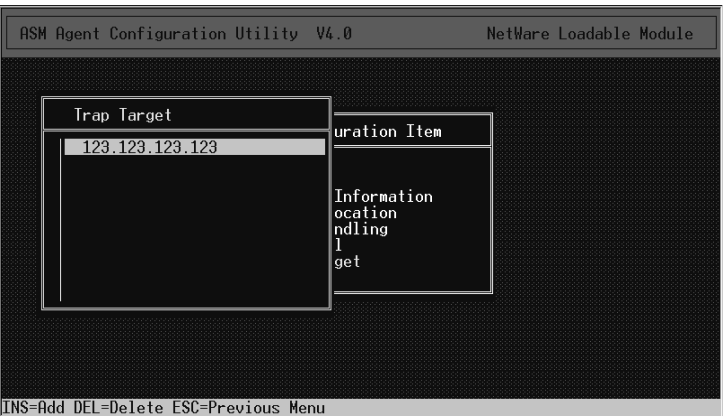
To add an IP address to the trap list:

1. Press the **Insert** key. The Add Trap Target window appears.



2. Type the IP address and press **Enter**.

To remove an IP address from the trap target list, select the IP address and press the **Delete** key.



Saving changes in asmcfg

After you are finished making changes, select the **Exit** option. The following dialog box displays:



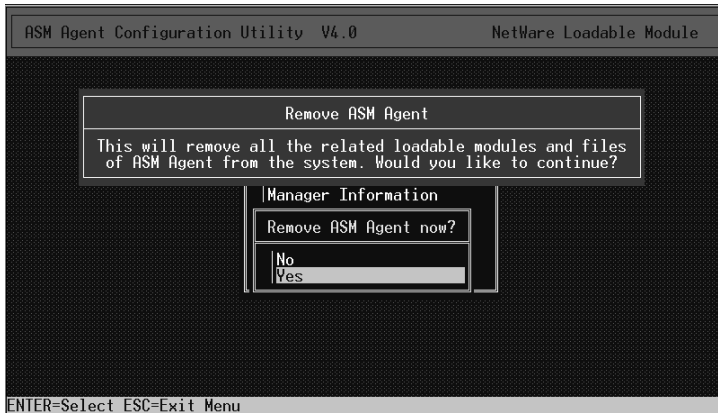
To exit asmcfg, select **Yes**. If you choose to exit asmcfg, the following dialog box displays:



To save changes, select **Yes**. Press the **Esc** key to exit asmcfg.

Uninstalling ASM Pro server agent

From the main asmcfg screen, select **uninstall**, and follow the onscreen prompts.



► asmcfg for Linux

asmcfg is invoked during ASM Pro Server Agent installation to set up the agent password. It may be invoked at any time by typing asmcfg from a Unix shell prompt. The executable file is found in the /usr/local/share/asm directory.

```
SNMP_Config Manager_Info Event_Action Password Threshold Event_Log Quit
+-----+
|
|
|                                     +-----+
|                                     |         |
|                                     |Password:|
|                                     |         |
|                                     +-----+
|
|
|-----+
| Configure Trap Targets for SNMP/SNMPX
```

Working in asmcfg:

- Use the right and left arrow keys to select a menu item.
- Use the up and down arrow keys to highlight the item and press the return key to execute or select the highlighted item.
- Use the left and right arrow keys to switch control between the main window and confirm selection window shown at the bottom of the screen.
- To quit, select Quit from the main menu and press Enter.

SNMP Config

This function allows you to add, change, or delete any IP address in `/usr/local/share/snmp/snmpd.conf`. When you want the ASM Pro Console to monitor the ASM Pro Server Agent, the Console's IP address must be included in `/usr/local/share/snmp/snmpd.conf` on the server site.

SNMP_Config	Manager_Info	Event_Action	Password	Threshold	Event_Log	Quit
<div> <div> Manager Name : - </div> <div> Office Phone : </div> <div> Office Address : </div> <div> Home Phone : </div> <div> Home Address : </div> <div> Pager Number : </div> <div> Email Address : </div> <div> Server Location : </div> </div>						
Use arrow key and edit.....						

Event action

One of the most important functions performed by ASM Pro is event trapping and handling. This is done through the use of threshold settings, hardware error-detection methods, and fault management. When an “event” occurs, Agent performs the event action and sends a trap to Console. It uses the IP address specified in SNMP Config to send the trap to the ASM Pro Console.

This function allows you to specify the type of action that ASM Pro Agent takes when an event occurs. The ASM Pro events that Agent traps are predefined in the ASM Pro software. You can use the Event_Action function to define agent actions performed on the agent system. After ASM Pro Console receives the trap it takes the action defined by the System Alert Manager or ASM Pro Console Setup event handler. You can also use the related Threshold function, described later, to change some of the threshold settings. For more information on threshold settings and event types, refer to “System Alert Manager” on page 131. A typical Event_Action screen is shown below. The types of events this screen displays are dependent on the specific server hardware configuration. For example, not all server models have a UPS or a redundant power supply.

SNMP_Config Manager_Info Event_Action Password Threshold Event_Log Quit		
Event	Agent Action	Execution Program
Temperature Warning	Broadcast	
Temperature Critical	Broadcast	Shutdown
ECC Memory Error	Broadcast	
Fan Stops	Broadcast	
Voltage Exceeds Safe Range	Broadcast	
BUS Utilization High		
Memory Utilization High		
File System Utilization High	Broadcast	
Power Supply Fail	Broadcast	
AC Power Fail	Broadcast	Shutdown
Power Supply Fan Fail	Broadcast	
UPS Battery Fail	Broadcast	
Chassis Intrusion	Broadcast	
Fuse Fail	Broadcast	
Redundant Power Supply Fail	Broadcast	
Redundant Power Supply Fan Fail	Broadcast	
[Broadcast]	[Execution]	[Cancel] PgDn/Next Page

To specify the desired event action, use the up and down arrow keys to select the event, then press **Enter** or **Tab** to move the cursor to the bottom of the screen. Use the left and right arrow keys to move between the **Broadcast**, **Execution**, and **Cancel** options. You can also specify the name of an **Execution Program** to run when the event occurs.

To exit the Event_Action screen, press **Tab** and the left/right arrow key.

Password

This item allows you to change or enable or disable the agent password. A password must have a minimum of 3 characters and a maximum of 16 characters. If you disable the password, the ASM Pro Server Agent does not execute password checking when the threshold is set from the Console.



Caution: If the password feature is disabled, the server has NO SECURITY protection.

ASM Pro has password protection for setting values. This means that if you want to change threshold values, manager contact information or server location, the Console asks you to enter the ASM Pro Server Agent's password.

SNMP_Config	Manager_Info	Event_Action	Password	Threshold	Event_Log	Quit
<div> <div>Change Password</div> <div>Disable Password</div> </div>						
You can change a new password which is from 3 to 16 letters...						

Threshold

The four threshold items that can be set at the server site are: PCI Bus Utilization (for systems equipped with PCI Bus hardware), Memory Utilization, BIOS Event Log Utilization, and global File System Utilization (for all file systems).

Setting a PCI or memory threshold is the same as setting these thresholds from the Console side. However, the File System Utilization threshold is a global value that applies to all of the file systems on the agent system.

When the agent uses a resource up to its threshold value, it generates a trap. You use this to ensure that resources are used within reasonable limits.



Note: All threshold settings are preset to factory-recommended values. Some are user-configurable, others are not. For more information on threshold settings and event types, refer to “System Alert Manager (SAM)” on page 131.

SNMP_Config	Manager_Info	Event_Action	Password	Threshold	Event_Log	Quit
-------------	--------------	--------------	----------	-----------	-----------	------

Do you want to restart ASM Agent ?

Note: If you want ASM Agent to execute correctly,
please choose [Restart] after you finish all
modifications.

[Restart]

[Cancel]

6 ASM Pro Local Console

This chapter describes how to view ASM Pro Agent system information locally. Windows NT and Windows 2000 agents come with ASM Pro Local Console. ASM Pro Local Console displays the agent information and some performance and health data.

► Basic system information

Click the **System** tab to display basic information about the system. Basic information includes system name, operating system, and system board and memory information.



This screen shows the agent system software and basic motherboard information. Some system models have an asset tag property in their motherboard BIOS. If the asset tag property is available, the “Asset Tag” field appears in this window. The Asset Tag function allows you to assign a name to the current asset information.

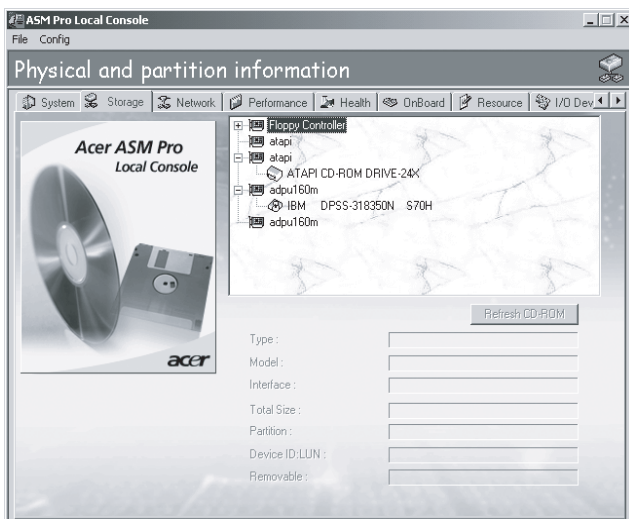
► Physical and partition information

Click on the **Storage** tab to display storage device and partitions information when you select a drive. The screen is divided into two sections: the display window and the information section.

Accessing physical storage device information

To access physical storage device information:

1. Click on a device in the display window. For example, a hard disk.
2. Click on the logical drive to display more partition information and the usage pie chart..
3. Click the **Refresh** button to display the most current device setup.

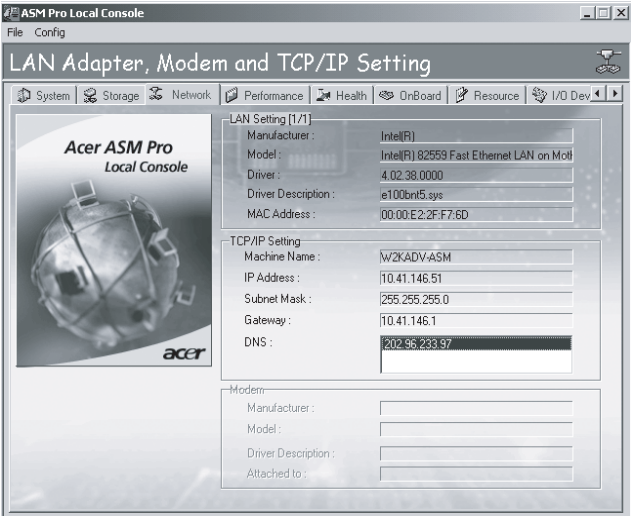


The information section displays the following:

Parameter	Description
Type	Type of storage device (i.e., hard disk, cd-rom, etc.)
Model	Model name of the storage device
Interface	Type of interface the storage device uses (i.e., SCSI, IDE, etc.)
Device ID:LUN	<p>Device ID and LUN (Logical Unit Number) of physical devices.</p> <p>ID number is 0 or 1 for IDE (Integrated Drive Electronics) interface devices, while 0 to 7 is for SCSI (Small Computer System Interface) devices.</p> <p>LUN is an encoded 3-bit identifier used by the SCSI system as a secondary address associated with the SCSI ID. There can be up to 8 LUNs per target ID.</p>
Removable	Identifies whether the storage device is removable or not
Total Size	Maximum storage capacity of the storage device
Partition	Total number of partitions in the storage device

► LAN adapter, TCP/IP, and modem setting

Click the **Network** tab to access information about the system's network settings. If you have more than one network card installed, click the arrow button to cycle through them. The screen contains three sections: LAN, TCP/IP, and Modem.



LAN (Local Area Network)

This section displays information about your LAN card or NIC (Network Interface Card).

Parameter	Description
Manufacturer	Name of the manufacturer
Model	Model name of the device
Driver	Device driver identifier and version number
Driver Description	Brief description of the driver

TCP/IP (Transmission Control Protocol/ Internet Protocol)

This section displays information about your connection to the Internet.

Parameter	Description
System Name	Name of your system
IP Address	IP address of the system
Subnet Mask	Mask address of an IP. A mask is use to identify what subnet your IP belongs to
Gateway	The IP address the system is connected to. A gateway is any device that links two different types of networks
DNS (Domain Name System)	Address of your network domain server

Modem

This section displays information about your modem connection. This section is grayed out when the system does not have a modem.

Parameter	Description
Manufacturer	Manufacturer of the modem
Model	Model identifier and version number
Driver Description	Brief description of the modem's driver
Attached to	COM port the modem is assigned to (COM1 or COM2)

System performance information

Click the **Performance** tab to access information about the system's performance in the following areas: CPU utilization, memory management, file swapping, and file system utilization.



CPU utilization

This section displays a line graph for the use of your system's CPU. The graph is interpreted as the percentage of utilization during the time indicated.

Parameter	Description
Current Usage	Current percentage of CPU utilization
Thread	Number of total executing threads

Virtual memory manager

This section displays the available memory resources in the system.

Parameter	Description
Allocated Memory	Total amount of memory in kilobytes used on the system
Locked Memory	Amount of memory allocated and locked
Swappable Memory	Amount of memory in kilobytes allocated in the swap file
Free Memory	Amount of memory in kilobytes not in use

Swap file

This section shows the available memory allocated for swap file use.

Parameter	Description
Size	Total amount of memory in kilobytes allocated for swap file use
In use	Total amount of swap file memory in use
Page Discards	Amount of page discarded (dumped) to a physical device per second. Pages that haven't been used for a long time are discarded to free memory space
Page Fault	Amount of faulty pages in memory which are discarded to free memory space

File system

This section shows the file read and write performance of the system.

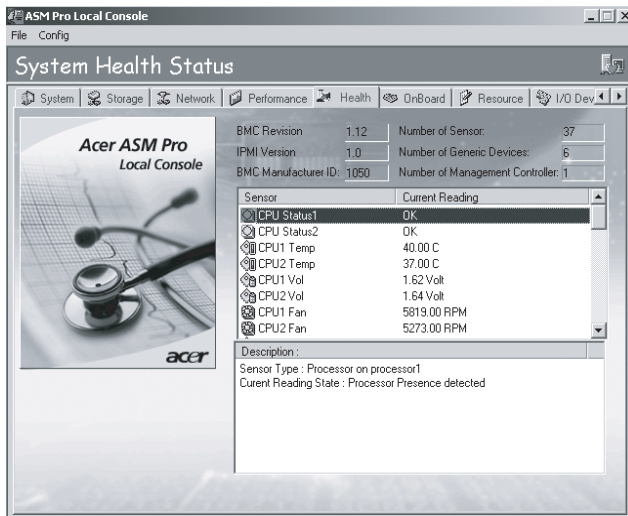
Parameter	Description
Bytes Read/Sec	Speed at which the system can read files
Bytes Write/Sec	Speed at which the system can write files

Parameter	Description
Read/Sec	Number of times the system can read per second
Write/Sec	Number of times the system can write per second

► System health status

Click the **Health** tab to display the current fan, CPU temperature, and CPU voltage status.

Desktop Agent sends a warning to the Console if any of the instruments fail to operate or malfunction. The Console SAM (System Alert Manager) receives the warning information from different system protocols. For more information, refer to “System Alert Manager (SAM)” on page 131.



Fan

This section displays all of the fans installed in the system. Fan status is monitored through the hardware module of the desktop. The green check icon indicates that the fan is functioning properly. The icon turns to a red X mark when the fan is not working.

Temperature

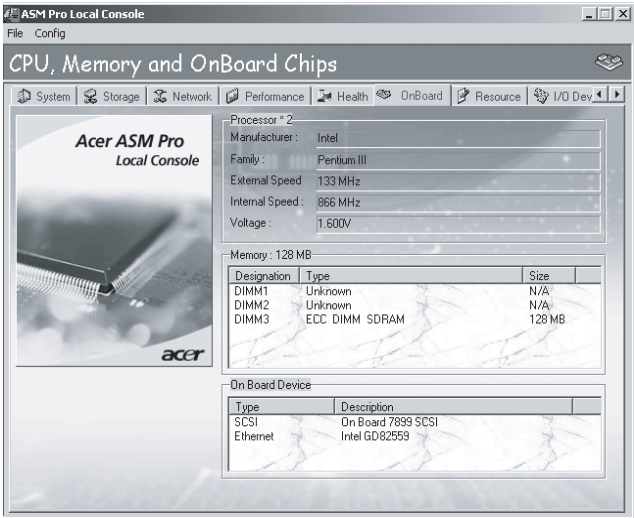
This section displays the CPU's temperature. Temperature status is monitored through the hardware module of the desktop. The green check icon indicates that the CPU temperature is normal while the red X mark icon indicates that the temperature exceeds the normal threshold.

Voltage

The voltage for the processor and the motherboard is shown here. The icon is green when the voltage is within the normal range. The icon turns red when the voltage is not within this range.

CPU, memory, and onboard chips

Click the **Onboard** tab to display basic motherboard information including the system's CPU, memory, and other onboard devices.



Processor

This section displays information about the system's CPU.

Parameter	Description
Manufacturer	Manufacturer of the CPU
Family	Model identifier of the CPU
External Speed (Bus speed)	External speed of the CPU in MHz
Internal Speed	Internal speed of the CPU in MHz
Voltage	Current voltage setting of the CPU

Memory

This section's title bar shows the total amount of memory, in Megabytes, installed in the system. It also shows the number of memory slots available on the system board, and the number of slots currently occupied.

Parameter	Description
Designation	Designated name of the memory module
Type	Type of memory module installed
Size	Total capacity of the memory module

Onboard device

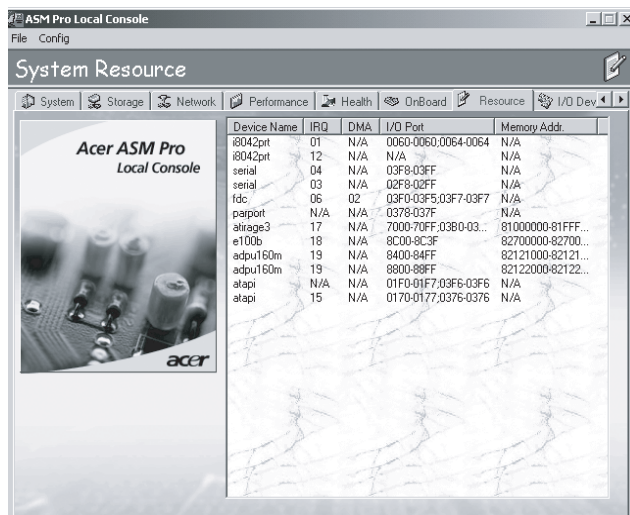
This section displays all the onboard devices installed in the system. Refer to your system board manual for more information about its onboard devices.

Parameter	Description
Type	Type of onboard device in the system
Description	Brief description of the device

► System resource

Click the **Resource** tab to view the system's IRQ, DMA, I/O port, and memory address assignments. This information is useful for detecting hardware interrupt conflicts.

Click on the item title to sort the data.

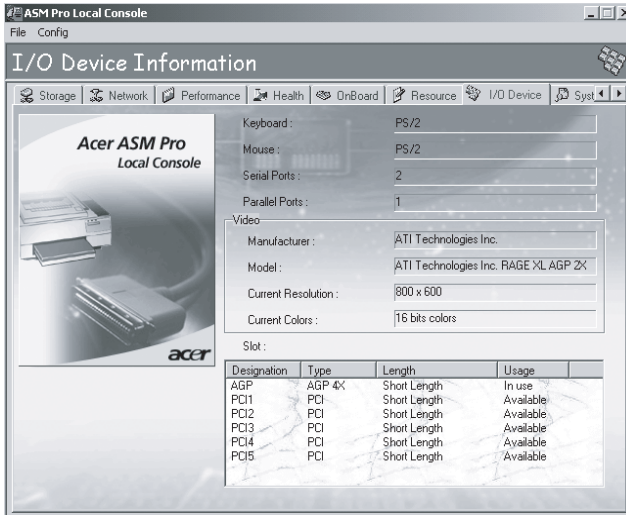


The screenshot shows the 'Acer ASM Pro Local Console' window with the 'System Resource' tab selected. The window has a menu bar with 'File' and 'Config', and a toolbar with icons for System, Storage, Network, Performance, Health, DrBoard, Resource, and I/O Dev. The 'Resource' tab is active, displaying a table of system resources. On the left side of the window, there is a graphic with the text 'Acer ASM Pro Local Console' and an image of a circuit board with the Acer logo.

Device Name	IRQ	DMA	I/O Port	Memory Addr.
i8042prt	01	N/A	0060-0060,0064-0064	N/A
i8042prt	12	N/A	N/A	N/A
serial	04	N/A	03F8-03FF	N/A
serial	03	N/A	02F8-02FF	N/A
fdc	06	02	03F0-03F5,03F7-03F7	N/A
parport	N/A	N/A	0378-037F	N/A
atapi3	17	N/A	7000-70FF,03B0-03...	81000000-81FFF...
e100b	18	N/A	8C00-8C3F	82700000-82700...
adpu160m	19	N/A	8400-84FF	82121000-82121...
adpu160m	19	N/A	8800-88FF	82122000-82122...
atapi	N/A	N/A	01F0-01F7,03F8-03F6	N/A
atapi	15	N/A	0170-0177,0376-0376	N/A

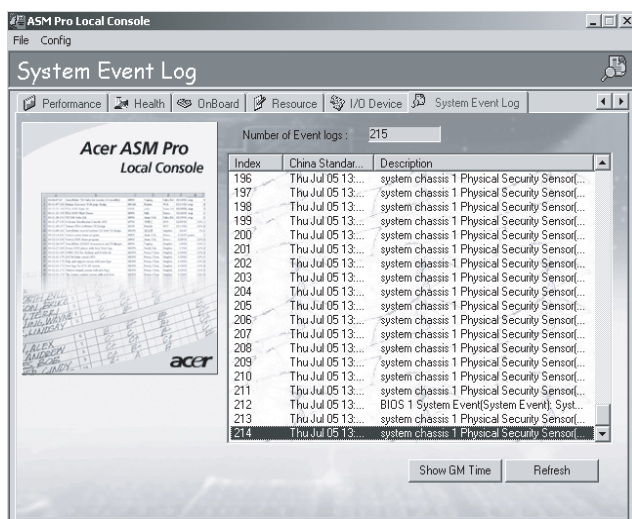
► I/O device information

Click the **I/O Device** tab to display the types of Input/Output devices installed in the system. I/O devices include the keyboard, mouse, serial ports, parallel ports, video devices, and expansion slots.



System event log

Click the **System event log** tab to display the record of system events .



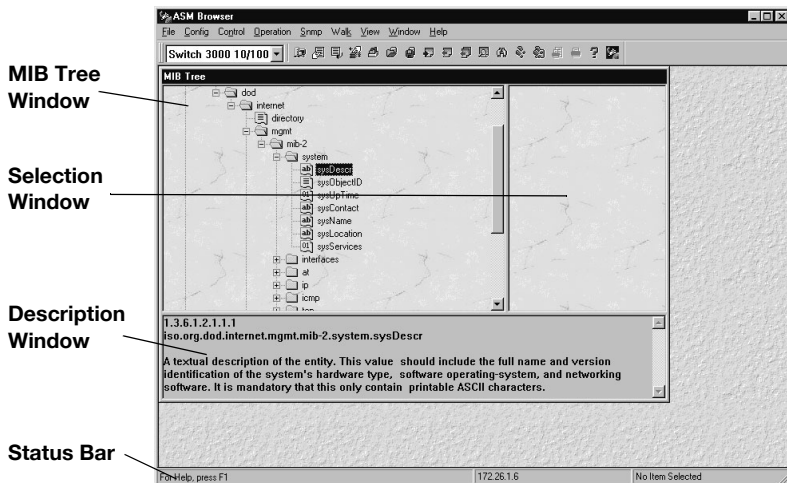
7 ASM Pro MIB Browser

ASM Pro MIB Browser is a MIB (Management Information Base) file browsing tool. It is an add-on utility available with the ASM Pro package. ASM Pro MIB Browser allows you to view and change the OID (Object ID) values of the systems you are managing on your network. It also allows you to define and maintain a list of OIDs to view.

► Installing ASM Pro MIB Browser

To install ASM Pro MIB Browser, run the setup program under the ASM Pro Console directory, select **Custom** as the setup type, then select **Utility**, and click **Change**. Then check the **ASM Pro MIB Browser** subcomponent.

To launch ASM Pro MIB Browser from the ASM Pro Console, click on the **ASM Pro MIB Browser** icon on the toolbar or select **Utility > ASM Pro MIB Browser** from the menu bar.



User interface

The ASM Pro MIB Browser user interface allows you to move around easily and to access information either by using menu commands or by clicking buttons. When you start ASM Pro MIB Browser, the main screen displays the information from your last ASM Pro MIB Browser session.

This section discusses the following screen components:

- Menu Bar, Toolbar, and System List Combo Box
- MIB Tree Window
- Selection Window
- Description Window
- Status Bar


Menu bar and toolbar


The System List box lists all of the systems added to the Selected list in the Auto Discovery window. Click on the down arrow and select the name of the system whose Object Identifiers (OIDs) you want to view.





Toolbar buttons provide quick access to selected functions in ASM Pro MIB Browser with a single mouse click. The Menu Bar contains the following items and commands:

- File Menu - allows you to save and print your files.



Command	Icon	Description
Save		Save an existing query
Print Setup		Setup printer parameters
Print Preview		Shows a preview of the materials to be printed


Command	Icon	Description
Print		Prints information contained in the current window
Exit		Terminates ASM Pro MIB Browser session

- **Config Menu** - controls the environment of the browser. You can select systems to view and set polling intervals.






Command	Icon	Description
Auto Discovery		Searches for available systems in the network and displays them for monitoring purposes
Trap		Enables or disables the Trap Handling function of the browser and also displays the alert log. This function is disabled when ASM Pro Console is running
Community and Port		Specifies the SNMP community and port for Get and Set Operations
Option		Sets up the MIB Browser configuration option

- **Control Menu** - contains the tools for manipulating and querying MIBs.







Command	Icon	Description
Define New Query		Specifies your own query (list of OIDs) to browse
Select Query		Select from a list of previously defined queries to browse or to remove queries from the list

Command	Icon	Description
Manage MIB Database		Displays a window where you can add, remove, initialize, and view the history of MIB files
Telnet		Connect to the server by telnet



- Operation Menu - contains the tools for manipulating and viewing OIDs. It includes commands to add or remove OIDs in the Selection window and to view the values of these OIDs.


Command	Icon	Description
Add		Appends the highlighted OID or OIDs of a highlighted node in the MIB Tree window to the Selection window
Remove		Deletes the selected OIDs from the Selection window
Remove All		Clears the Selection window
Browse		Displays the values of the OIDs in the Selection window
Find		Searches for the OID the user wants to find in the MIB tree

- SNMP Menu - SNMP (Simple Network Management Protocol) allows you to control and view information about OIDs. The pulldown menu is enabled when the SNMP Table is open. Refer to “Browsing OIDs (SNMP table)” on page 229 for more information on how to open the SNMP Table.

Command	Icon	Description
Get		Updates the contents of the OID Value table with the current OID values
Set		Enabled only when the SNMP Table is the active window and when the OID selected can be modified
Polling		Continually retrieves the current values of OIDs and updates the OID Value Table
Stop		Stops browsing the OID
Rotate		Switches the order in which the contents of the OID Value Table are displayed and acts as a toggle between views, so rows are turned into columns and vice versa
Option		Displays the Option window

- Walk Menu - detects available OIDs from a node or subnode and displays their values.

Command	Icon	Description
Walk		Displays the values of a selected node and its subnodes in the Walk Operation window
OID		To specify an OID in the Walk Operation - Input dialog box from which the walk operation starts

Command	Icon	Description
Pause		Available only when a walk operation is in progress to temporarily halt or resume the walk operation
Set		Enabled only when the Walk Operation window is the active window and when the OID selected can be modified, displays the Set Operation dialog box


- View Menu - allows you to show the toolbar and status bar.

Command	Description
Toolbar	Displays/hides the toolbar
Status Bar	Displays/hides the status bar
Trap Log	Displays the trap log dialog box

- Window Menu - allows you to arrange the windows in your ASM Pro MIB Browser.

Command	Description
Cascade	Arranged the open windows in a cascading manner
Tile	Arranged the open windows in tile manner
Arrange Icons	Arranges the icons properly

- Help Menu - The context-sensitive Help menu contains the following items.

Command	Icon	Description
Help Topics		Starts ASM Pro MIB Browser Help, displaying the Index screen
About		Displays ASM Pro MIB Browser product information

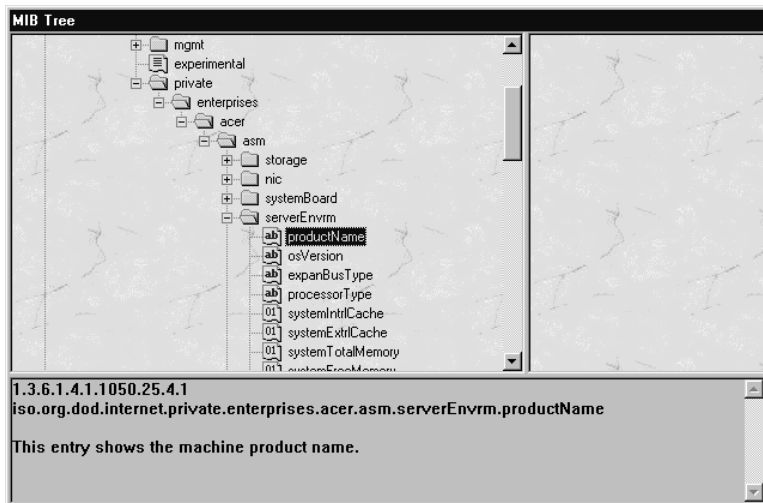
MIB tree window

Located on the left side of the screen, this window shows the MIB tree structure. MIB nodes and subnodes are represented by folders, and the OIDs are represented by files listed under the folders.

You can expand or collapse the nodes and subnodes by clicking on the folders. If you double-click on a node, all of the OIDs contained in that level are shown.

If you double-click on an OID, ASM Pro MIB Browser gets its value and shows it in the Description Window.

MIB tree



ASM Pro MIB information is located under:

iso/org\dod\internet\private\enterprises\acer (or subtree)

If you cannot see the ASM Pro folder, use the MIB Database option to add the ASM Pro MIB file to it. All of the ASM Pro-supported MIB files are located in the program files in the the /Acer/ASM Pro Console directory.

Selection window

This window is on the right side of the MIB Tree Window. OIDs can be added by selecting OIDs and clicking on the “Add OID” button. You can select the OIDs from the MIB Tree Window or use previously defined OIDs from the Select Query dialog box.

Description window

The description window is located at the lower part of the MIB Tree Window. It displays OIDs, labels and a brief description of the node or OID highlighted in the MIB Tree Window.

Status bar

The status bar is located along the bottom of the screen. The left side displays a brief description of a highlighted menu command or a clicked toolbar button. The right side contains the network address of the selected systems.

► Functions

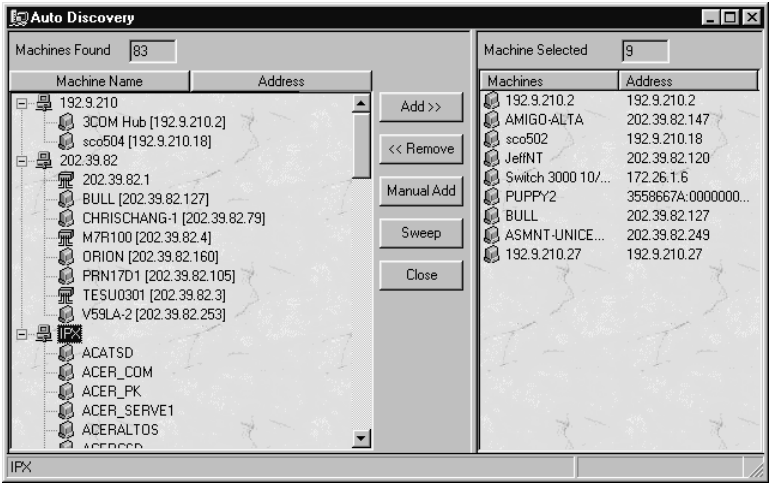
This section tells you how to perform the following tasks:

- Selecting browsing systems
- Setting up browsing options
- Configuring community and port
- Defining a new query
- Selecting a query
- Managing the MIB database
- Adding an OID
- Removing an OID
- Browsing OIDs (SNMP Table)
- Taking a Walk through the MIB
- Finding an OID
- Saving Information

Selecting browsing systems

When you launch MIB Browser from the ASM Pro Console, all the systems that the console monitors are added to the system listing. You can make changes to the systems using the Autodiscovery option.

From the Config menu, select **Auto Discovery**, or click on the **Auto Discovery** icon on the toolbar menu, to display the Auto Discovery dialog box.



This window displays all IP/IPX systems in your network detected by the ASM Pro MIB Browser. The following items are available in this dialog box.

Auto Discovery dialog box items

Item	Description
Machines Found	Displays all the IP/IPX systems available on your network
Machines Selected	Shows all the systems to be monitored by ASM Pro MIB Browser
Button	Description
Add	Appends the highlighted systems to the Systems Selected list
Remove	Deletes the highlighted systems from the Systems Selected list
Manual Add	Allows you to enter an IP address manually to add a system to a selected list.

Item	Description
Sweep	Searches an address by matching the first three parts of the IP Address that you specify
Refresh	Searches the subnet that is currently in the Auto Discovery database.
Close	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now contains all the systems you specified in the Systems Selected list



Note: For the auto discovery function work properly, the agent must be able to respond to standard MIB-II requests.

Setting up browsing options

From the Config menu, select Options to display the Configure Options dialog box.

Configure Options

SNMP Table Options

☐ Set Log File

☐ Rotate Table

☒ Show Enumeration ☒ Decimal ☐ Hexadecimal

☒ Show Grid Polling Interval

Graphic Options

☐ Graphic ☒ Value ☐ Deviation

☒ Create New Graphic Window

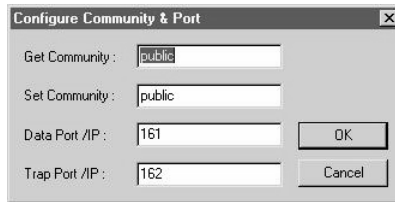
☒ Load Trap Handler

Configure timer dialog box items

Item	Description
Set Log File	Sets the log file and starts to record SNMP values to the log file
Rotate Table	Switches the order in which the contents of the table are displayed and acts as a toggle between views, so rows are turned into columns and vice versa
Show Enumeration	Shows the Enum String if this OID is declared as an enum value in the MIB file
Show Grid	Shows grid lines in the SNMP table
Set Decimal/Hexadecimal	Shows decimal or hexadecimal type of OID values
Polling Interval Field	Specifies the amount of time in seconds for the browser to retrieve data from the target system. You can type an integer from 1 to 60
Graphic Options	Displays the SNMP table with graphics
Create New Graphic Window	Specifies a new graphic window
Load Trap Handler	Loads trap handler to handle trap receiving operations
Button	Description
OK	Closes the dialog box and causes the modifications you made to take effect
Cancel	Closes the dialog box, discarding all changes made

Configuring community and port

You can set Get/Set communities and ports for SNMP Operations by selecting Configure Community and Port from the Config menu.

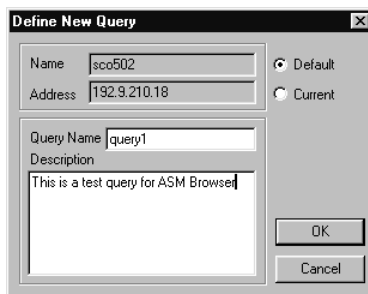


Defining a new query

This dialog box lets you specify names and descriptions for a list of OIDs that are frequently viewed, and saves this information to the database. This eliminates the need to search for the same sets of OIDs each time you start ASM Pro MIB Browser. After setting a query, it is added to the Name field in the Select Query dialog box.

Follow these steps to define a new query (set a list of OIDs to view):

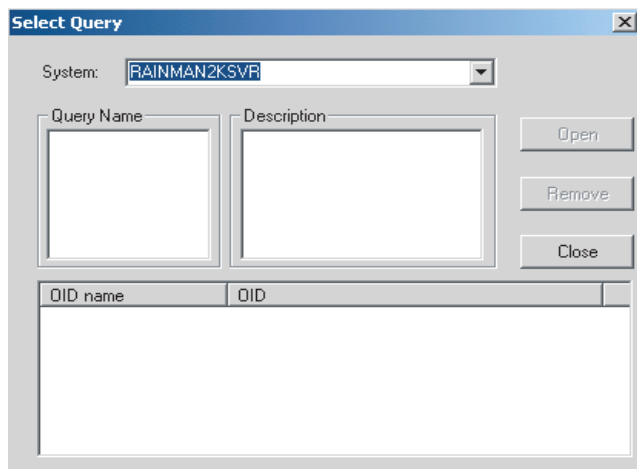
1. From the MIB tree window, select the OIDs you want to include in the query and add them to the Selection Window.
2. Select **Control > Define New Query**. The Define New Query dialog box displays.
3. Type a name and description for the query.
4. Click **OK** to accept it.



Each time you want to view this list, select its name from the Select Query dialog box (under the control menu). All of the OIDs are listed in the Select Query window. Highlight the query name that you want to view, and click on the open button. See "Selecting a Query" below for more information.

Selecting a query

From the Control menu, click on “Select Query”. The Select Query dialog box, shown below, appears. This dialog box allows you to choose from a list of previously defined queries. It displays all OIDs in a query in the Selection window. You can also remove queries from the database, or clear the database of all queries.



Select query dialog box items

Item	Description
System Field	Shows the name of the systems you are currently browsing
Address Field	Displays the network address of the systems you are currently browsing
Query Name	All query names defined in the Define New Query dialog box are listed here. Click the name of the query you want to view or remove from the database
Description Field	Displays a brief description of the selected query

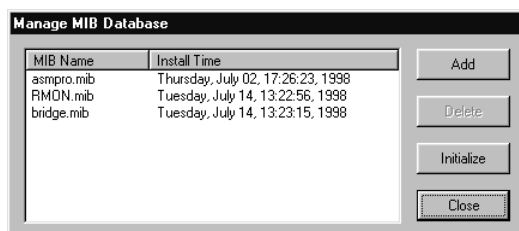
Item	Description
Button	Description
Open	Opens the selected query. A SNMP table appears.
Remove	Removes all queries in the database. This action takes effect only after clicking OK
Close	Closes the dialog box, discarding all changes made

When you select a query name, all of the previously defined OIDs are listed in the OID name table.

Managing the database

The MIB Browser needs a description file to identify each Object ID that you plan to browse. ASM Pro server Agent uses a `asmnt.mib` file to describe its own object IDs. It is installed on the `asm agent` system. ASM Pro Desktop also includes a number of MIB files in its MIB directory.

Select **Control > Manage MIB Database** to launch the MIB database managing dialog box.



Initializing the database

The Initialize command removes all added MIB files from the existing MIB database. After this process is carried out, only the basic MIB tree contents remain. Select **Control > Manage MIB Database > Initialize** to confirm the initialization.

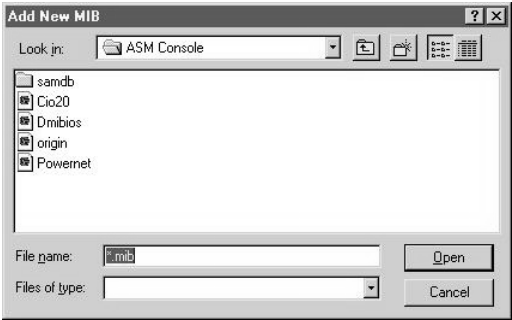
This dialog box prompts you to confirm whether or not to continue initializing the MIB database. To continue, click **OK**; otherwise, click **Cancel** to close this box without initializing.



Warning! The initialize action cannot be undone. Do not click the OK button unless you are sure about removing all installed MIB files from the database.

Adding a new MIB

To install a new MIB file into the existing MIB database, select **Add** from the MIB database managing dialog box. The Add New MIB dialog box appears. Specify the path and filename of the MIB file you want to install, and click on the “Open button.



Add new MIB/remove MIB dialog box items

Item	Description
File Name	Type or select the filename you want to add or remove. This box displays the files with the extension you specified from the List Files of Type box
Files of Type	This box lets you specify the extension of the file you want to add or remove
Look in:	Use this box to specify the drive and folder containing the file you want to add or remove

Removing a MIB

To remove an installed MIB file from the existing MIB database, click **Delete** from the MIB database managing dialog box.

To remove all installed MIB files from the MIB database, select the Initialize command. Refer to “Initializing the database” on page 227.



Note: You cannot browse OID data unless a MIB file has been added to the database.

Adding an OID

Select the OIDs you want to view by highlighting them from the MIB Tree, then select **Operation > Add** or click the **Add** icon on the toolbar. The OID appears in the selection window.



Note: If you highlight a node, all of the OIDs on that node are added.

Removing an OID

Select the OID you want to remove by highlighting it in the Selection window then select **Operation > Remove OID** or press the **Delete** key on the keyboard. The OID disappears from the Selection window.

Removing all OIDs

You can remove all of the OIDs in the Selection window by clicking on the **Remove all** toolbar button or by selecting **Operation > Remove All**.

Browsing OIDs (SNMP table)

To get the OID values of an SNMP agent:

1. From the System List Combo Box on the toolbar, select the system's name.
2. Browse through the MIB Tree window to select the OIDs you want to view.
3. Select **Operation > Add** or click the **Add** button from the toolbar. The OID appears in the upper right frame of the MIB Tree window.

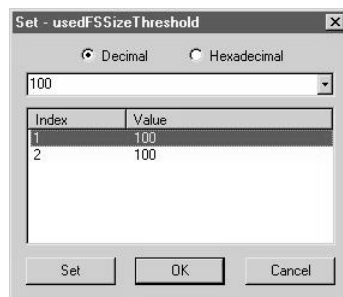
- Access Type - Read, Write, R/W or No Access for each OID, depending on the definition in the MIB file. Only an OID whose access type is R/W or Write can be set.
- Data Type - Integer, Unsigned Integer, Gauge, Counter, Counter64, TimerTick, OctetString, BitString, Network Address, IP Address, Opaque, Object ID, and Unknown.
- OID Value - The value returned by SNMP agent for this OID. If the OID is a table, i.e., the values of this OID are more than one, the values are shown in columns "OID Value #1", "OID Value#2", etc.

Set operation

The OID value can be set if the attribute of the OID is R/W (Read/Write) or Write. If you highlight a R/W OID the Set button is enabled.



If the OID has multiple values, use another Set dialog box to set another value in the table.



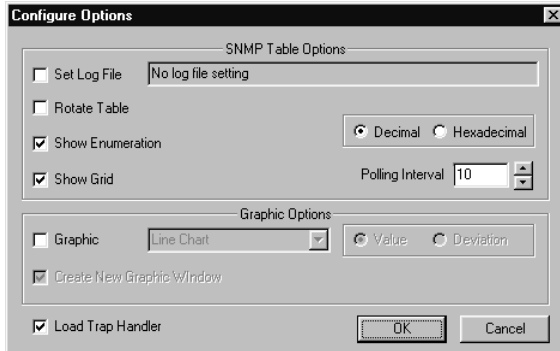
Decimal or hexadecimal

The OID Value column heading can be viewed in two ways: Decimal and Hexadecimal. The SNMP Table displays the OID values in decimal when you click Decimal and in hexadecimal if you click Hexadecimal.

Activating the log file

To activate the log file:

1. In the SNMP Table window, click the **Option** button. The SNMP-Option dialog box appears.



2. Click **Set Log File**. The Save Log File dialog box appears.
3. Enter the filename of the log file then click **Open**. The filename appears in the text box.

Enumeration display

This window displays a list of string-to-integer mappings for the selected OID. You can highlight an OID and press the right button of mouse and then choose Enumeration from the pop-up menu. The Enumeration window appears.

Value	Enumeration
0	netware
1	sounix
2	windowsNT
3	unixware

You can view OIDs by the enumeration values defined in the MIB file instead of the original values.

To see the Enumeration Display:

1. Click the Option button in the SNMP Table window. The SNMP-Option dialog box appears.
2. Click on the Enumeration Display checkbox.

Recording OID polling information

The Polling button continually retrieves the current values of OIDs and updates the OID Value table. You can record this information by activating the Log File. If the Log File is not activated, it is not recorded. Refer to “Activating the log file” on page 232 for more information.

Setting the time interval for polling

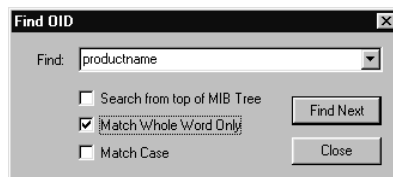
You can set the time interval for polling. The polling interval must be in the range from 1 to 60 seconds.

Rotating the SNMP table

The Rotate button is used to switch the order in which the contents of the OID Value Table are displayed. It also acts as a toggle between views, so rows are turned into columns and vice versa. If you select non-tabled OIDs in the SNMP Table window, this function is disabled.

Finding OIDs in the SNMP table

To search for an OID, click the **Find** button. The Find OID dialog box displays. For more information about the Find OID dialog box, refer to “Finding an OID” on page 235.



Taking a walk through the MIB

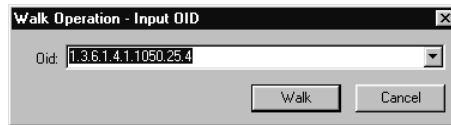
You can use the Walk function to automatically view OID values starting from a particular node or OID.

To Walk from a Node (MIB Tree):

1. From the System List Combo Box in the toolbar, select the system's name.
2. Browse through the MIB Tree window and select an OID or node from which you'd like to start the walk operation then select **Walk > Walk** or click the **Walk** button on the toolbar.
3. The Walk Operation window appears and the OIDs pop up in the window.

To Walk from a query input OID:

1. To start at a particular OID, select **Walk > OID** or click the **OID** button on the toolbar. Type in the OID you want to Walk in the OID text box.



2. Click **Walk**. The Walk Operation window appears and all available OIDs start popping up one-by-one.

Walk operation window

The Walk Operation window shows detailed information about each OID. It keeps displaying OIDs as long as there are OIDs available. The **Pause** button on the right side of the window pauses the walk function. The **Find** button displays the Find OID dialog box. The **Set** button displays the Set Operation dialog box. You can only set an OID, if it can be modified.

Walk Operation - sco502 - 192.9.210.18

sco502 Decimal Hexadecimal

OID	OID name	Access Type	Data Type	OID Value
1.3.6.1.4.1.1050.25...	productName.0	Read	OctetString	
1.3.6.1.4.1.1050.25...	osVersion.0	Read	OctetString	SCO UNIX System ...
1.3.6.1.4.1.1050.25...	expansionBusType.0	Read	OctetString	ISA MCA
1.3.6.1.4.1.1050.25...	processorType.0	Read	OctetString	Pentium Pro 200Mhz
1.3.6.1.4.1.1050.25...	systemIntrCache.0	Read	Integer	512
1.3.6.1.4.1.1050.25...	systemExtIntrCache.0	Read	Integer	0
1.3.6.1.4.1.1050.25...	systemTotalMemory.0	Read	Integer	33157120
1.3.6.1.4.1.1050.25...	systemFreeMemory.0	Read	Integer	12709888
1.3.6.1.4.1.1050.25...	systemSerialPort1In...	Read	OctetString	Serial Port 16550A...
1.3.6.1.4.1.1050.25...	systemSerialPort2In...	Read	OctetString	Serial Port 16550A...
1.3.6.1.4.1.1050.25...	systemParallelPortIn...	Read	OctetString	Parallel Port ECP/E...
1.3.6.1.4.1.1050.25...	keyboardType.0	Read	OctetString	PS/2
1.3.6.1.4.1.1050.25...	videoType.0	Read	OctetString	VGA/EGA
1.3.6.1.4.1.1050.25...	mouseType.0	Read	OctetString	PS/2
1.3.6.1.4.1.1050.25...	sysBiosVer.0	Read	OctetString	*** Error *** Bad string...
1.3.6.1.4.1.1050.25...	serverName.0	Read	OctetString	sco504
1.3.6.1.4.1.1050.25...	serverUpTime.0	Read	OctetString	0 days 00 : 53 : 13
1.3.6.1.4.1.1050.25...	serverMgrName.0	Read	OctetString	

59 Items

Finding an OID

To find an OID:

1. In the MIB tree, highlight the node where you would like to start the search.
2. Click the **Find** button on the toolbar or select **Operation > Find**. The Find OID dialog box appears.

Find OID

Find:

☐ Search from top of MIB Tree
☒ Match Whole Word Only
☐ Match Case

Find Next Close

3. Type in the OID name you want to find in the Find text box. You can check the checkbox for the browser to do the following:
 - Search from top of MIB - the browser searches the whole MIB tree.
 - Match Whole Word Only - the browser searches the MIB tree for matching words.
 - Match Case - the browser searches the MIB tree for case-sensitive words.

4. Click **Find Next**. The Browser starts searching for a match.
5. The find result appears in the bottom part of the MIB Tree window.

Saving information

This command works two ways, depending on the current active window:

If the SNMP Table window is active, this command displays the Save SNMP Information dialog box. The information is saved as a text file with an .smp file extension.

If the Walk Operation window is active, this command displays the Save Walk Information dialog box. The information is saved as a text file with a .wlk file extension.

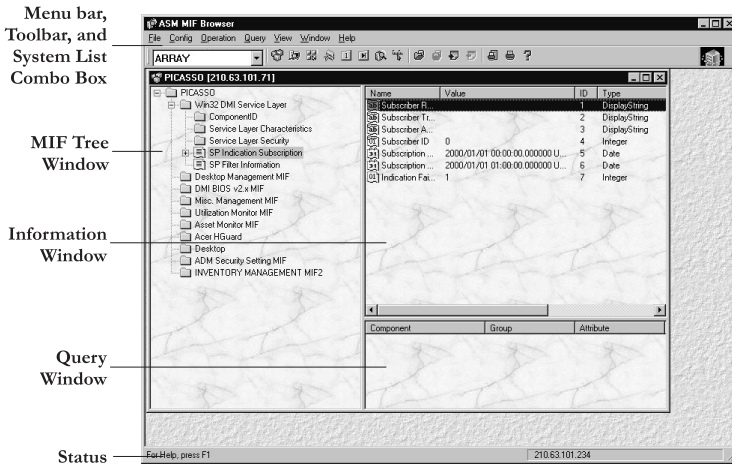
8 ASM Pro MIF Browser

ASM Pro MIF Browser is a MIF (Management Information Format) file browsing tool. It is an add-on available with the ASM Pro package, and describes a hardware or software component of a system. MIF files are used by DMI (Desktop Management Interface) to report system configuration information to the Console.

► Installing ASM Pro MIF Browser

To install ASM Pro MIF Browser, run the setup program under the ASM Pro Console directory, select **Custom** as the setup type, then select **Utility**, and click **Change**. Then check the **ASM Pro MIF Browser** subcomponent.

To launch ASM Pro MIF Browser from the ASM Pro Console, click the **ASM Pro MIF Browser** icon on the toolbar or select **Utility > ASM Pro MIF Browser** from the menu bar.



User interface

The ASM Pro MIF Browser user interface allows you to move around easily and access information using menu commands or by clicking buttons. When you start ASM Pro MIF Browser, the main screen displays the information from your last ASM Pro MIF Browser session.

This section discusses the following major screen components:

- Menu Bar, Toolbar, and System List Box
- MIF Tree Window
- Information Window
- Query Window
- Status Bar



Menu bar, toolbar, and system list box


The system list box allows you to select the name of the systems whose configuration you want to view. It contains all the systems added to the Systems Selected list in the Auto Discovery window.





Toolbar buttons enable quick access to selected functions in ASM Pro MIF Browser through a single mouse click. The Menu Bar contains the following items and commands:

- File Menu - allows you to save and print your files.






Command	Icon	Description
New		Creates a new DMI window for a system
Print Setup		Set up printer parameters
Print Preview		Shows a preview of the materials to be printed

Command	Icon	Description
Print		Prints information contained in the current window
Exit		Terminates ASM Pro MIF Browser session





- Config Menu - searches for available systems in the network and controls the environment of the browser. You can select systems to view and set polling intervals.

Command	Icon	Description
Auto Discovery		Searches for available systems in the network and displays them for monitoring purposes
Options		Displays the browsing options window. See "Setting up browsing and default connection options" on page 248

- Operation Menu - contains the tools to move around and view table information of MIFs.

Command	Icon	Description
First Row		Goes to the beginning or first row of the table, if the data is listed in MIF table format
Next Row		Goes to the next row in the table, if the data is listed in MIF table format
Browse		Displays the whole DMI information. Use it to view all of the records.
Edit		Allows you to change the value of an item if the item is configurable. Changing the value of an item requires no password from desktop agent
Property		Displays item properties

- Query Menu - contains the tools for assigning and defining queries for later use.

Command	Icon	Description
Add Item		Adds an item to the query window
Remove Item		Removes an item from the query window
Define New Query		Saves the item list in the query window to disk for later use
Select a Query		Opens a query file from disk
Polling		Updates information on screen


- View Menu - gives you the option of whether or not to show the toolbar and status bar..

Command	Description
Toolbar	Displays/hides the toolbar
Status Bar	Displays/hides the status bar

- Window Menu - allows you to arrange the windows in your ASM Pro MIF Browser.






Command	Description
Cascade	Arranges the open windows in a cascading manner
Tile	Arranges the open windows in tile manner
Arrange Icons	Arranges the icons properly

- Help Menu - ASM Pro MIF Browser comes with a context-sensitive Help menu with the following items:

Command	Icon	Description
Help Topics		Starts ASM Pro MIF Browser Help, displaying the Contents screen
About		Displays ASM Pro MIF Browser product information

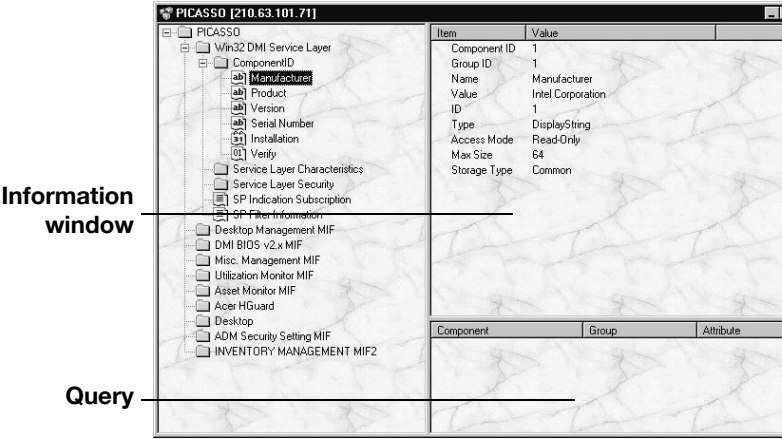
MIF tree window

Located on the left side of the screen, this window shows the MIF tree structure. MIF nodes and subnodes are represented by folders while item attributes are represented by documents. These documents appear in the following form:

Icon	Document type
	String data
	Integer data
	Hexadecimal data
	Date data
	Table data

You can expand or collapse the nodes by clicking on the folders. If you double-click a node, all of the item attributes and folders contained in that level are displayed in the Information Window.

When you double-click on an item attribute or a DMI table attribute, ASM Pro MIF Browser displays its value in the Information Window.



Information window

This window is to the right of the MIF Tree Window. The attributes selected from the MIF Tree Window can be seen here.

Query window

The Query Window is below the Information Window. It displays the component, group and attribute of the item you want to put into a query.

Status bar


Located along the bottom of the screen, the status bar provides different information as you work with ASM Pro MIF Browser. The left side displays a brief description of a highlighted menu command or a clicked toolbar button. The right side contains the network address of the selected systems.

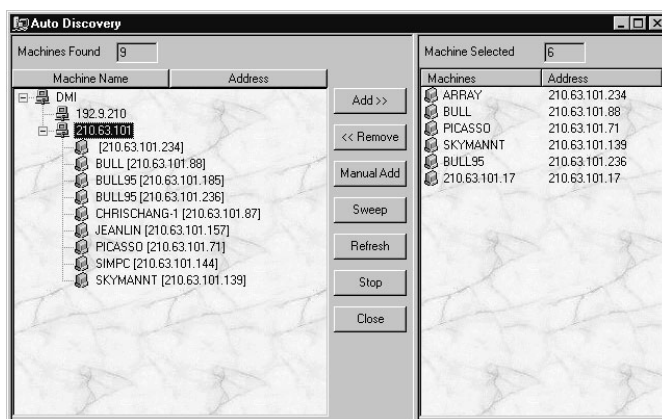
► Functions

This section tells you how to perform the following tasks:

- Selecting browsing systems
- Setting up browsing options
- Browsing the DMI table
- Defining a new query
- Selecting a query

Selecting browsing systems

Select **Config > Auto Discovery** or click on the Auto Discovery icon  on the toolbar menu to display the Auto Discovery dialog box.



This window displays all Desktop Management Interface (DMI) systems in your network detected by the ASM Pro MIF Browser.

The following items are available in this dialog box:

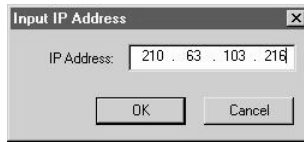
Item	Description
System Found	Displays all the DMI systems available on your network
System Selected	Shows all the systems to be monitored by ASM Pro MIF Browser
Button	Description
Add	Appends the highlighted DMI systems in the System Found list to the System Selected list
Remove	Deletes the highlighted system from the System Selected list
Manual Add	Manually adds an IP address
Sweep	Searches an address by matching the first three parts of the IP address that you specify
Close	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now contains all the system you specified in the System Selected list.
Refresh	Refreshes the information display in the System Found panel



Note: For the auto discovery function to work properly, the agent must install Intel DMI Service Provider 2.0. Refer to the DMI 2.0 Service Provider SDK Release 1.0 for more information.

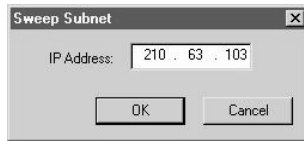
Manually adding a system

To manually add a system, type the IP address of the system in the text box and then click **OK**. If found the system is displayed in the System List Combo box and MIF Tree window. If the address is not found, it displays a not found message.



Sweeping subnets

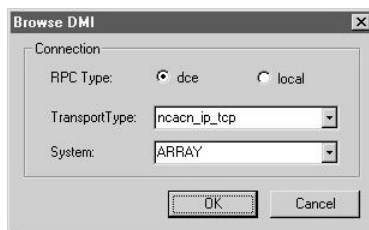
To sweep subnets, type the first three address blocks of the subnet and click **OK**. If the sweep finds a system in the subnet, it is displayed in the System List Combo box and MIF Tree window. If the sweep does not find anything, it displays a not found message.



Starting a new connection

When you start MIF Browser, it follows a default setting connection configuration described in the Browing Options window (see next section). However, you can use this function to make a new connection without following this configuration.

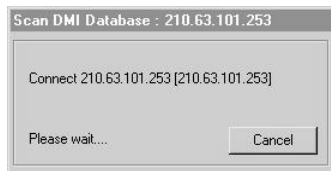
Select **File > New** to start a new connection. The Browse DMI window displays.



Item	Description
RPC Type	MIF Browser supports two kinds of RPC (Remote Procedure Call) types: dce (remote) and local
Transport Type	Defines a transfer protocol for your default connection. Lists all the protocols available to the system
System	Lists all systems included in the MIF Tree window. Choose a system you want to connect to, or type its IP address.

To make a new connection:

1. Choose the type of RPC you want to use.
2. Choose a transport type from the pulldown list.
3. Choose the system you want to connect to in the pulldown list
4. Click **OK** to connect. A message dialog box appears.

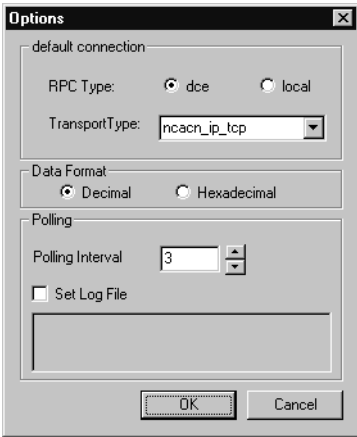


5. Click **Cancel** to stop the process.

Setting up browsing and default connection options

Browsing options allow you to preset configurations for the MIF Browser. This includes connection features, data formats, and polling intervals.

Select **Config > Options** to display the Configure Options dialog box.



Item	Description
RPC Type	MIF Browser supports two kinds of RPC (Remote Procedure Call) types: dce (remote) and local
Transport Type	Defines a transfer protocol for your default connection. Lists all the protocols available to the system
Data Format	Displays data format in decimal or hexadecimal
Polling Interval	Defines the number of seconds between polling sessions
Set Log File	Stores information gathered from the system in a file
Button	Description
OK	Closes the dialog box and causes the modifications you made to take effect
Cancel	Closes the dialog box, discarding all changes made

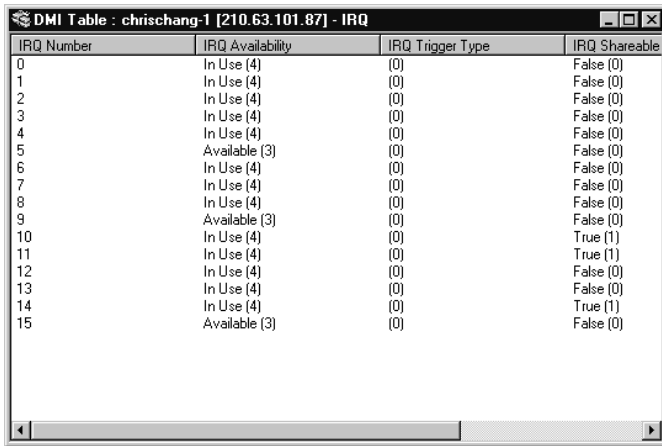
Browsing the DMI table

A DMI table is displayed in the information window when you double-click a DMI table attribute. To view information in the table, you can either use the **Next Row**, **First Row**, or **Browse** button.

Select **Operation > Next Row** or click the **Next Row** button to cycle through the table one row at a time until it reaches the end of the table.

Select **Operation > First Row** or click the **First Row** button to go back to the beginning of the table.

Select **Operation > Browse** or click the **Browse** button to display table attributes in the browse window. This way you can see several rows at a time as shown below.



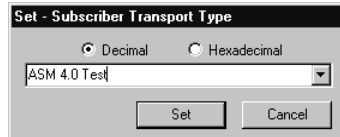
IRQ Number	IRQ Availability	IRQ Trigger Type	IRQ Shareable
0	In Use (4)	(0)	False (0)
1	In Use (4)	(0)	False (0)
2	In Use (4)	(0)	False (0)
3	In Use (4)	(0)	False (0)
4	In Use (4)	(0)	False (0)
5	Available (3)	(0)	False (0)
6	In Use (4)	(0)	False (0)
7	In Use (4)	(0)	False (0)
8	In Use (4)	(0)	False (0)
9	Available (3)	(0)	False (0)
10	In Use (4)	(0)	True (1)
11	In Use (4)	(0)	True (1)
12	In Use (4)	(0)	False (0)
13	In Use (4)	(0)	False (0)
14	In Use (4)	(0)	True (1)
15	Available (3)	(0)	False (0)

Changing table Attribute Value

Select **Operation > Edit** or click the **Edit** button to change attribute value in the table document. This function is available if the table has the write attribute. The table attribute value can be set if the attribute is R/W (Read/Write) or Write. If the table attribute you chose is not R/W or Write, the **Set** button is disabled.

For Integer and String Attributes

Type the new value in the text box and then click **Set** to save changes. Click **Cancel** to disregard changes.

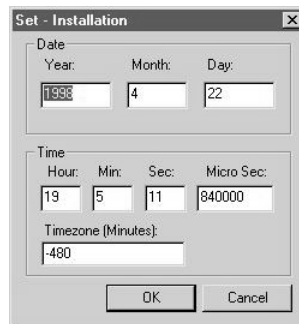


The dialog box titled "Set - Subscriber Transport Type" contains two radio buttons: "Decimal" (selected) and "Hexadecimal". Below them is a text box containing the text "ASM 4.0 Test". At the bottom are two buttons: "Set" and "Cancel".

The attribute value can be viewed in two ways: Decimal and Hexadecimal. Click the radio button to toggle between views.

For date attributes

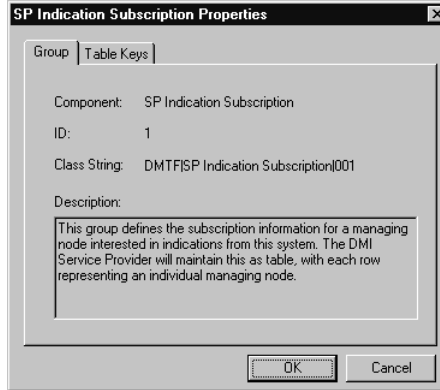
Type the new value in the text box as indicated and then click **OK** to save changes. Click **Cancel** to disregard changes.



The dialog box titled "Set - Installation" has a "Date" section with fields for Year (1998), Month (4), and Day (22). Below this is a "Time" section with fields for Hour (19), Min (5), Sec (11), and Micro Sec (840000). There is also a "Timezone (Minutes)" field with the value -480. At the bottom are "OK" and "Cancel" buttons.

Viewing table document properties

Select the table item from the MIF Tree Window, and select **Operation > Property** or click the **Property** button to view table document properties. Table property items may vary for different table documents.

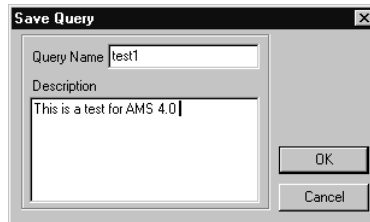


Defining a new query

This dialog box allows you to specify a name and description for a list of frequently viewed MIF items, and saves this information to the database. This eliminates the need to individually search for the same sets of MIF items to view each time you start ASM Pro MIF Browser. After setting a query, it is added to the Name field in the Select Query dialog box.

Follow these steps to define a new query (set a list of attributes to view):

1. Highlight an attribute or a list of attributes in the information window and select **Query > Add Item** or click the **Add Item** button to add the attributes to the query window. If you want to remove an item in the query window, select **Query > Remove Item** or click the **Remove item** button.
2. Select **Query > Define New Query** or click the **Define New Query** button to create a new query file. The Save Query window appears.



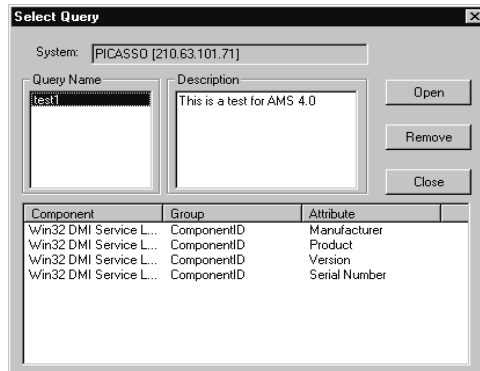
3. Type a name and description for the query.

4. Click **OK** to save it.

Each time you want to view this list, simply select its name from the Select Query dialog box. Refer to “Selecting a query” on page 253.

Selecting a query

Select **Query > Select a Query** to choose from or remove a list of previously defined attributes to view. The Select Query dialog box appears.



This dialog box allows you to choose from a list of previously defined queries. It also places all attributes in this query into the Query window. You can also remove queries from the database or clear the database of all queries.

Select query dialog box items

Item	Description
System	Shows the name or address of the system you are currently browsing
Query Name	All query names defined in the Define New Query dialog box are listed here. Click the name of the query you want to view from the database
Description	Displays a brief description of the selected query
Button	Description
Open	Opens the selected query
Remove	Removes the selected query from the database
Close	Closes the dialog box, discarding all changes made

9 Asset Manager

Asset Manager gathers information about the hardware and software configuration of each system being monitored by the ASM Pro Console. This information is saved in an asset log file for future reference.

► Introduction

Asset Manager consists of four parts:

- Asset Control - shows you the hardware and software configuration of the system currently being monitored.
- Asset Statistics Information - summarizes the hardware information contents of two or more systems.
- Asset Log - Displays the asset log and saves it to disk.
- Asset History - Shows a comparison of two or more asset log versions of a system.

Select one of the following methods to run Asset Manager from the Console:

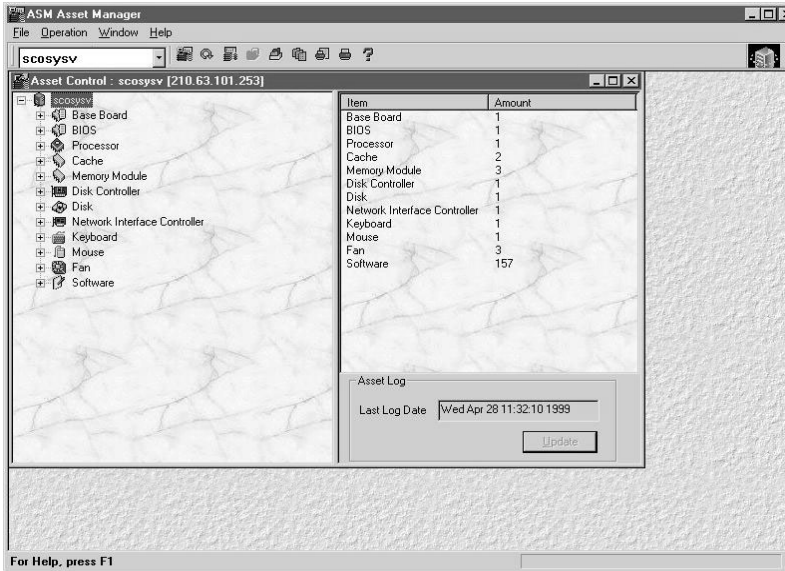
- Select **Asset Manager** from the Utility menu.
- Click the **Asset Manager** icon in the toolbar.

The Asset Manager works with ASM Pro Agent. If the monitored system is not an ASM Pro agent, the “Cannot Load Asset Log File” message appears.

► Asset Manager user interface

This section discusses the following major components:










- Menu bar and Toolbar
- System List Combo Box
- Auto Discovery



Menu bar and toolbar

The toolbar, located at the top of the Asset Manager window, contains two components: the System list box and the toolbar buttons.

The toolbar buttons allow quick access to selected Asset Manager functions via a single mouse click. You can also access all of these functions from the menu bar.

Icon	Description
	Get Asset Information. Activates the Asset Control window and displays information about the currently monitored server or desktop
	Refresh. Refreshes the display information in the active window
	Statistics. Activates the Asset Statistics Information window and displays hardware summary information about the chosen server(s) or desktop(s)
	Asset Log. Displays the asset list log of a system. It is automatically generated every time you start Asset Manager
	Show Asset Log. Shows the difference between the asset list log versions of a system
	Show Asset History. Activates the Asset Information Query window to help you find the information you are looking for
	Preview. Displays the layout and format of information to be printed
	Print. Prints information regarding the server or desktop currently being monitored
	Help. Presents help information

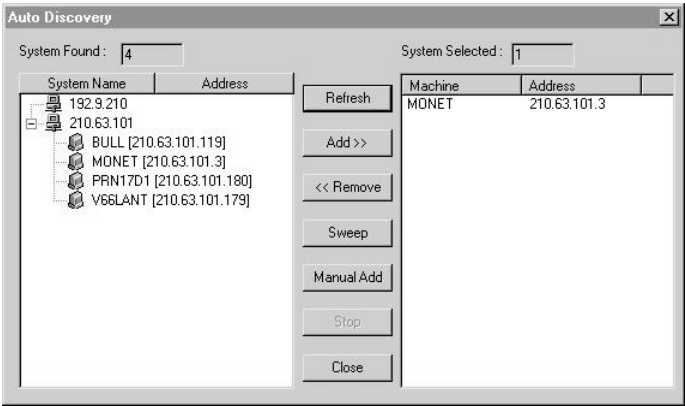
System list combo box

The System list box lists all the servers and desktops available for monitoring. Use this box to select the name of the system you want to view.



Auto Discovery

From the File menu, select **Auto Discovery** to display the Auto Discovery dialog box.



This window displays all IP/IPX systems in your network. The following items are available in this dialog box.

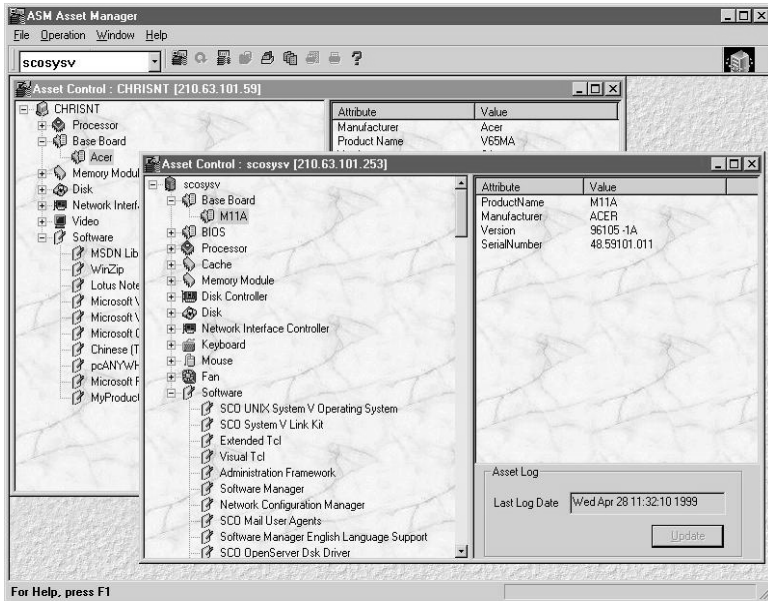
Auto Discovery dialog box items

Item	Description
Systems Found	Displays all the IP/IPX systems available on your network
Systems Selected	Shows all the systems to be monitored

Item	Description
Button	Description
Add	Appends the highlighted systems in the Systems Found list to the Systems Selected list
Remove	Deletes the highlighted systems from the Systems Selected list
Sweep	Searches an address by matching the first three blocks you specify
Manual Add	Allows you to manually add an IP address
Stop	Immediately halt the discovery operation if it is running
Close	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now contains all the systems you specified in the Systems Selected list

▶ Asset control

The Asset Control window displays the hardware and software configuration of a system. Clicking on an item with a plus (+) sign shows you one or more devices available for that item.



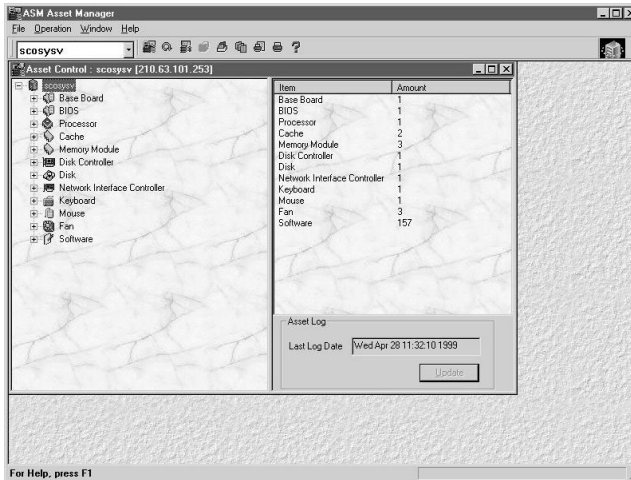
Asset Control also monitors the hardware and software changes within a system. It compares the devices currently installed in the system with the ones recorded earlier in the asset list log file.

If Asset Manager detects any changes within the system, like installing a new device or software, or replacing or removing old devices or software, it displays a question mark beside the device.

Once a change has been made, it shows the number of devices that have been removed or installed in the system. For example, 0 to 1 means that a device has been added to the system. 1 to 0 means that a device has been removed.

► Updating hardware and software information

The question mark on the item displays every time a device is installed, replaced or removed within the system. You can confirm these changes by clicking on the **Update** button of the Asset Log dialog box.

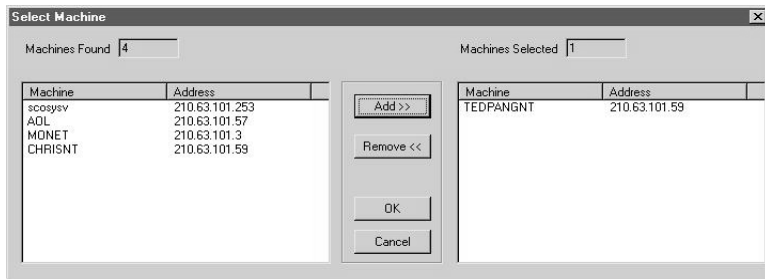


The Asset Log dialog box automatically updates the log file and displays the date and time of the latest update.

► Asset statistics information

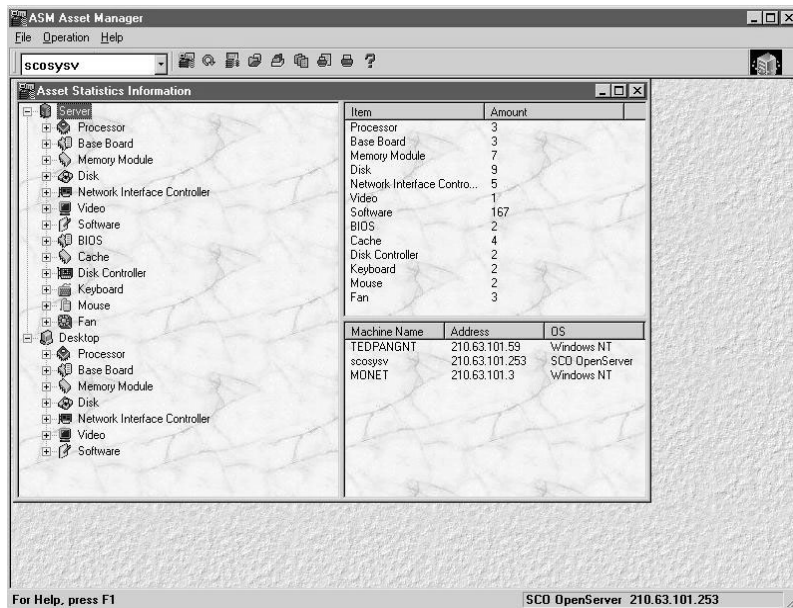
The Asset Statistics Information window collects the total number of hardware devices and software components installed in a system and displays them for your reference. You can choose one or more systems at the same time as shown below.

Select **Operation > Asset Statistics Information** or click on the **Asset Statistics Information** icon on the toolbar to display the Select System window.



To select a system:

1. Click on the name of the agent you want to view from the left panel. To make multiple selections, hold down the Control key and click on the names of all the agents you want to view.
2. Click the **Add** button. The system you selected moves to the Systems Selected window.
3. Repeat steps 1 and 2 if you want to add more systems. When you have finished adding, click **OK**. The Asset Statistics Information window appears.



The left window displays all the items currently available to all the servers or desktops being monitored. Clicking an item with a plus (+) sign displays the type of device and the total number of the device installed in the servers or desktops being monitored.

The upper right side of the screen displays the types of devices, and the total number of devices and software components. The lower right side displays the servers and desktops currently being monitored. Click on one of the systems to see the number of devices installed in that system.

► Asset information query

The Asset Information Query is a search function that helps you find what you are looking for. It can only be activated in the Asset Statistics Information window. Choose an item in the Asset Statistics Information window, and click the **Asset Information Query** icon on the toolbar to activate the window below.

Item	Amount
Pentium Pro	1
Pentium Pro	1

Machine Name	Address	Amount
scosysv	210.63.101.253	1
MONET	210.63.101.3	1

The left side of Asset Information Query window lists a number of fields that are associated with the type of item you chose.

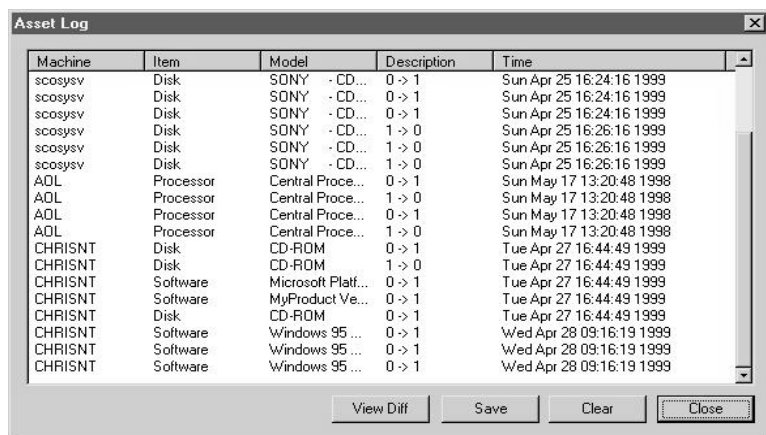
You encounter two types of fields in this window:

- Search fields - are used to specify the device you want to find in the servers or desktops being monitored.
- Numeric operator field - is used when you encounter a numeric input such as the capacity of a hard disk drive. Select one of the operators (<, =, or >) and type in the capacity of the device you want to find and click **Query**. Asset Query displays anything that matches your search items in the device list window.

The item list box lists all of the items allocated to the servers and desktops being monitored. Click on the pulldown menu to see a list of items available and click one of them to search a device in that item.

► Asset log

The Asset Log window displays the systems that have undergone hardware or software changes. You can save this information to a file for future reference. Choose an item in the Asset Control window and select **Operation > Asset Log** or click the **Asset Log** icon on the toolbar to activate the window below.



The screenshot shows a window titled "Asset Log" with a table containing the following data:

Machine	Item	Model	Description	Time
scosysv	Disk	SONY --CD...	0 -> 1	Sun Apr 25 16:24:16 1999
scosysv	Disk	SONY --CD...	0 -> 1	Sun Apr 25 16:24:16 1999
scosysv	Disk	SONY --CD...	0 -> 1	Sun Apr 25 16:24:16 1999
scosysv	Disk	SONY --CD...	1 -> 0	Sun Apr 25 16:26:16 1999
scosysv	Disk	SONY --CD...	1 -> 0	Sun Apr 25 16:26:16 1999
scosysv	Disk	SONY --CD...	1 -> 0	Sun Apr 25 16:26:16 1999
ADL	Processor	Central Proce...	0 -> 1	Sun May 17 13:20:48 1998
ADL	Processor	Central Proce...	1 -> 0	Sun May 17 13:20:48 1998
ADL	Processor	Central Proce...	0 -> 1	Sun May 17 13:20:48 1998
ADL	Processor	Central Proce...	1 -> 0	Sun May 17 13:20:48 1998
CHRISNT	Disk	CD-ROM	0 -> 1	Tue Apr 27 16:44:49 1999
CHRISNT	Disk	CD-ROM	1 -> 0	Tue Apr 27 16:44:49 1999
CHRISNT	Software	Microsoft Platf...	0 -> 1	Tue Apr 27 16:44:49 1999
CHRISNT	Software	MyProduct Ve...	0 -> 1	Tue Apr 27 16:44:49 1999
CHRISNT	Disk	CD-ROM	0 -> 1	Tue Apr 27 16:44:49 1999
CHRISNT	Software	Windows 95 ...	0 -> 1	Wed Apr 28 09:16:19 1999
CHRISNT	Software	Windows 95 ...	0 -> 1	Wed Apr 28 09:16:19 1999
CHRISNT	Software	Windows 95 ...	0 -> 1	Wed Apr 28 09:16:19 1999

At the bottom of the window are four buttons: "View Diff", "Save", "Clear", and "Close".

Items	Description
System	Shows the monitored systems that undergo a hardware or software change
Item	Shows the kind of device or program that was changed
Model	Shows the model name of the item
Description	Shows a brief description of the items added or removed from the system
Time	Shows when the change occurred

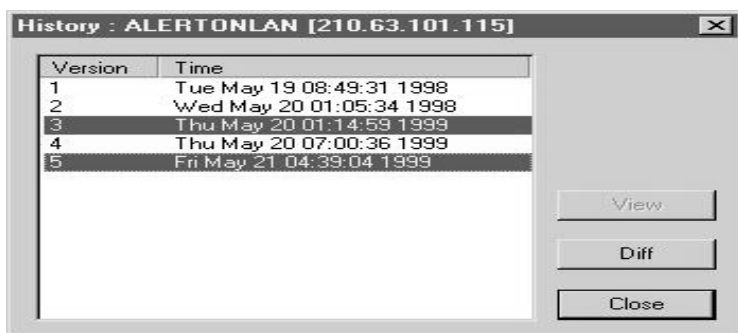
To save the log file, click the **Save** button and choose a filename for the log.

To erase the list, click the **Clear** button.

To view the difference between two log versions, click the **View Diff** button. Refer to “Viewing and comparing different log versions” on page 269 for more information.

► Asset history

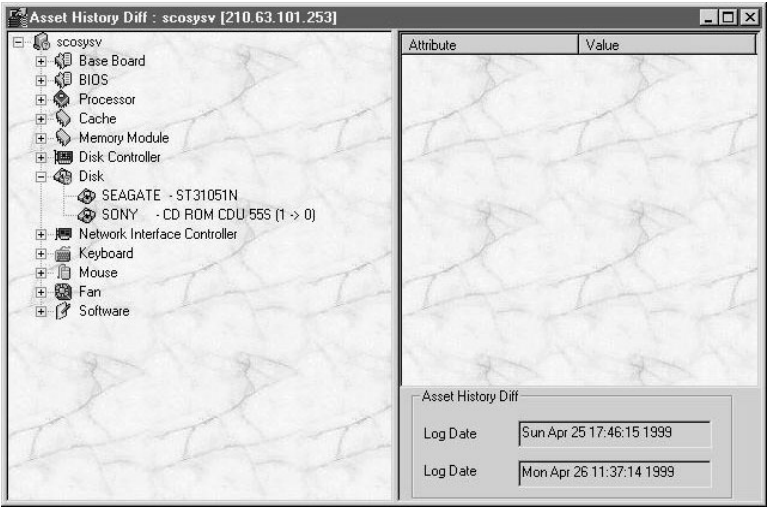
The Asset History window displays a list of log versions with their date. You can view each version independently or compare two log versions to view the hardware and software configurations of the system. Choose an item in the Asset Control window and select **Operation > Asset History** or click the **Asset History** icon on the toolbar to activate the window below.



Viewing and comparing different log versions

You can select two log versions and compare their hardware and software configuration status. Select two log versions in the Asset History window and then click the **Diff** button. The Asset History Diff window appears.

To view a log version, select the version you want and click **View**. The Asset History Window appears.



A question mark beside a device means that the device has been changed. Select one of the devices to view its attributes and value.

10 Statistics Viewer

Statistics Viewer is an optional package that records and displays system utilization information about the systems being monitored that can be saved for future reference.

► Adding Statistics Viewer to your system

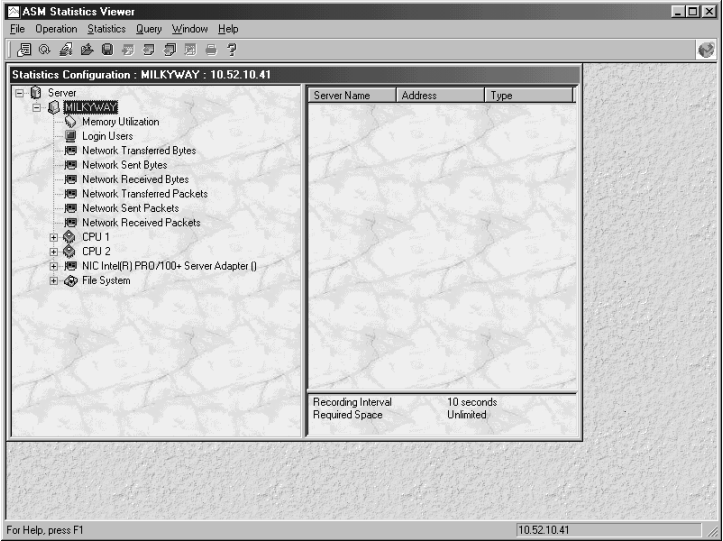
To add Statistics Viewer to your system, select **Custom** as the setup type during ASM Pro Console installation, then select **Utility**, and click **Change**.

Use one of the following ways to run Statistics Viewer from Console:



- Select **Statistics Viewer** from the Tools menu.
- Click the **Statistics Viewer** icon in the toolbar.









► Statistics Viewer user interface

The following figure illustrates the Statistics Viewer window, which is its primary user interface.



The Toolbar buttons provide quick access to selected Statistics Viewer functions. You can also access these functions from the menu bar.

Icon	Description
	Bring up Statistic Configuration. Brings the Statistics Configuration window to the forefront when you have multiple windows open.
	Refresh. Refreshes the display of information in the active window.

Icon	Description
	Setup Statistic Item. Sets the statistical recording method.
	Open Query. Displays the previously saved query file.
	Save Query. Saves new query file information to disk.
	Add Item. Adds a selected item to the viewing window.
	Remove Item. Removes an item from the viewing window.
	Remove All. Clears the viewing window.
	View Statistical Information. Displays the Statistics Graph View window.
	Print. Prints query files.

To record the utilization data, highlight an agent, and click the Setup toolbar button to open the Setup window, shown below.

From the setup window, select the item you want to record, then click on the record button. Press the Apply button to start recording.



The Item column lists the items that can be recorded. The Record Status column indicates whether the item is being recorded (“Recording”) or is not recorded (“N/R”).

To select item(s) for recording:

- Highlight the item(s) you want to record and click the **Record** button.



Note: The Record Status for the item(s) changes from “N/R” to “Recording.”

- Click **Start** to start the recording process.

To deactivate the recording of items, highlight the items, and click the **Not Record** button. The Record Status for the items changes to “N/R.”

To deactivate the recording of all selected items, click the **Clear** button.

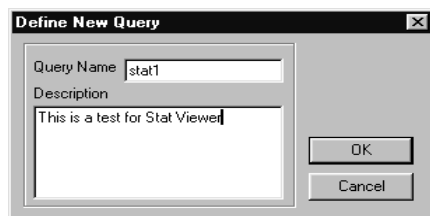
To specify the recording interval and file size for each item you are recording, use the items in the Recording Parameters section.

The Recording Interval specifies the amount of time that elapses between the times that Statistics Viewer obtains information from the monitored system. The minimum time interval is 10 seconds; the maximum is one hour.

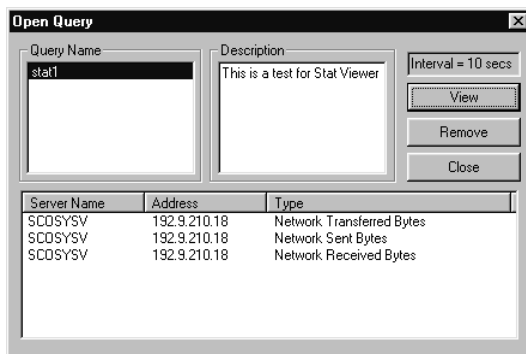
The Record Size limits the number of records that are recorded for each item. Choose **Limited** and specify the number of allowable records for each item. The Required Space field is calculated automatically based on the number of records that you specify. Choose Unlimited for unlimited file size.

► Saving and loading query files

You can save recorded utilization information for future reference. To do this, click the **Save Query** button, or Query Save, after the desired utilization information has been recorded. The following Define New Query dialog box appears to allow you to name and describe the query file.



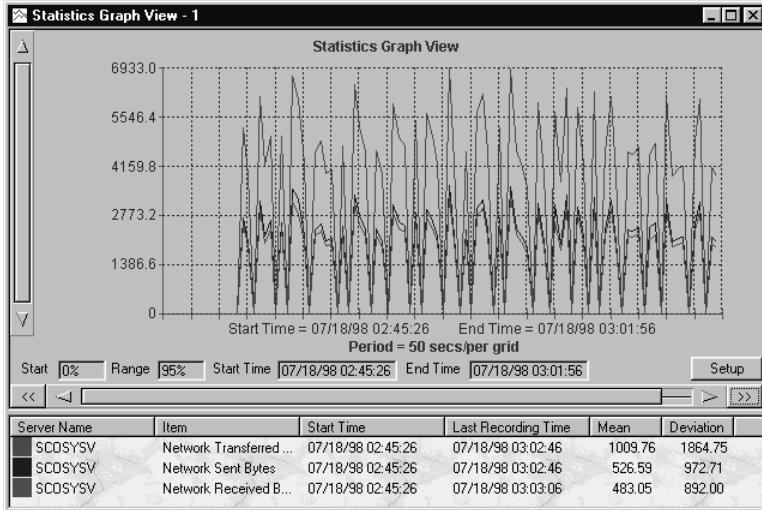
To open an existing query, click the **Open Query** toolbar button. The following Open Query dialog box appears.



To specify the query file you want to load, highlight its name and click the **View** button. The **Remove** button erases highlighted query files; the **Close** button closes the dialog box.

► Working with statistics graph view

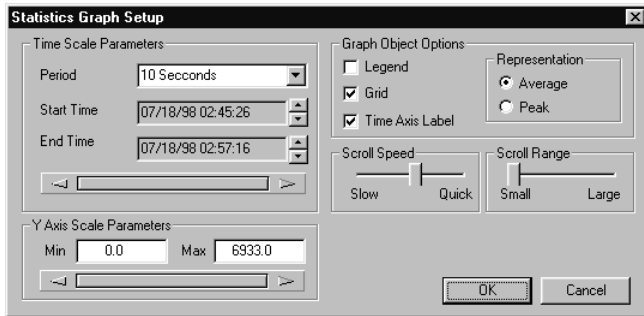
The Statistics Graph View window displays item utilization graphically. It is a “snapshot” of selected utilization statistics information. The y-axis (vertical) indicates utilization frequency; the x-axis (horizontal) indicates utilization start and end times.



The legend below the graph lists the names of the items whose utilization information is displayed by the line graph. Their colors correspond to the colored lines on the graph.

The legend lists the server name, the name of the item being recorded, recording start and stop times, and utilization mean and deviation. The mean measures average utilization, while the deviation measures the difference of the utilization against a fixed value.

To specify the information you want the line graph to display, click the **Setup** button in the Statistics Graph View window. The following Statistics Graph Setup window displays.



Use the Time Scale Parameters section to set the time intervals between each grid (x-axis) on the graph. The display bar at the bottom of this section focuses the graph display to a limited time frame.

Use the Y-Axis Scale Parameters section to set the minimum and maximum values for the y-axis. The display bar at the bottom of this section focuses the graph display to a limited performance frame.

Use the checkboxes in the Graph Object Options section to enable/disable display of:

- the legend below the graph that acts as a key to the data being graphed
- grid lines that appear in the body of the graph to improve readability
- labels beneath the x-axis that indicate the recording time interval

Use the Average and Peak radio buttons to specify the type of performance data you want the graph to display.

11 Alert via LAN

The ASM Pro Alert via LAN (Local Area Network) function allows administrators to monitor and reconfigure local systems via a network.




▶ Alert via LAN Manager function



To launch the Alert via LAN function on a server system, do one of the following:

- Select **Admin > Alert via LAN Manager** from the ASM Pro Main menu
- Click on the **Alert via LAN** button from the ASM Pro toolbar

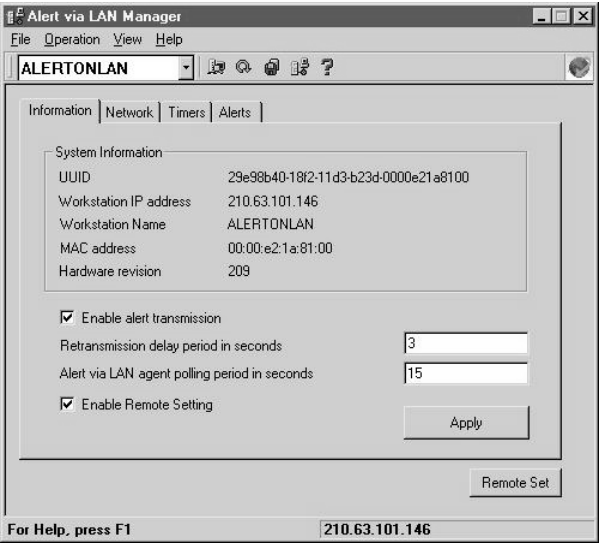
Menu bar and toolbar

The menu bar and toolbar are located at the top of the Alert via LAN Manager window. The table below describes the function of each menu item and toolbar icon.

Item	Icon	Description
File Menu		
Exit		Choose this command to close the Alert via LAN Manager window
Operation Menu		
Add Client		Allows the administrator to add local system(s) to the list of systems currently connected to the server. Selecting this command displays the Input IP Address dialog box To add a local system, simply enter the IP address of the desired local system in the IP Address textbox then click on OK
Refresh		Choose this command to update the local system information currently displayed on the screen
Save Config		Allows the administrator to save the local system configuration. This function is the same as clicking on the Set button located at the bottom of the Alert via LAN Manager window

Item	Icon	Description
View Menu		
Toolbar		Display or hide the Toolbar, i.e., the buttons just below the Menu bar. When the Toolbar is displayed, a check mark appears beside the command item
Status Bar		Display or hide the Status bar, i.e., the bar located along the bottom of the window. When the Status bar is displayed, a check mark appears beside the command item
Help Menu		
Help Topics		Opens the Alert via LAN Manager Help. This Help file contains information on how to use the Alert via LAN Manager function
About Alert Via LAN		Displays the copyright notice and the version number of the Alert via LAN Manager utility

Information tab



Item	Description
System Information	Displays the system configuration of the local system currently being monitored

Item	Description
Enable alert transmission option	<p>Activates the alert function. Once an alert packet is issued, notification methods specified in the Alerts page are automatically performed</p> <p>Retransmission delay period in seconds - specifies the period (in seconds) after which retransmission of an alert packet is repeated</p> <p>Alert on LAN agent polling period in seconds - specifies the period (in seconds) after which the server system repeats the polling process</p>
Enable Remote Setting option	<p>Allows the administrator to reconfigure the local system via the network. If this option is disabled, the local system information that appears on the server screen becomes nonconfigurable</p>

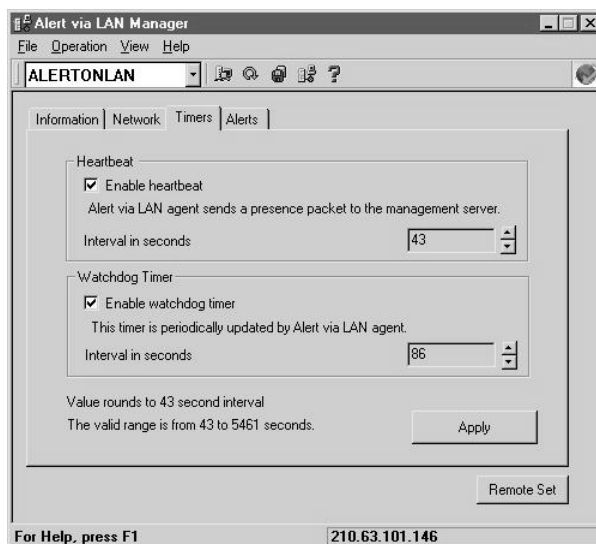
After you have entered your settings, click on the **Apply** button.

Network tab



Item	Description
Admin Console IP Address	Specifies the IP address of the server system to which the local system is connected
Admin Console Port	Specifies the port used by the local system for sending alert packets

Timers tab

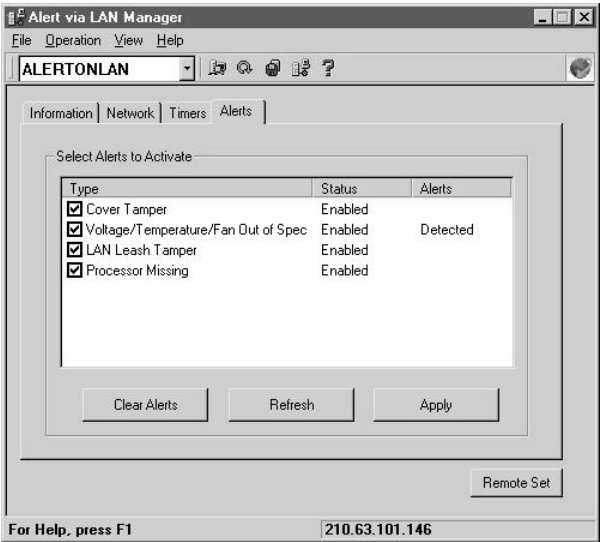


Item	Description
Heartbeat: Enable heartbeat	When enabled, the server checks for the heartbeat signal sent by the local system to determine its connection status Interval in seconds - specifies the period (in seconds) after which, if the server does not detect any heartbeat signal, the local system is automatically considered disconnected
Watchdog Timer: Enable watchdog timer	When enabled, the local system's processor checks for any register setting change to verify its status Interval in seconds - specifies the period (in seconds) after which, if no register setting is detected, the local system is considered to be OFF

The Valid period setting for both the Heartbeat and Watchdog timers range from 43 to 5,461 seconds.

After you have entered your settings, click on the **Apply** button.

Alerts tab



Item	Description
Select Alerts to Activate	Specifies the local system's hardware parameters to monitor
Alert Action	Specifies the notification methods that Alert via LAN utility performs once a local system issues an alert packet

To clear all settings on the Alerts page, click on the **Clear Alerts** button. This disregards the previous settings and the settings which you have just entered.

To refresh the page information to its saved settings, click on the **Refresh** button.

To save your settings, click on the **Apply** button.

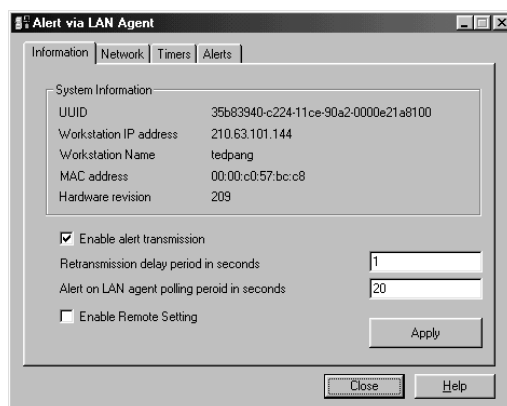
Saving the Alert via LAN Manager settings

After you have configured the Alert via LAN function, click the **Set** button for the changes to take effect.

► Alert via LAN local function

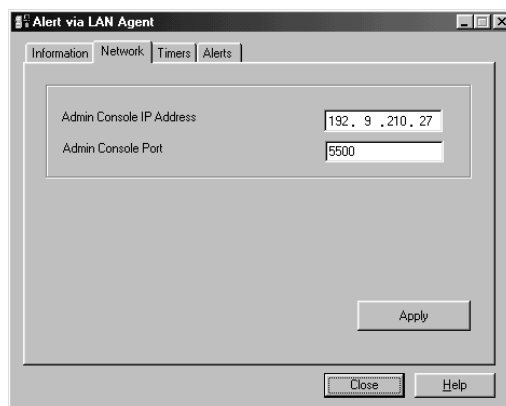
To launch the Alert via LAN function on a local system, click on the **Alert via LAN** icon located on the Taskbar.

Information tab



The Information tab of the Alert via LAN Agent window displays the system configuration of the local system. The parameters that appear here are exactly the same as those in the Alert via LAN Manager window. Refer to “Information tab” on page 287 for the description of these parameters.

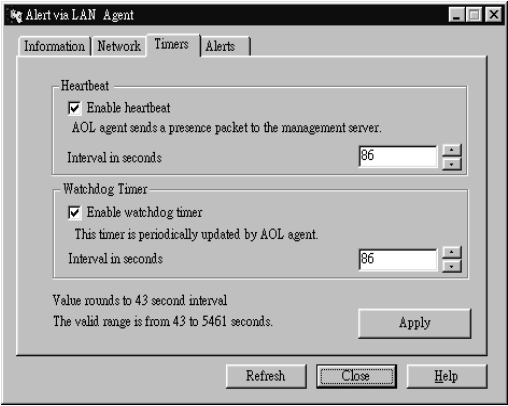
Network tab



Item	Description
Admin Console IP Address	Specifies the IP address of the server system to which the local system is connected
Admin Console Port	Specifies the local port used by the local system for sending alert packets

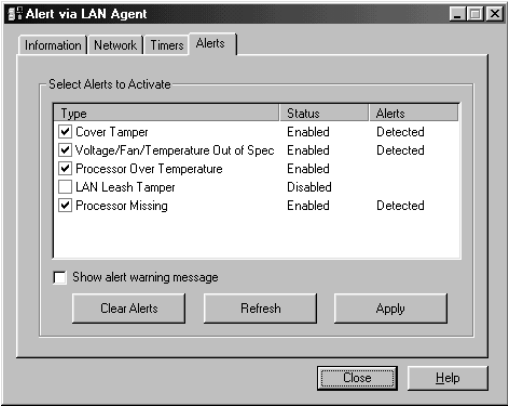
Click on the **Apply** button for your settings to take effect.

Timers tab



This page is exactly the same as the Alert via LAN Manager Timers tab. For more information, refer to “Timers tab” on page 289.

Alerts tab



Item	Description
Select Alerts to Activate	Specifies the local system's hardware parameters to monitor
Show alert warning message	When this option is enabled, a warning message appears once an alert packet is detected

To clear all settings on the Alerts page, click on the **Clear Alerts** button. This disregards the previous settings and the settings which you have just entered.

To refresh the page information to its saved settings, simply click on the **Refresh** button.

To save your settings, simply click on the **Apply** button.

Updating the onscreen information

To update the onscreen system information, simply click on the **Refresh** button.

Quitting alert via LAN agent

To close the Alert via LAN Agent window, simply click on the **Close** button.

Getting help information

If you need help on how to reconfigure the Alert via LAN Local function and move around the window, simply click on the **Help** button. This displays the Alert via LAN Agent Help topics.

12 Remote Console

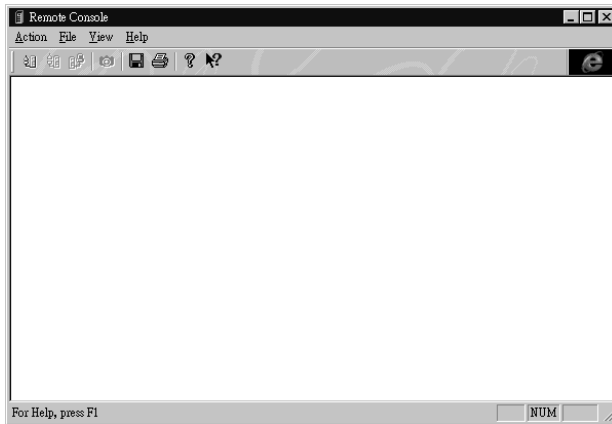
The Remote Console function allows you to control the ASM Pro agent systems through the Local Area Network (LAN).

► Remote Console administrator function

To activate the Remote Console administrator function do one of the following:

- Select the **Admin > Remote Control Console** from the ASM Pro main menu
- Click on the **Remote Console** button from the ASM Pro toolbar
- Run the Remote Console program from the ASM Pro Console program group

The Remote Console window appears on the screen:



Menu bar and toolbar

The menu bar and toolbar are located at the top of the Remote Console window. The table below describes the function of each menu item and toolbar icon.

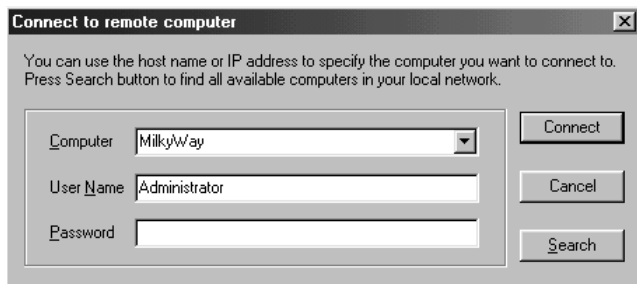
Item	Icon	Description
Action menu		
Connect		Choosing this command enables the administrator to establish connection to an ASM Pro agent system.
Disconnect		Choosing this command automatically disconnects the existing server-client connection
File Transfer		Opens the File Transfer window, allowing the server to send and receive files from an ASM Pro agent system. For more details, refer to “File transfer function” on page 302
Snapshot		Allows you to copy the currently displayed image on the screen and store it onto the Clipboard
File menu		
Save Image		This command allows you to save the currently displayed image on the screen as a .BMP file
Save Image As		This command allows you to save an existing image file to another filename
Print Image		This command lets you print the currently displayed screen
Print Preview		This command lets you check the layout and format of the file before actually printing it

Item	Icon	Description
Print Setup		This command allows you to configure the printer according to your preferences
Exit		Choose this command to close the Remote Console window
View menu		
Toolbar		Displays or hides the toolbar, i.e., the buttons just below the menu bar. When the toolbar is displayed, a check mark appears beside the command item
Status Bar		Displays or hides the status bar, i.e., the bar located along the bottom of the window. When the status bar is displayed, a check mark appears beside the command item
Help menu		
Help Topics		Opens the Remote Console Help. This Help file contains information on how to use the Remote Console function
About Remote Console		Displays the copyright notice and the version number of the Remote Console utility

Establishing a connection to an ASM Pro server system

To establish connection to an ASM Pro system:

1. Select **Action > Connection** or click on the **Connect** button on the toolbar. The Connect to remote computer dialog box appears.



2. Enter the name or the IP address of the desired ASM Pro server system. You may also click on the **Search** button to view a list of available systems you can connect to. If the password function of the ASM Pro server system is enabled, you are prompted to enter the correct password.
3. Enter the correct password in the Password textbox.
4. Click on **Connect** to proceed with the connection process or **Cancel** to disregard the entry that you have just entered.

Once connection is established, you can access the selected ASM Pro agent system from your site.

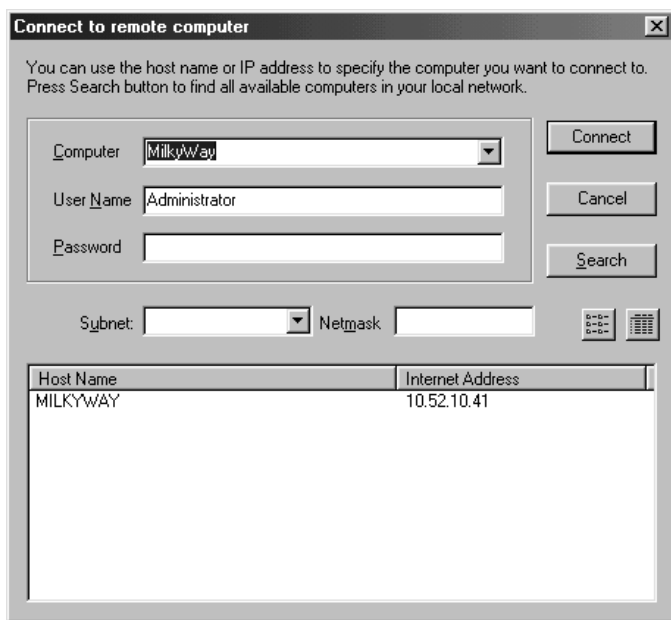
File transfer function

The File Transfer function of the Remote Console application enables the server to send and receive files from any ASM Pro agent system. It is based on the standard file transfer protocol (FTP). But unlike FTP which uses the standard FTP port, File Transfer uses a private port to avoid conflicts with FTP.

To enable the File Transfer function, do either of the following:

- From the Remote Console menu, select **Action > File Transfer** or
- Click on the **File Transfer** button from the Remote Console toolbar.

The File Transfer window appears on the screen.



The server's file information appears in the top box, while the currently connected remote system's file information appears in the bottom box. The lower box displays the time, file and error messages for all transfers.

Disconnecting from an existing remote console connection

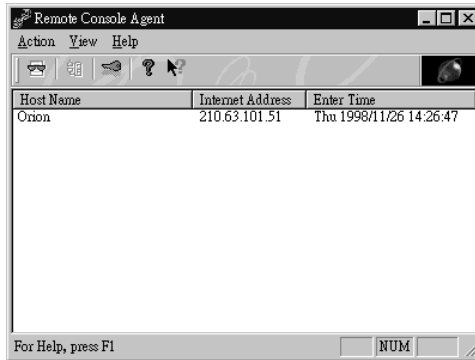
To disconnect, do one of the following:

- Select **Action > Disconnect** from the menu bar
- Click on the Disconnect button from the Toolbar.

► Remote console server function



The Remote Console server function is automatically enabled when a system boots up. To display the Remote Console window on the agent system, simply click on the **Remote Console Server** icon located on the taskbar.





The Remote Console Server window appears on the screen:



Menu bar

The menu bar is located at the top of the Remote Console Server window. It contains the following menus:

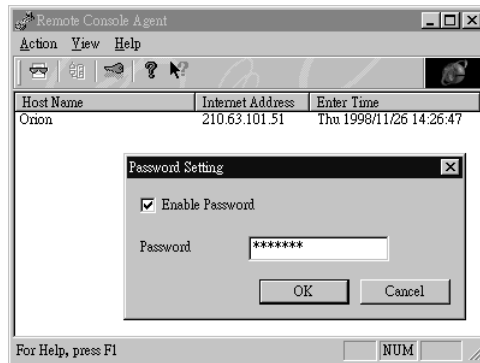
Item	Icon	Description
Action menu		
Hide		Minimizes the screen and reduces it into an icon on the taskbar. To restore the window, simply click on the icon
Enable Command		Enables the Remote Console function. When enabled, it allows you access to control the server system

Item	Icon	Description
Disable Command		Disables the Remote Console function
Disconnect		Automatically disconnects the existing server-client connection
Set Password		Sets a password to protect your system from unauthorized access
Exit		Closes the Remote Console Agent window
View menu		
Toolbar		Displays or hides the Toolbar, i.e., the buttons just below the Menu bar. When the Toolbar is displayed, a check mark appears beside the command item
Status Bar		Displays or hides the Status bar, i.e., the bar located along the bottom of the window. When the Status bar is displayed, a check mark appears beside the command item
Help menu		
About Remote Console		Displays the copyright notice and the version number of the Remote Console Agent utility
Help Topics		Opens the Remote Console Agent help

Setting a password

To set a password:

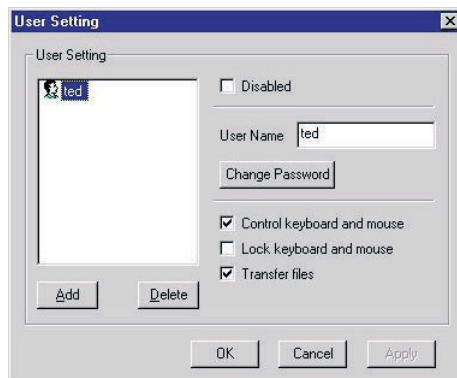
1. Select **Action > Set Password** from the menu bar, or click the **Set Password** button on the toolbar. The Password Setting dialog box appears:



2. Click on the **Enable Password** option.
3. Enter your password in the Password textbox then click on **OK**.

User setting

This option allows administrator to set the users' names and passwords and privileges. When you choose this command, the User setting dialog box automatically appears.



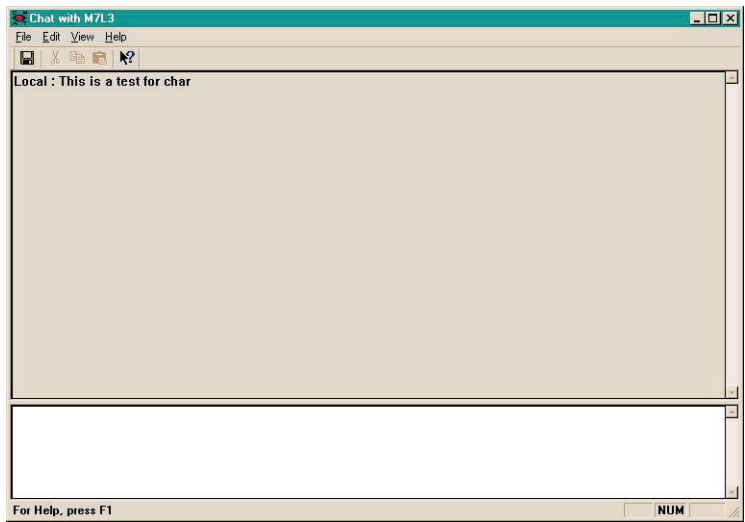
You can add or remove users by selecting the user's name and then clicking Add or Delete. The Disable checkbox prevent the user from any access to remote console. This is a nice way of suspending the user without erasing the user from the list.

To add a new user:

1. Type the name of the user in the User Name edit box.
2. Click the **Password** button to assign or change the password of the user.
3. Choose one of the attributes of the user by clicking the attribute checkboxes.
4. Click the **Add** button to add the user into the list.
5. Click **OK** to exit.

► Chatting

The chat function enables the client user to chat with the server user. This feature is based on TCP. The chat function is enabled only when a connection has been established.



Item	Icon	Description
File Menu		
Save		Save the conversation on screen to a file
Exit		Quits chatting
Edit Menu		
Undo		Undo the last function
Cut		Cuts the selection and put it on the Clipboard

Item	Icon	Description
Copy		Copies the selection and put it on the Clipboard
Paste		Inserts Clipboard contents
View Menu		
Toolbar		Displays or hides the toolbar, i.e., the buttons just below the menu bar. When the toolbar is displayed, a check mark appears beside the command item
Help Menu		
Help Topics		Opens the Remote Console Help. This Help file contains information on how to use the Remote Console function

The window is split into two views. At the bottom of the window is the input area and at the top is the display area (read-only). Type your messages in the input area and then press the **Enter** key on your keyboard to send.

To open the Chat function for Remote Console Client and Server, do either of the following:

- Select **Action > Chat**
- Click on the **Chat** button on the toolbar.

13 CMOS Setup Manager and BIOS Update Manager

This chapter describes how to install and use the CMOS Setup Manager and the BIOS Update Manager.

► CMOS Setup Manager

CMOS Setup Manager is an ASM Pro utility programs that is used to change the CMOS settings remotely. This means that you do not need to visit machines physically to change the CMOS settings for abnormal system configurations.

This feature does not to replace the common CMOS setup function provided by all BIOS vendors. It is for Windows environments, including Windows 95, Windows 98, Windows NT, and Windows 2000systems.

Menu commands

Command	Description
File menu	
Auto Discovery	Searches for available systems in the network and displays them for monitoring purposes
Get CMOS	Retrieves the CMOS data of the selected system and puts it into the cache
Save CMOS	Stores the CMOS data in the cache to the selected system
Load Previous Settings	Resets the CMOS data in the cache to that previously saved one
Load Previous Settings and Close	Resets the CMOS data in the cache to that previously saved and closes the update window
Save Settings and Close	Stores the CMOS data in the cache to the selected system and closes the update window
Import CMOS definition	Imports a CMOS script file
Exit	Exits CMOS Setup Manager
View menu	
Toolbar	Shows/hides the toolbar
Status Bar	Shows/hides the status bar
Window menu	
Cascade	Cascades the open update window
Tile	Tiles the open update window
Arrange Icons	Arranges icons in the client area

Command	Description
Help menu	
Content	Launches the Help Content window
About CMOS	About dialog box of CMOS Setup Manager

Installation and uninstallation

To install CMOS Setup Manager:

1. CMOS Setup Manager is an ASM Pro Console component that is automatically installed when you install the ASM Pro Console. Refer to “Installing ASM Pro Console” on page 13 for the installation instructions for ASM Pro Console under Windows NT 4.0 and Windows 95/98.
2. Restart the system.

To uninstall CMOS Setup Manager:

1. Click on the **Start** menu, select the **Programs** folder, then the **Acer ASM Pro Console** folder. Click on the **Uninstall Acer ASM Pro** option to uninstall the whole ASM Pro package.
2. Restart the system.



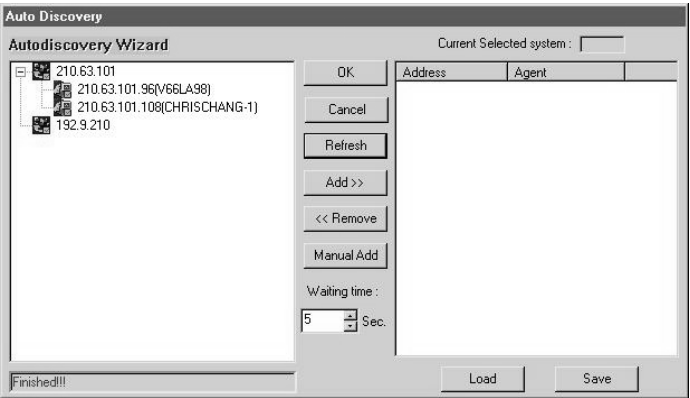
.....

Note: Only the ASM Pro Console includes the CMOS Setup Manager. This function is not available in the Agents.

Selecting browsing systems

From the File menu, select **Auto Discovery** to display the Auto Discovery dialog box.

Double click on the subnet address to search for an available ASM Pro agent.



This window displays all IP/IPX systems in your network detected by ASM Pro. The following items are available in this dialog box.

Auto Discovery dialog box items

Item	Description
Current Selected Systems	Shows all the systems to be monitored by ASM Pro
Waiting Time	Indicates the amount of time before the system terminates the operation if the system is not responding
Button	Description
OK	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now contains all the systems you specified in the left panel
Cancel	Exits the auto discovery window without saving
Refresh	Refreshes the System Listing (left panel display)

Item	Description
Add	Appends the highlighted IPX systems in the Systems Found list or the IP systems specified in the IP Address field to the Systems Selected list
Remove	Deletes the highlighted systems from the Systems Selected list
Manual Add	Allows you to manually add an IP address
Load	Loads the system list in the left panel of the auto discovery window
Save	Saves the current system list (left panel) to file for future use



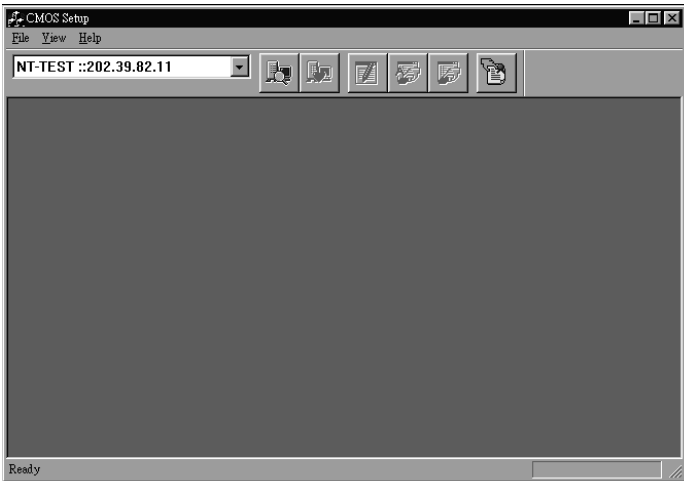
.....

Note: In order to make the Auto Discovery function work properly, the agent must be able to respond to standard MIB-II requests. Please refer to RFC1213 for more information about MIB-II.

Basic operations

To launch the CMOS Setup Manager:

1. Make sure the desired system is available in the system list. To do this, find the ASM Pro agent systems automatically via the **Auto Discovery** function, then select the desired system from the system list.
2. Click on the **CMOS Setup Manager** button on the ASM Pro Console Toolbar or select **Tools > CMOS Setup Manager**.
3. The CMOS Setup Manager main window appears on the screen.

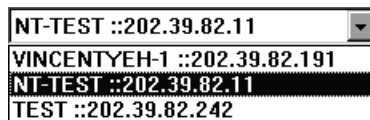


.....

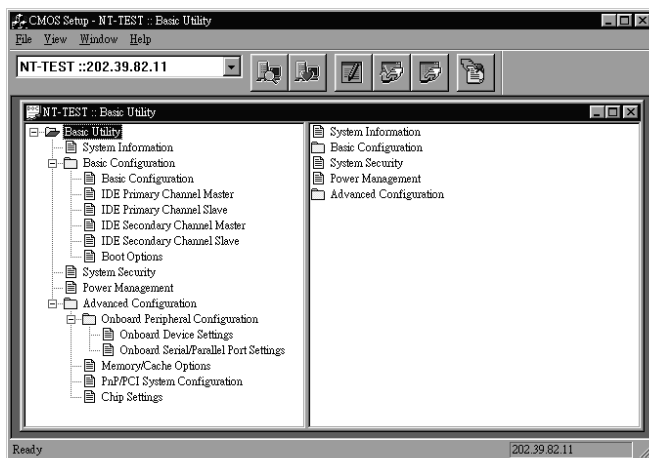
Note: You can use the auto discovery function to find the system whose CMOS data can be setup remotely.

To launch the CMOS Setup window:

1. In the CMOS Setup Manager main window, select the system you want to setup in CMOS from the Available System List box.



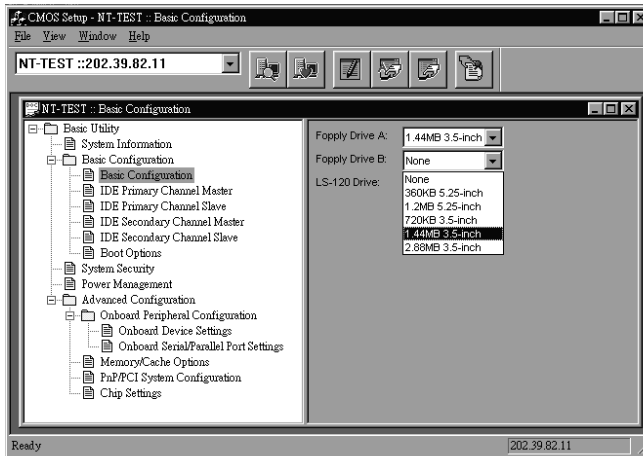
2. Select **File > Get CMOS** to launch the CMOS Setup window.



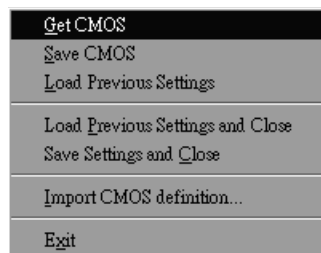
► Advanced operations

To change the CMOS settings:

1. Open the CMOS Setup Window.
2. Click the desired page in the left pane, e.g., Basic Configuration.



3. Notice that the right pane displays the settings defined on this page. Change the settings.
4. Select **File > Save CMOS** to save the new settings to CMOS.



To import a CMOS definition file for another model:

1. Select **File > Import CMOS definition...** to launch the Import CMOS definition dialog box.
2. Select the desired ICF file and click on the **OK** button to import the ICF file.

► BIOS Update Manager

BIOS Update Manager is an ASM Pro utility used to update the BIOS remotely. You do not need to visit the machine physically to upgrade the system BIOS. You can also schedule the time to perform the updating task in advance, then the BIOS Update Manager performs the task at the time scheduled.

Menu commands

Command	Description
File menu	
Exit	Exits BIOS Update Manager
Action menu	
Auto Discovery	Searches for available systems in the network and displays them for monitoring purposes
Start Up Service	Starts the BIOS update service. The Update manager checks if the job in the queue needs to be processed in a fixed interval
Stop Service	Stops the BIOS update service
Package	Defines the package to deliver to the client side; defaults are Remote Shutdown and Remote Wake-up
Job	Defines the job needed to be executed
System menu	
Setting	Configures the system settings
View menu	
Toolbar	Shows/hides the toolbar
Status Bar	Shows/hides the status bar

Command	Description
About menu	
About CMOS	About dialog box of CMOS Setup Manager

Installation and uninstallation

To install the BIOS Update Manager:

1. The BIOS Update Manager is an ASM Pro Console component. It is automatically installed once you install the Console of ASM Pro. Refer to “Installing ASM Pro Console” on page 13 for the installation instructions of ASM Pro Console under Windows NT 4.0 and Windows 95/98.
2. Restart the system.

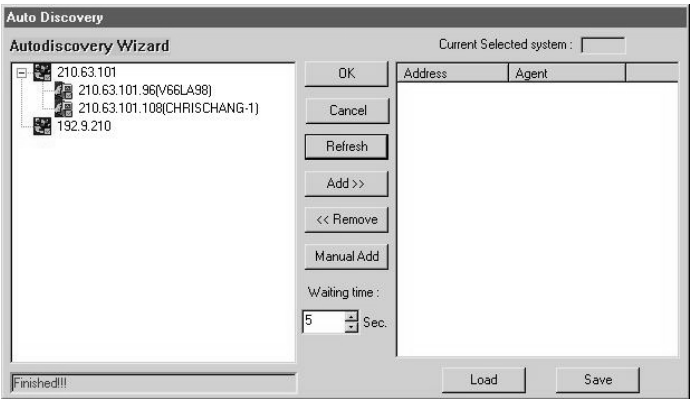
To uninstall the BIOS Update Manager:

1. Click on the **Start** menu, select the **Programs** folder, then the **Acer ASM Pro Console** folder. Click on **Uninstall Acer ASM Pro** to uninstall the whole ASM Pro package.
2. Restart the system.

Selecting browsing systems

From the File menu, select **Auto Discovery** to display the Auto Discovery dialog box.

Double click on the sub-net address to search for an available ASM Pro agent.



This window displays all IP/IPX systems in your network detected by ASM Pro. The following items are available in this dialog box.

Auto Discovery dialog box items

Item	Description
Current Selected Systems	Shows all the systems to be monitored by ASM Pro
Waiting Time	Indicates the amount of time before the system terminates the operation if the system is not responding
Button	Description
OK	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now contains all the systems you specified in the left panel
Cancel	Exits the auto discovery window without saving
Refresh	Refreshes the System Listing (left panel display)
Add	Appends the highlighted IPX systems in the Systems Found list or the IP systems specified in the IP Address field to the Systems Selected list

Item	Description
Remove	Deletes the highlighted systems from the Systems Selected list
Manual Add	Allows you to manually add an IP address
Load	Loads the system list in the left panel of the auto discovery window
Save	Saves the current system list (left panel) to file for future use

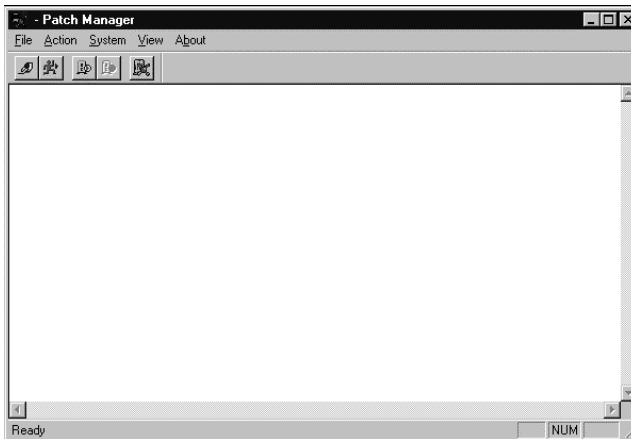


Note: In order to make the Auto Discovery function work properly, the agent must be able to respond to standard MIB-II requests. Please refer to RFC1213 for more information about MIB-II.

► Basic operations

To launch the BIOS Update Manager:

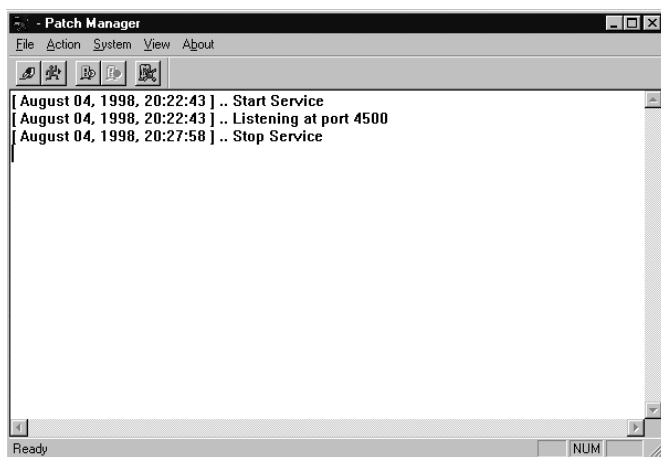
1. Make sure the desired system is available in the system list. To do this, find the ASM Pro agent systems automatically via the Auto Discovery function and then select the desired system from the system list.
2. Click on the **BIOS Update Manager** button on the toolbar or select **Tools > BIOS Update Manager** to launch BIOS Update Manager. The BIOS Update Manager main window appears.



Update operations

To start the BIOS Update service:

1. Select **Action > Start Up Service** or click on the **Start Service** button on the toolbar to start the update service. Make sure the service is on; otherwise, the scheduled jobs won't be executed.
2. The status window appears on the screen.

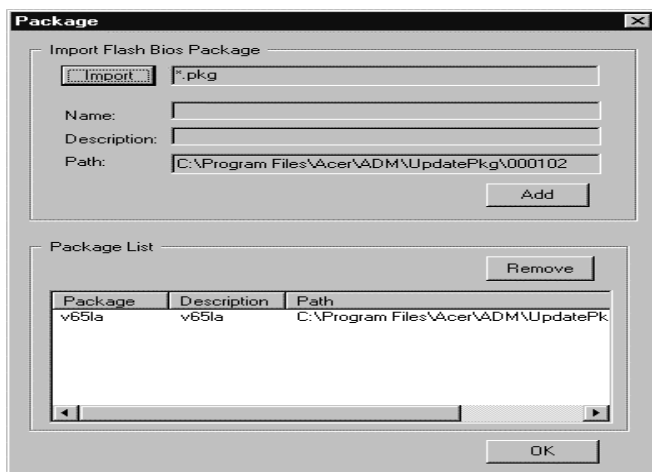


To stop the BIOS update service:

Select **Action > Stop Service** or click on the **Stop Service** button on the toolbar to stop the update service.

To prepare the package:

1. Select **Action > Package** or click on the **Package** button on the toolbar to launch the Package dialog box.



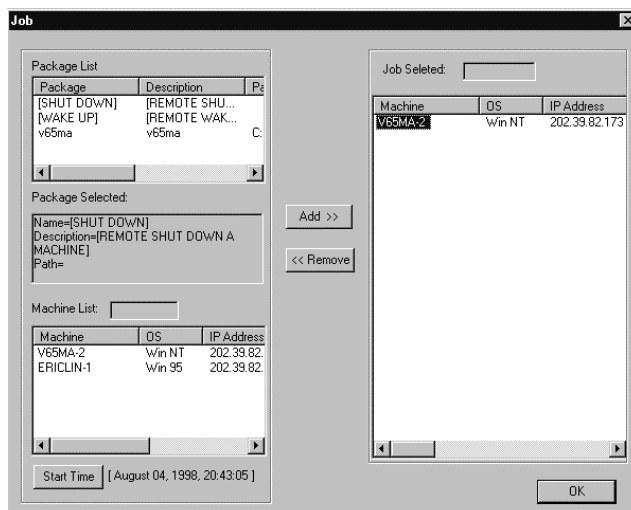
- Click on the **Import** button to launch the Open dialog box.



- Select the PKG file and click on the **Open** button to close the dialog box.
- Click on the **Add** button to add the selected package to the package list.
- Click on the **OK** button to close the Package dialog box.

To prepare the job:

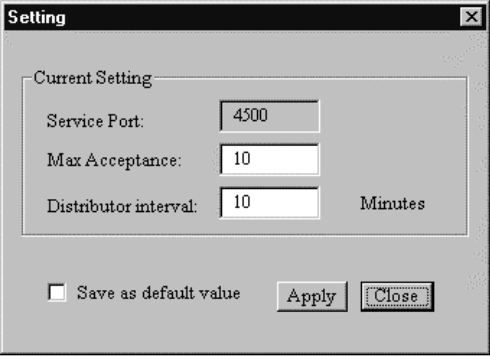
- Select **Action > Job** or click on the **Job** button on the toolbar to open the Job dialog box.
- Select the package item from the Package List and select the system where you want to apply the package.
- Click on the **Add >>** button to add the job to the Job list.
- Click on the **OK** button to close the Job dialog box.



Note: The newly added job is placed in the job queue waiting for the processing of the Update Manager. The interval defined in the Setting dialog box is used by the Update Manager to process the job by fixed interval, so the start time defined in the job is not the accurate time to process the job.

To change the settings:

1. Select **System > Setting**.
2. To change the maximum acceptable connection, type the desired value in the Max Acceptance box, then click on the **Apply** button.
3. To change the distributor interval, type the desired value in the Distributor interval box, then click on the **Apply** button.



A screenshot of a 'Setting' dialog box. The title bar is black with the word 'Setting' in white and a close button (X) on the right. The main area has a light gray background. A section titled 'Current Setting' is enclosed in a rounded rectangle. Inside this section, there are three labels with corresponding text input fields: 'Service Port:' with the value '4500', 'Max Acceptance:' with the value '10', and 'Distributor interval:' with the value '10'. The word 'Minutes' is positioned to the right of the 'Distributor interval' field. Below the 'Current Setting' section, there is a checkbox labeled 'Save as default value' which is currently unchecked. To the right of the checkbox are two buttons: 'Apply' and 'Close'.

Setting

Current Setting

Service Port: 4500

Max Acceptance: 10

Distributor interval: 10 Minutes

☐ Save as default value

Apply Close

14 Remote Diagnostic Manager (RDM)

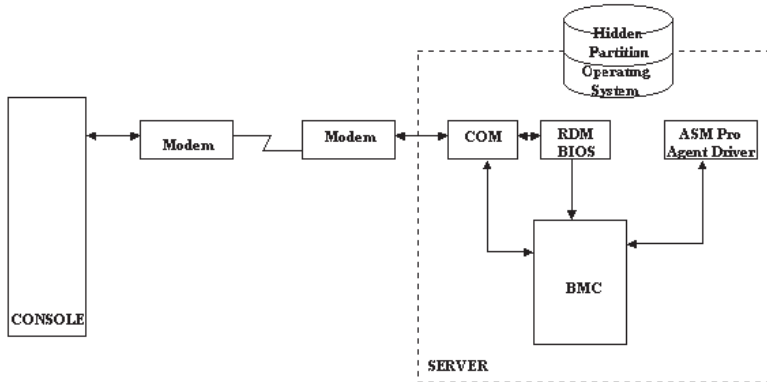
Remote Diagnostic Manager (RDM) is a server service program that offers remote server management functionality. It utilizes modems and telephone lines to remotely monitor and analyze the server condition via a remote RDM Console, allowing you to update system BIOS settings for quick restoration of the system to normal operation. It also uses a pager to notify the system administrator of server failures. This "quick response" feature of RDM minimizes the system down time due to system failures and therefore, offers the best solution to overcome the distance barrier of the remote server management.

► Overview

RDM architecture

The RDM architecture consists of three main components:

- ASM Pro Server Agent
- RDM Console
- RDM connectivity



During normal operation, the ASM Pro Server Agent periodically sends a heartbeat signal to the BMC. Once the server fails, the RDM driver stops sending heartbeat signals to the BMC. If the BMC does not receive any signal for a certain period of time, RDM learns that the server has crashed and then takes some emergency management.

When BMC takes emergency management, it takes control of the COM port. It notifies the system administrator (through paging) that the server failed. RDM operates according to the RDM Work Mode in BIOS Setup (refer to page 343).

ASM Pro Server Agent

Refer to Chapter 1 for ASM Pro Server Agent for different O.S. platform.

RDM Console

The RDM Console can be any standard PC system with RDM Console software installed and the necessary peripherals connected. For details on how to install the RDM Console software and the necessary peripherals, refer to page 340.

RDM connectivity

This refers to the RDM connection. To establish connection, it must have the ASM Pro Server Agent installed into the server. For the RDM Console to connect, it must have the RDM Console software installed.

Peripherals such as a modem and pager are necessary for RDM to function properly. The ASM Pro Server Agent and the RDM Console communicate via modem protocol.



.....

Note: Make sure that the modem and other peripherals are turned ON. Otherwise, the ASM Pro Server Agent will not be able to establish connection with the RDM Console.

RDM features

The following features explain how RDM offers efficient server diagnostic service to reduce the server down time.

Remote management features

- RDM offers remote server diagnostic service, eliminating the distance barrier for remote server management
- Informs the system administrator once the server hangs
- Allows automatic system reboot once failure is detected
- Supports Novell NetWare, Microsoft Windows NT, SCO OpenServer, SCO UnixWare and RedHat Linux.
- Monitors and displays server status information (such as health log, critical event, CPU information, temperature, voltage, fuse, CPU critical event, power supply, etc.) and configuration, even in the event of server failure

- Automatically powers off the system when there is a system failure or the processor temperature exceeds the maximum limit
- Allows the server to boot from any available processor through its smart recovery feature
- Can power on/off or reboot the server from the RDM Console

RDM Console features

- Monitors the system boot sequence
- Allows updating of the system BIOS or changing of the CMOS setup remotely
- Allows the system to boot normally or to the RDM hidden partition
- Allows remote access to the server's diagnostic utilities
- Supports file transfers
- BIOS supports ANSI terminal, allowing the RDM Console to display the RDM server screen after connection is established
- Features the Talk utility that allows users at both server and RDM Console sites to communicate easily

► RDM installation

This section gives step-by-step instructions on how to install the RDM module, the RDM function in agent side and console side of ASM Pro software.

System requirements

Before you begin the installation, make sure that you have the following:

RDM server requirements

Hardware

- External modem
- Pager

Software

- Novell NetWare v4.1 or later, and/or
- SCO OpenServer 5.0 or later, and/or
- Microsoft Windows NT 4.0 or later, and/or
- SCO UnixWare 7.0 or later
- RedHat Linux 6.2 or 7.1
- ASM Pro (Advanced System Manager Pro) agent

RDM Console requirements

Hardware

- Pentium or faster PC
- At least 16-MB RAM
- At least 5-MB free hard disk space
- Modem

Software

- Microsoft Windows 98, Microsoft NT Workstation 4.0, or Windows 2000
- ASM Pro 4.5 Console

Connecting communication peripherals

Modem

The Server and the RDM Console communicate via modem protocol. Therefore, you need to connect an external modem with a baud rate of not less than 9600 baud to both systems. To connect an external modem, connect the RS232C serial cable to the modem data port and the appropriate COM port of the system.



Note: Use only modems that are purchased locally to ensure compatibility with your telephone system. The modem must have a transfer rate of at least 28.8K.

When the modem is turned ON, the CD/DCD (Carrier Detect/Data Carrier Detect) signal light on the front panel must be OFF for RDM to function properly. If this is not the case, refer to the modem's user's guide and check the section on DIP switches for information on how to adjust the CD/DCD light. If your modem does not have a DIP switch, then we recommend that you replace it with another model that supports such switches.

Telephone

To connect the modem to a telephone outlet, plug in the telephone connector to the telephone outlet. Then, insert the telephone line connector to the modem line port.

Pager

The pager is necessary for notification purposes only.

Post-installation instructions.

- Make sure the modem cables are properly connected.
- Turn on the system and the peripherals connected to it.

Installing RDM Utilities

You must do the following to ensure successful installation of the RDM Utilities:

1. If you have created a RDM hidden partition through EasyBuild System CD, skip step 2.
2. Create a RDM hidden partition.

The RDM hidden partition is a DOS partition on the hard disk that allows you to run preinstalled diagnostic tools when necessary, without using a diskette or a CD. It also allows you to access your system from a remote RDM Console.

To create a RDM hidden partition, do the following:

- Prepare a "clean" hard disk, i.e., a hard disk without any operating system installed on it.
- Create a bootable RDM floppy diskette from the Management CD of EasyBuild.
- Insert RDM floppy diskette into the diskette drive.
- After booting from the floppy diskette drive, use the DOS FDISK command to create a DOS partition. The minimum partition size is 33 MB.
- Activate the partition and exit FDISK; then reboot the system.
- Format the DOS partition. When formatting is completed, label the partition as RDM for easy identification.
- Install (or transfer) the DOS operating system to the partition.
- Run \RDM\install.bat* from the RDM floppy diskette to install the RDM driver and hide the RDM partition. These settings will take effect only after you reboot the system.

After you create the hidden partition, you can now install other operating systems on the same hard disk. But before doing so, make sure that the Hidden Partition parameter in the RDM BIOS is set to Disabled. For more information on RDM BIOS, refer to RDM BIOS chapter of the ASM Pro manual.



.....

Important! If you are using an IDE hard disk with a capacity less than 540 MB, make sure that you disable the LBA mode. Otherwise, you will be required to use the LBA mode that you set for the other operating systems when you create the RDM hidden partition.



.....

Note: When you boot the system to the hidden partition, you cannot use other utilities (e.g., FDISK.EXE) to change the hidden partition settings.

Deleting the hidden partition



Important! You cannot recreate the RDM hidden partition once you delete it. Before proceeding, make sure that you will not need to create a hidden partition in the future.

Follow these steps to delete the hidden partition:

- Insert a bootable diskette into the diskette drive.
- Enter the BIOS Setup and set the Hidden Partition parameter in the RDM BIOS to Enabled.
- After the system boots from the diskette drive, use FDISK to delete the RDM hidden partition. Do not delete other partitions or change or reformat the active partition.
- Exit FDISK and reboot the system.
- Enter the BIOS Setup and set the Hidden Partition parameter in the RDM BIOS to Disabled.

3. Install an operating system.

RDM supports the following operating systems:

- Novell NetWare
- Microsoft Windows NT and Windows 2000
- SCO OpenServer
- SCO UnixWare
- RedHat Linux

You can install any or all of the operating systems. For the installation instructions, refer to the documentation that came with the OS package.

4. Install the ASM Pro Server Agent.



Note: Before you proceed, make sure that you have installed the necessary components and peripherals, for both the RDM server and RDM Console.

The ASM Pro Server Agent driver or the server driver is contained in the Advanced System Manager Pro (ASM Pro) software package. Therefore, to install the ASM Pro Server Agent driver, you need to install the ASM Pro agent software. For information on how to install

the ASM Pro software, refer to the documentation that comes with the ASM Pro package.

RDM Console setup

This section describes how to install and uninstall the RDM Console software.

Installing the RDM Console software



.....

Important! Before you proceed, make sure that you have installed the necessary components and peripherals, both for the RDM server and RDM Console.



.....

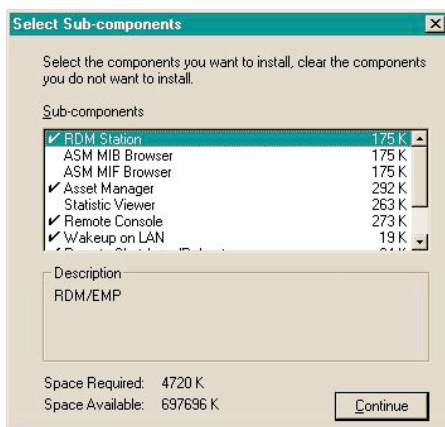
Note: The RDM Console software can be installed only under Windows NT 4.0/Workstation or Windows 95/98/2000.

The RDM function is one component of ASM Pro 4.5 Console software.

Follow these steps to install the RDM Console software:

1. Turn on the system.
2. Turn on the peripherals connected to the system such as the monitor, modem, etc.
3. Install ASM Pro Console. Run the installation program, i.e., SETUP.EXE. The Setup Program Welcome screen appears.

4. For typical installation in ASM Pro Console, the RDM Console will be installed. In Custom mode, user can choose to install RDM Console or not.



5. Continue to finish the installation of ASM Pro Console.

Uninstalling the RDM Console software

RDM Console software can only be uninstalled within ASM Pro Console package.

► Configuring the RDM functions in server

This section discusses the different RDM operation modes. It also explains the RDM BIOS features, as well as how to configure the RDM function via RDM BIOS.

RDM operation modes

The RDM enabled servers can run in three different RDM operation modes:

- RDM Local mode
- RDM Remote mode
- RDM Runtime mode

RDM local mode

In the RDM Local mode, the RDM hidden partition is activated; the server boots up to the activated RDM partition. This allows you to run diagnostics and other test programs locally on the server. However, in this mode, there is no remote connection. Thus, all RDM features are only locally available on the server console.

This mode is useful only if you are physically located next to the server.

RDM remote mode

In this mode, the RDM hidden partition is activated; the system boots up to the activated RDM partition; and a remote connection is automatically established to the pre-specified RDM Console. This makes all RDM features available to both the local server and the RDM Console. You can run any RDM utilities remotely from the RDM Console. However, this requires operator intervention since Remote mode can only be activated locally through the server's RDM BIOS Setup.

RDM runtime mode

The RDM Runtime mode is the normal RDM operation mode. In this mode, the system operates under its installed operating system. In the event of system failure, the driver stops sending heartbeat signal to the RDM

module. The RDM module then takes over the COM port and dials the pager number(s) pre-specified in the Remote Diagnostic Configuration menu.

There are two types of Runtime mode operations:

- Runtime Reboot Mode (Smart Reboot)
- Runtime Remote Mode (Waiting Mode)

The procedures to setup and to make use of the RDM operation modes are described in the sections that follow:

RDM BIOS

This section explains how to configure the RDM functions via RDM BIOS. The settings entered in the RDM BIOS determine how RDM handles a server failure.

Entering the RDM BIOS

To enter the RDM BIOS, press the **Ctrl+Alt+Esc** key to enter the BIOS Setup utility. Highlight the Remote Diagnostic Configuration option and press the **Enter** key. Page one of the Remote Diagnostics Configuration appears on screen. This page is for configuring the RDM Console functions.

Remote Diagnostic Configuration	
RDM 4.3 BIOS Version	000608
Console Redirection.....	[Disabled]
Hidden Partition	[Disabled]
Communication Protocol	[N,8,1]
COM Port Baud Rate	[57600]
Remote Console Phone No.....	[1699]
Dial Out Retry Times	[2]
Modem Initial Command	[]

↑↓ = Move highlight bar, ←→ = Change Setting, F1 = Help
PgUp/PgDn = Move screen

Press the **Page Down** key to view page two of the Remote Diagnostic Configuration menu. This page is for configuring the RDM module functions.

Remote Diagnostic Configuration	
RDM Work Mode	[Waiting]
Waiting Mode Password	[1234]
Paging	[Enabled]
System Critical Paging No.	
1.	[1234566789,,,,,#8823940]
2.	[
Paging Times	[1]
↑↓ = Move highlight bar, ←→ = Change Setting, F1 = Help PgUp/PgDn = Move screen	

After entering all the necessary settings, press the **ESC** key to exit the RDM BIOS setup.

RDM 4.5 BIOS version

This parameter specifies the version of the RDM BIOS.

Console redirection

This parameter lets you enable or disable the connection to the RDM Console. If enabled and conditions are met, the RDM enabled server automatically dials the RDM Console using the phone number specified in the Remote Console Phone No. parameter (see page 345) when the server reboots. Once the connection is established, both the RDM server and RDM Console display the same screen which enables the RDM Console to function the same as the server console. Setting this to Disabled deactivates the RDM Console.

Hidden partition

If you want the hidden partition to become accessible, set this parameter to Enabled. When enabled, the server boots to the hidden partition.

To disable the hidden partition and return to the normal booting procedure, set this parameter to Disabled.



Note: We recommend that you set this parameter to Enabled especially when you are troubleshooting system problems.

Communication protocol

This parameter specifies the parity, stop bits, and data length for the COM port to be used for the RDM connection. This is fixed at N (none), 8, 1 setting and is non-configurable. RDM requires no parity and one stop bit settings.

COM port baud rate

This parameter lets you set the transfer rate of the COM for the RDM connection. The parameter setting depends on your modem specification; therefore, before you change the setting of this parameter, check your modem user guide.



Important! Check your Onboard Peripherals settings in the BIOS Setup and make sure that you have assigned a port to serial 2. Otherwise, RDM will not function.

Remote Console phone number

This parameter allows you to set the phone number of the RDM Console that the RDM module must dial once RDM is activated and the Remote Console is enabled. To set, simply highlight the parameter and enter the Remote Console phone number.

Remote Console Phone No....[5455299]

If the remote console phone number is using a Private Branch eXchange¹ (PBX) line, then you must enter six commas (,) after the phone number and before the extension number, if any. When entering the extension number, we recommend that you insert a comma after each number. The commas specify delay.

Remote Console Phone No...[5455299,,,,,,6,6,4,9]

If this parameter is left blank, the Remote Console calling function is disregarded.

¹ PBX is a telephone switching system that requires manual operation to get an outside line. This is synonymous to PABX - Private Automatic Branch eXchanges.

Dial out retry times

This parameter lets you specify the maximum number of times the RDM server must retry to connect to the RDM Console once the server fails and RDM is activated. If the server has completed the specified number of tries and the connection still fails, the server bypasses RDM and goes into normal mode.

Modem initial command

Some modems require specific commands for initialization. This parameter allows you to specify the required command to enable your system to support special types of modems. If you do not specify any command, BIOS uses the default method to initialize the modem.



.....
Important! Specify an initialization command only when you receive a Modem Initial Command Fail error message. Otherwise, leave this parameter blank.

RDM work mode



.....
Note: Before you set this parameter, make sure that you have an RDM module. Otherwise, you cannot set this parameter.

This parameter lets you specify the RDM work mode or the notification procedure. If you enable this function and system crash, RDM module will do some emergency actions, like power off and paging. The mode options are listed in the following table:

Mode	Description
Waiting(Runtime Remote mode)	Once RDM is activated, the server dials the pager number(s) specified in the System Critical Paging No. parameters (see section page 348) and waits for the RDM Console to call in. When the RDM Console calls in with the specified phone number and password, the Agent Information automatically appears on the RDM Console screen.
Reboot (Runtime Reboot mode)	Once RDM is activated, the server dials the pager number(s) specified in the System Critical Paging No. parameters (see section page 348) and automatically reboots the system to its original operating system.
Disabled	Deactivates RDM.

Waiting mode password

This parameter prevents unauthorized access to the server. To set a password, simply highlight the parameter and enter your code. Your password may contain at least three characters but no more than eight alphanumeric characters (i.e., the 26 letters of the alphabet plus the numbers 0-9). You cannot use special characters.

Make sure to remember your password. Before the server grants RDM Console access, you will be prompted to enter this password.



Note: You must set a password; otherwise, the server will not establish connection with the RDM Console.

Paging

These parameters allow you to enable the paging feature once the server fails or hangs.

System critical paging numbers

These parameters allow you to set the pager numbers that the RDM module must dial once the server fails or hangs. To enter the pager number, simply highlight 1, 2 or 3. Type in the pager number followed by commas ',' which specify the delay. The number of commas to enter varies for every country depending on the communication switch used. Make sure that you enter the appropriate number of commas; otherwise, the pager may not receive the complete message. You can use any modem utility to determine the number of commas to enter. For example, to determine the number of commas via Windows Terminal:

1. Initialize the COM port assigned for the modem function.
2. Enter the system administrator's pager number (for example: 54555499,,,,,#XXXX#). The default is four commas (,,,,). If paging is successful, that means that the number of commas entered is enough. If not, add one comma to your entry. Repeat the procedure until paging is successful.

You may also include the server modem number or the message that you want to send in the pager notification. To do this, simply enter a # sign after the commas. Then enter your message. At the end of the message, type another # sign. The message entry must start and end with # sign.

To bypass this feature, do not enter any number after the comma.

System Critical Paging No.

1. [**123456789,,,,,,#8823940#**]
2. [**847982493,,,,,,#3442442#**]

Leave this parameter blank to disregard this function.



.....

Note: You can enter a maximum of two sets of pager numbers. Each line accommodates a maximum of 45 characters. Follow the same procedure to set the additional pager numbers.

Paging times

Similar to the Dial Out Retry Times parameter, this parameter lets you specify the number of times the server must dial the pager number(s) specified in the System Critical Paging No. parameters (see page 348) once the server fails and RDM is activated.

Setting RDM operation modes

The RDM server can be set to run in one of three different RDM operation modes: local mode, remote mode, and runtime mode. These sections will describe how to configure the RDM server and RDM Console to run in different RDM operation modes.

RDM local mode

In RDM Local mode, the RDM server boots to the RDM hidden partition, which allows you to run diagnostics and other test programs on the server locally.

Enabling local mode

Follow these steps to enable the Local mode:

- Reboot the server and enter the BIOS Setup.
- From the main menu, select Remote Diagnostic Configuration.
- Set the Hidden Partition parameter to Enabled.
- Save your changes and exit the BIOS Setup. The server automatically reboots.

Exiting from local mode

After running the diagnostics, you may now resume the system to normal operation. To do this, you need to exit from RDM Local mode.

To exit from RDM Local mode, do the following:

- Reboot the server and enter the BIOS Setup.
- From the main menu, select the Remote Diagnostic Configuration option.
- Set the Hidden Partition parameter to Disabled.
- Save your changes and exit the BIOS Setup.

RDM remote mode

In RDM remote mode, the system boots to the RDM hidden partition and automatically establishes a remote connection, which makes all the RDM features available to both the RDM server and RDM Console sites. However, the RDM Remote mode can only be activated by a local operator in the server BIOS Setup.

Enabling remote mode

Follow these steps to enable the RDM Remote mode:

- Reboot the server and enter the BIOS Setup.
- From the main menu, select the Remote Diagnostic Configuration option.
- Set the Console Redirection parameter to Enabled.
- Set the Dial Out Retry Times parameter to the desired number of times the server must attempt to call the RDM Console to make a connection.
- In the Remote Console Phone No. parameter, enter the RDM Console phone number.
- Save your changes and exit the BIOS Setup. The server automatically reboots and dials the specified RDM Console phone number to establish remote connection.

Remotely Accessing the RDM Server

Once the RDM server is rebooted into the RDM Remote mode, the RDM server will try to establish a connection with the RDM Console.

If the remote RDM connection is successfully established, you can access all RDM utilities from the RDM Console.

From the RDM Console, you can do either of the following:

- Press the **Shift+1** key to view the server BIOS Setup. For details on BIOS Setup, refer to the system's documentation.
- Boot to the hidden partition.



.....

Note: RDM Console supports VGA text mode only.

Exiting from remote mode

If you want to resume the server system to normal operation mode, the server needs to exit from the RDM Remote mode.

To exit from RDM Remote mode, do the following:

- Run the RDM Console program (See xx).
- From the menu bar, select Agent.
- Select the Reboot Agent command. The Confirm RDM Server Reboot dialog box appears.

- Click on Disconnect. The server system automatically reboots, terminates connection and returns back to normal operating mode.



Note: If you click on the Keep Monitoring option, the server reboots without disabling the connection with the remote RDM Console.

RDM runtime mode

The RDM Runtime mode is the normal RDM operation mode in which the server system operates under its installed operating system. In the event of server system failure, the RDM driver stops sending heartbeat signals to the RDM module which, then, takes over the control of the server system and the COM port, and dials the pager number(s) to notify the specified system administrator.

Activating RDM



Note: Make sure that the modems are turned ON during remote RDM operation.

When the server system fails or hangs, the RDM driver stops sending heartbeat signal to the RDM module. When the RDM module does not receive any heartbeat signal for a certain period of time, RDM will be activated. However, if the temperature of any processors in the system exceed their limit, the RDM module will immediately turn off the system for safety purpose.

When RDM is activated, the RDM module takes control of the COM 2 port connected to the modem. It notifies the system administrator (through paging) of the server failure. RDM operates according to the RDM Work Mode specified in BIOS Setup and allows the system administrator to access the server remotely from the RDM Console.

There are two types of Runtime mode operations:

- Runtime Reboot Mode (Reboot Mode), and
- Runtime Remote Mode (Waiting Mode)

The sections below discuss how each mode operates.

Runtime reboot mode (Smart Reboot)

In this mode, RDM module checks the status of all processors installed in the server. If there is at least one processor in good condition, the server automatically reboots. However, if the temperatures of all processors in

the system are higher than the maximum limit, the RDM module will not reboot the system until the temperature of at least one of the processors returns to normal.



.....

Note: To minimize the system down time, we recommend that you set the RDM Work Mode parameter in the BIOS Setup to Reboot. This setting enables the server to start paging and reboot immediately in the event of system failure.

Enabling runtime reboot mode

Follow these steps to enable the Runtime Reboot mode:

- Enter the BIOS Setup.
- Highlight the Remote Diagnostic Configuration option.
- Go to page 2 of the RDM Configuration menu.
- Set the RDM Work Mode parameter to Reboot.



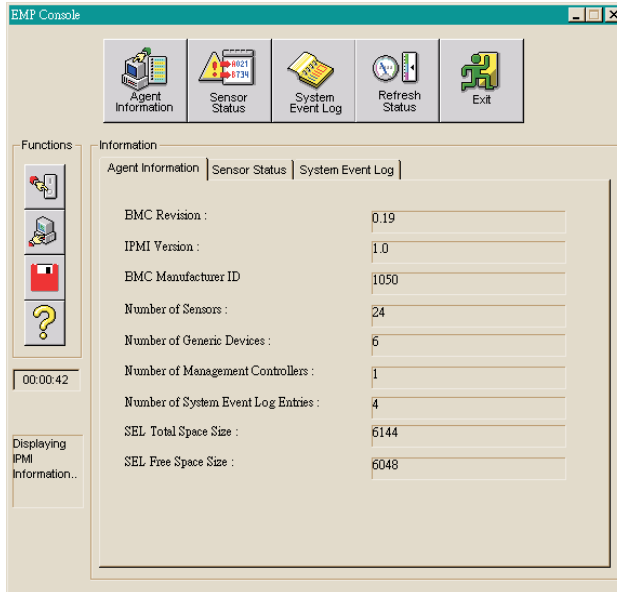
.....

Note: After Smart reboot, the processors with very high temperatures will be disabled. To enable the processors, you need to turn off the system.

- Specify the system administrator's pager number in the System Critical Paging Number parameter. You may enter a maximum of three pager numbers.
- Specify the desired setting for the Paging Times parameter.
- Save your changes and exit the BIOS Setup. The server automatically reboots and runs in Runtime Reboot mode.

Runtime remote mode

In this mode, when the server hangs or fails, the RDM module starts paging. Once the administrator receives the paging, he can establish a connection from the RDM Console to the RDM Server. Once the connection is established, the Emergency Management Console appears on the screen.



Through the RDM Console, the system administrator can access the following from the remote RDM-enabled server:

- Agent Information
- System Event Log
- Sensor Status

For detailed descriptions of these items, see page 355, using the RDM Console.

Enabling runtime remote mode

Follow these steps to enable the Runtime Remote mode:

- Enter the BIOS Setup.
- Highlight the Remote Diagnostic Configuration option.
- Go to the RDM Configuration menu.

- Set the RDM Work Mode parameter to Waiting.
- Enter a password in the Waiting Mode Password parameter. You will use this password to access the RDM server from an RDM Console.
- Specify the system administrator's pager number in the System Critical Paging Number parameter. You may enter a maximum of three pager numbers.
- Specify the desired setting for the Paging Times parameter.
- Save your changes and exit the BIOS Setup. The server automatically reboots and runs in Runtime Remote mode on the event of server system failure.

► Using the RDM Console

This chapter describes how to use the RDM Console.

Running the RDM Console



.....

Note: To optimize the screen resolution, select 800x600.

Starting the RDM Console

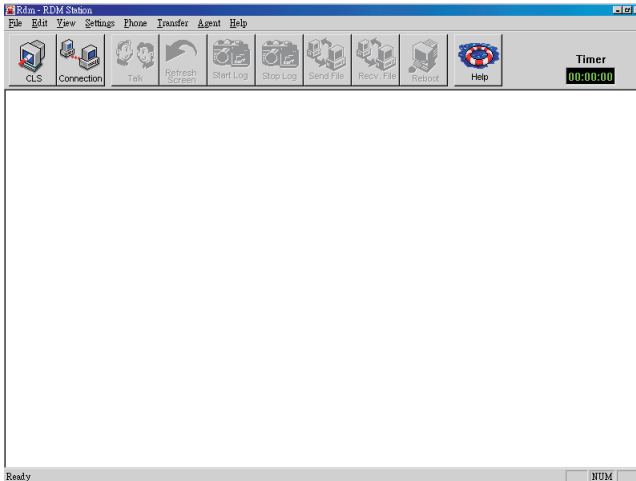
In order to run the RDM Console, connect to the RDM server by doing the following:

- RDM Console automatically starts when you run the ASM Pro console system. To start RDM Console manually, click on the RDM Console icon located on the toolbar of ASM Pro console or select **Utility > RDM Console** from the menu bar.
- Click on OK to continue. This process is followed by the initialization of the modem. The message Initialize modem successfully appears if the modem initialization is successful.
- Click on OK. The screen displays the RDM Console window.

Connecting to the RDM server

To access the remote server from the RDM Console, do the following:

1. From a remote location, launch the RDM Console program. The RDM Console Utility window appears on the screen.



For more details on the RDM Console Utility, see section page 362.

2. Do either of the following:
 - Click on the Connection button from the Toolbar, or
 - Click on the Phone menu and select the Agent Phone Book command
3. If the desired ASM Pro Server Agent icon already exists, double-click it. The station automatically dials to the ASM Pro Server Agent. Otherwise, create a new ASM Pro Server Agent. See section page 370 for details on creating a new ASM Pro Server Agent.
4. When the call is successful, the RDM module verifies the entered password. If the password matches the ASM Pro Server Agent password for remote connection, the station automatically displays the Agent Information window on the screen.

EMP (emergency management port) console

Once the RDM connection is established, the EMP Console window is displayed on the RDM Console screen. You may get ASM Pro Server Agent information by clicking various EMP Console buttons, or perform RDM functions by clicking on the function buttons.

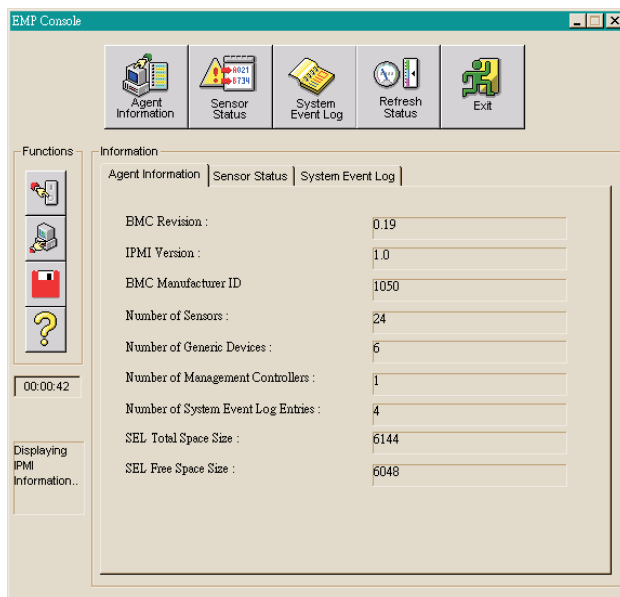
EMP console buttons

From the EMP Console window, you can do the following by clicking the respective ASM Pro Server Agent Information button:

Agent information



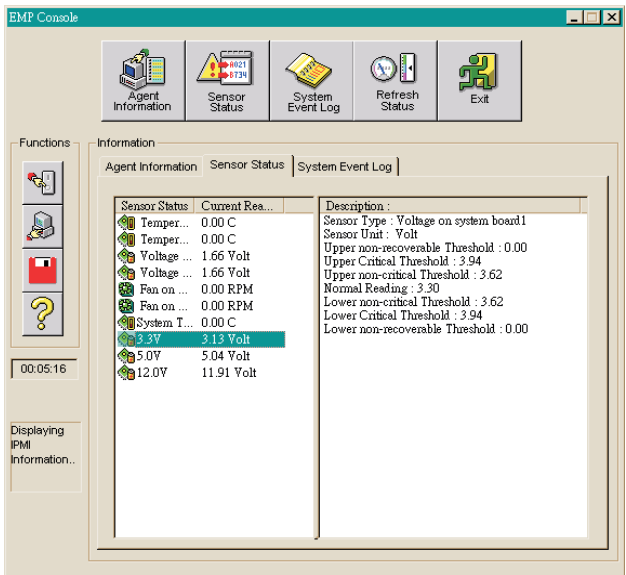
Displays important agent information.



Sensor status



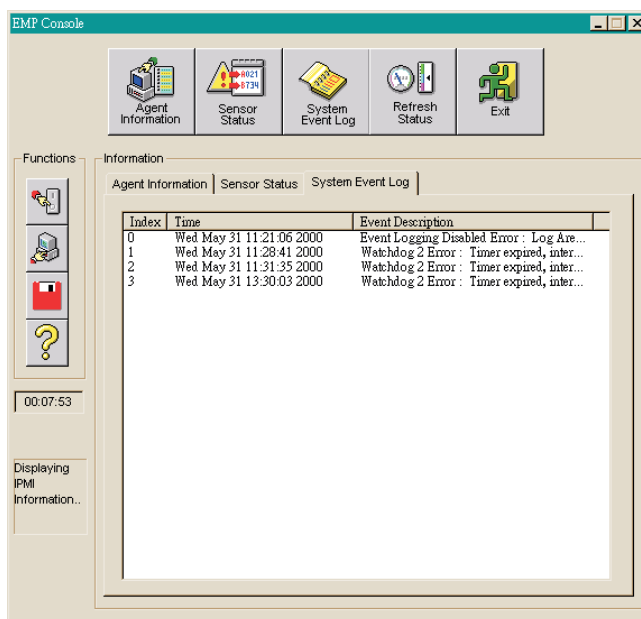
Displays readings of sensors.



System event log



Displays the system event log.



Refresh status



Refresh the information of current hardware component (Sensors status, System event logs, etc.) status of the server

Exit



If you click this button, a message box appears to ask: If you want to Power Off or Reboot the remote server, Please click Cancel, then select Power Off or Reboot function accordingly. If you select Cancel, the it goes back to the EMP console. If you select OK, another message box appears to confirm your choice, then the RDM Console automatically cuts off the existing connection with the server and allows the server to remain available for other RDM connections.

EMP console functions

From the EMP Console window, you can invoke the following ASM Pro Server Agent Information functions:

Power On/Off

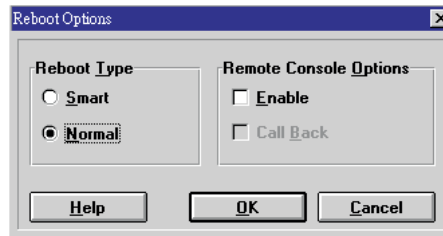


Turns off the server. If you click this button, the message System turned off appears. Simply click on OK.

Reboot



Displays the Reboot Options dialog box and reboots the server according to the specified reboot options.



Save



Saves System Event log as a file with .TXT extension.

Help



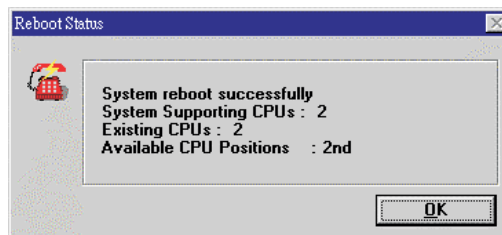
Displays the Help information.

RDM reboot options

From the RDM reboot options dialog box, the following reboot options are available:

Smart reboot

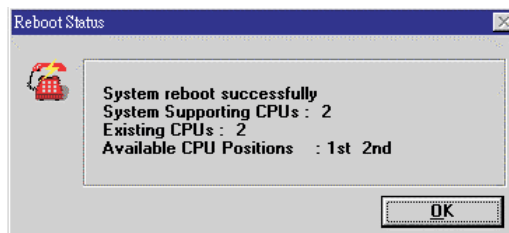
When the Smart Reboot option is selected, RDM checks the status of all processors installed in the server. If there is at least one processor that is in good condition, the system automatically reboots to that processor. After reboot, the following message box appears:



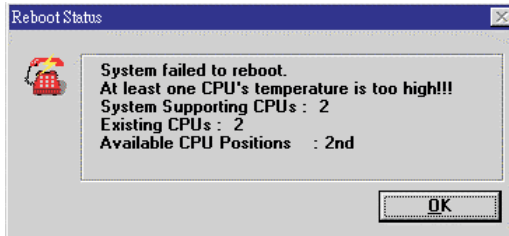
If all processors are in bad condition, a message informing you of the condition of the processor(s) appears, asking if you still want to force to reboot the system. Click Yes to "force" the reboot of the server. The system will use all the processors installed in it to reboot.

Normal reboot

When selected, RDM checks the status of all the processors installed in the server. If all processors are in good condition, the system automatically reboots and shows the following message:



If any of the processors are in bad condition, a message informing you of the condition of the processor(s) appears.



Click on OK, and then another message box appears to confirm if you want to force a reboot. Click on Yes to "force" the reboot of the server. The system will use all the processors installed to reboot.

RDM Console options

From the RDM reboot options dialog box, the following RDM Console options are available:

Enable

Maintains remote connection after server reboots and allows the RDM Console to fully control the server.

CallBack

When selected, remote connection cuts off before the server reboots. After reboot, the server dials back to the RDM Console to resume connection. This option is recommended if you want to pass the connection charges to the server.

After verifying your settings, click on OK. The server reboots according to your specified settings.

RDM Console utility

This section describes the functions available through the RDM Console utility.

RDM Console utility menus

The File Menu

The File menu contains the following commands:

View Snapshot File... - Displays a saved Snapshot file. It is only for RDM 4.0x Agent.

Close - Closes the RDM Console window.

Shutdown RDM Console - Exits the RDM Console utility.

The Edit Menu

The Edit menu contains the following commands:

Clear Window - Clears the utility screen.

Save Log File - Saves the current screen as .LOG file. This is very useful especially if you are debugging or troubleshooting. By default, this option is grayed out, i.e., disabled.

Stop Saving Log - Disables the Saving Log File function. By default, this option is grayed out, i.e., disabled.

The View Menu

The View menu contains the following options:

Toolbar - Shows or hides the utility Toolbar.

Status bar - Shows or hides the status bar, i.e., the bar located at the bottom of the utility window.

The Settings Menu

The Settings menu contains the following options:

Communication - Lets you configure the RDM Console function.

Font - Allows you to change your font properties.

The Phone Menu

The Phone menu contains the following commands:

Hang Up - Disables the telephone connection. By default, this option is grayed out, i.e., disabled. Once remote connection is established, this option becomes enabled.

Agent Phone Book - Allows you to add a new agent. To dial to the desired agent, simply double-click on its icon.

The Transfer Menu

The Transfer menu enables the RDM Console and the RDM server to send and receive files.

Send File - Enables the RDM Console to send files to the server.

Receive File - Enables the RDM Console to receive files from the server.



.....

Note: By default, these options are grayed out, i.e., disabled. Once remote connection is established and server boots to hidden partition, the options become available.

The Agent Menu

The Agent menu contains the following commands:

Refresh Screen - Updates the current screen.

RDM Console Talk - Runs the Talk utility. This utility allows the users located at RDM Console and ASM Pro Server Agent to communicate online.

Reboot Agent - Allows you to reboot the server from the RDM Console.



.....

Note: By default, all options are grayed out, i.e., disabled. Once a remote connection is established and the server boots to the hidden partition, these options become available.

The Help Menu

The Help menu contains the following commands:










Index - Displays the Help index. The index helps you to find the information that you want easily.



Using Help - Opens the RDM online help.

About RDM Console - Displays the copyright, version number and release date of the RDM Console utility.

RDM Console toolbar buttons

CLS Clears the screen.

		
CLS		Clears the screen.
Connection		Automatically dials the server phone number once the system fails. The button becomes gray or disabled after remote connection is established.
Talk		Opens the Talk utility. This utility allows the users located at the RDM Console and ASM Pro Server Agent to communicate online.
Refresh Screen		Updates the current screen.
Start Log		Saves the current screen as a .LOG file. This is very useful if you are debugging or troubleshooting. By default, this button is grayed out, i.e., disabled. Once remote connection is established, it becomes available.
Stop Log		Stops the logging function. By default, this button is disabled. Once the Start Log function is enabled, this button becomes available.
Send File		Enables the RDM Console to send files to the server.
Receive File		Enables the RDM Console to receive files from the server.

Reboot		Allows you to reboot the server from the RDM Console.
Help		Opens the RDM online help.

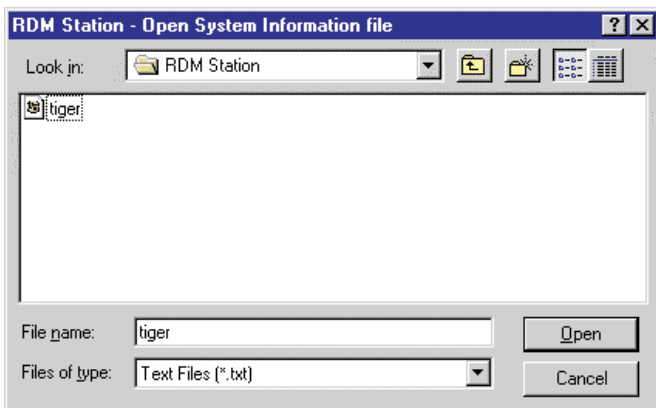
RDM Console functions

This subsection describes the various RDM Console functions you can perform through the RDM Console utility.

Viewing a snapshot file

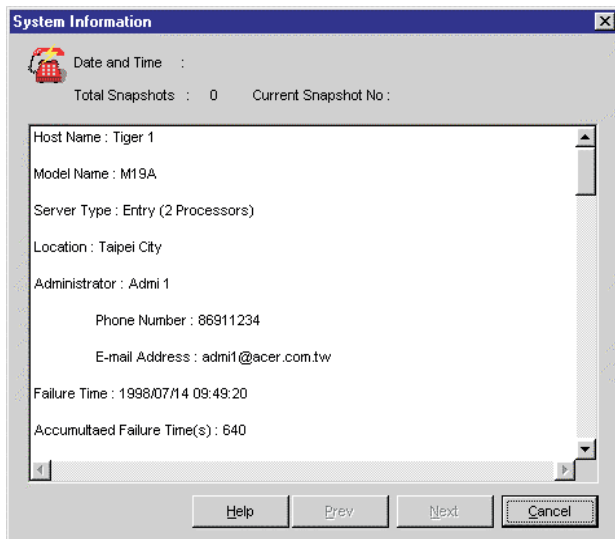
This feature is only for RDM 4.0x Agent. To view a previously saved Snapshot file, do the following steps:

1. From the menu bar, select the File menu.
2. Select the View Snapshot File command. The Open System Information File dialog box appears.



3. From the Folders box, select the path where the desired Snapshot file is located.
4. From the File Name list box, select the desired Snapshot file.

5. After making your selection, click on Open. The screen displays the selected Snapshot file.



Clearing the screen

To clear the screen, you can do either of the following:

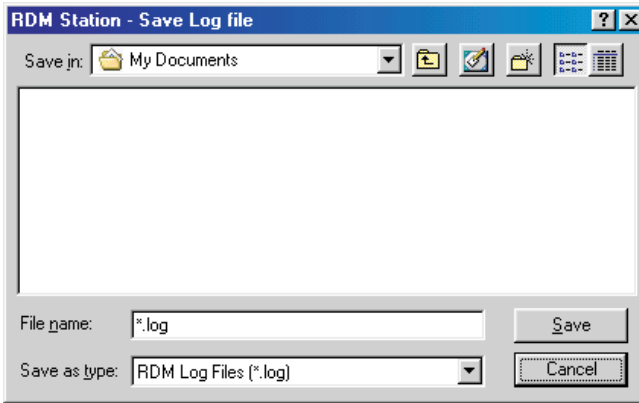
- Click on the Clear button from the Toolbar.
- From the menu bar, click on the Edit menu and select the Clear Window command.

Saving a log file

If you want to save the current screen as a .LOG file, do the following:

1. Do either of the following:
 - Click on the Log button from the Toolbar.
 - Click on the Edit menu and select the Save Log File command.

The Save Log File dialog box appears.



2. Enter a filename in the File Name box. Then specify the path where you want to save the .LOG file in the Save in box.
3. Click on Save to save the configuration to the specified filename or click on Cancel to disregard the entries and quit the Save Log File dialog box.



Note: Only the current screen on display when you clicked the Save Log File button will be saved. To save the following screens, you must click the Save Log File button after each screen. All saved screens will be appended to the specified Log filename.

Disabling the saving log file function

To disable the Saving Log File function, do either of the following steps:

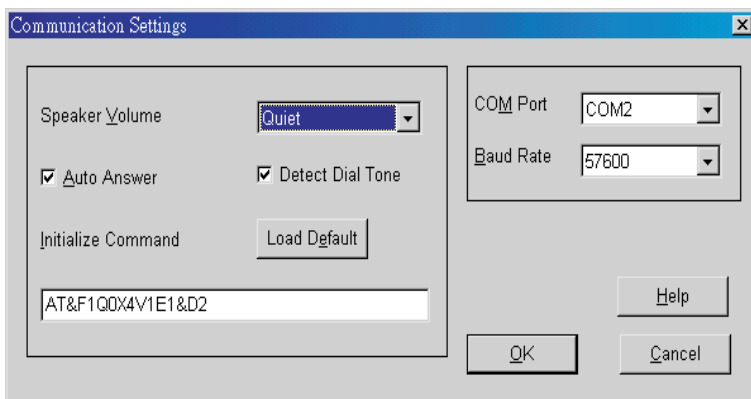
- Click on the Stop Log button from the Toolbar.
- From the menu bar, click on the Edit menu and select the Stop Saving log command.

Configuring RDM Console settings

To configure RDM, follow these steps:

1. Select Settings from the menu bar.

2. Select the Communication command. The Communication Settings dialog box appears.



3. If the modem currently in use requires a special command for initialization, specify the command in the Initialize Command box. We recommend that you use the default modem initialization command. To do this, simply click on the Load Default button.



.....

Note: If the modem initialization fails, check your modem's manual for the proper initialization command and enter it in the Initialize Command box.

4. Click on the down arrow of the COM Port box and select the COM port that you want to assign for the modem function.
5. Click on the down arrow of the Baud Rate box and select the baud rate that you want to support. The default setting is 57600.



.....

Note: We suggest that you leave the other parameters to their default settings.

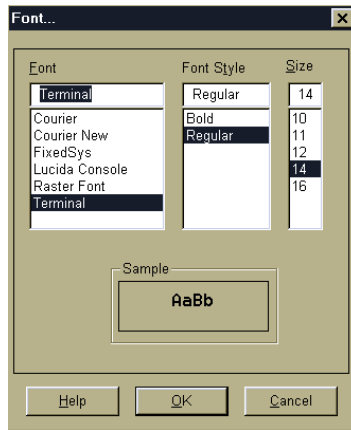
Setting the font properties

You can select the font that you want to appear on the RDM Console window for displaying text.

To select a font, do the following:

1. From the menu bar, select the Settings menu.

2. Select the Font command. The Font dialog box appears.

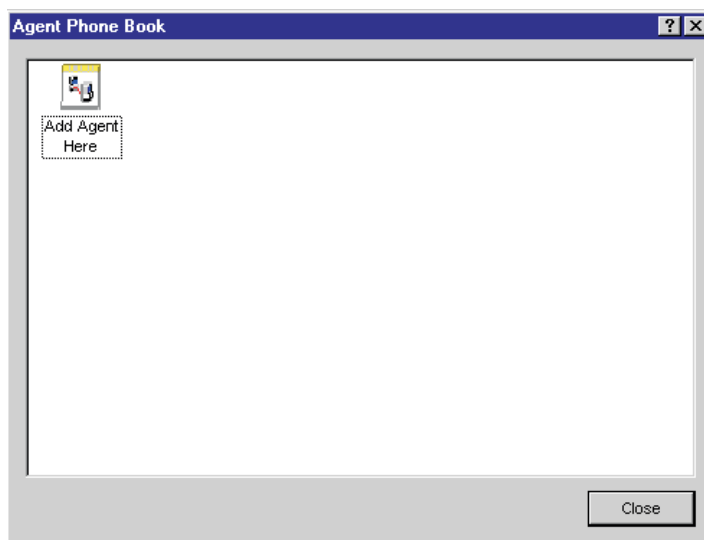


3. From the Font box, select the desired font type.
4. From the Font Style box, select the desired font style.
5. From the Size box, select the desired font size.
6. After making your selections, the desired character type appears in the Sample box. Verify your settings and click on OK.

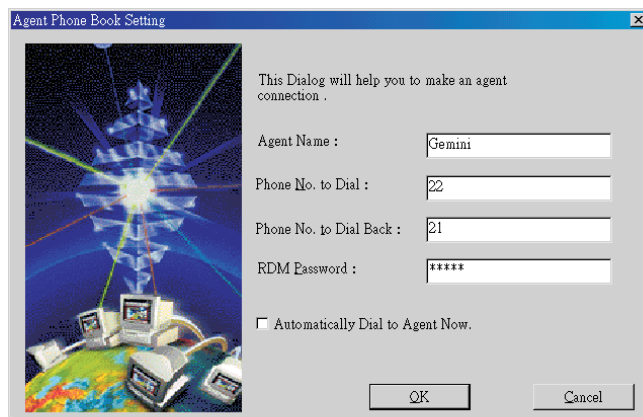
Creating a new ASM Pro Server Agent

To create a new ASM Pro Server Agent, do the following:

1. From the menu bar, click on the Phone menu and select the Agent Phone Book option. The Agent Phone Book window appears.



2. Click on the Add Agent Here icon. The Agent Phone Book Setting window appears on the screen.



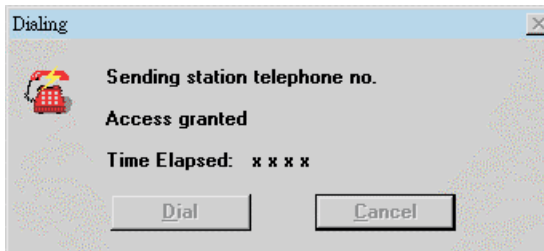
3. Enter the ASM Pro Server Agent in the Agent Name textbox, ASM Pro Server Agent phone number in the Phone No. to Dial textbox, RDM

Console's phone number in the Phone No. to Dial Back textbox, and the correct password in the RDM Password textbox.



Note: The RDM password entries must match with that specified in BIOS.

4. If you wish to connect to the agent immediately, simply click on the Automatically Dial to Agent Now checkbox, then click on Finish. The RDM Console automatically dials the server number. When the call is successful, the RDM module verifies the entered password and the following message box appears:



5. If the password matches the server's password for remote connection, the Agent Information window appears. This window displays general information about the server.
6. After verifying your settings, click on Exit. The server boots according to your specified settings.

Sending files



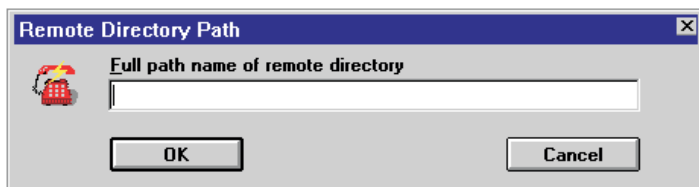
Note: Before you send files, make sure that the agent is in DOS command mode and that the files to be transferred are stored on the local hard disk.

To send files to the server, follow these steps:

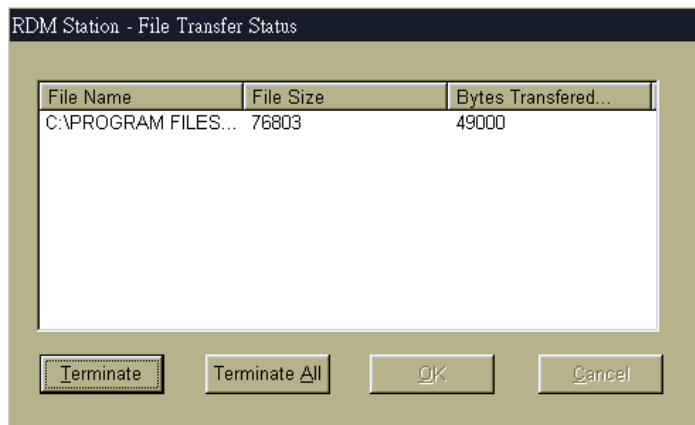
1. Do either of the following:
 - From the menu bar, click on the Transfer menu and select the Send File command.
 - Click on the Send button from the Toolbar.

The Open File dialog box appears.

2. Choose the file(s) that you want to send and then click on OK. You may choose as many files as you want. Then the Remote Directory Path dialog box appears.



3. Enter the directory in the server where you want to copy the selected files in the Full path name of remote directory entry box.
4. After verifying the entered path, click on OK. The File Transfer Status dialog box appears.



5. To stop the sending operation of the file that the RDM Console is currently transferring, click on the Terminate button. To stop the sending of all the selected files, click on the Terminate All button.

If the file(s) already exist, a message box prompting you to confirm the replacement of the files will appear. Click on Yes to confirm the replacement of the file that is currently being transferred. Click on Yes to All to confirm the replacement of all the common files. Click on No if you do not want to replace the file.

Notice that the OK button remains grayed until the file transfer is completed. The Cancel button becomes grayed if the file transfer fails.

To close the Transfer Status dialog box, click on OK. To disregard the operation that has been performed previously, click on Cancel.

The maximum file size that can be transferred is 18 MB.

Receiving files

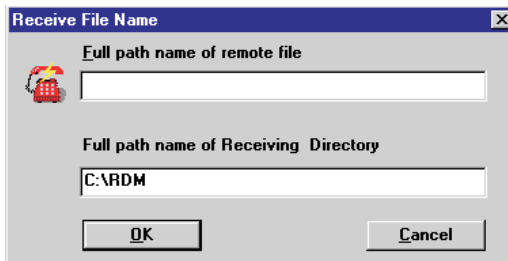


Note: Before you receive files, make sure that the agent is in DOS command mode.

To receive files from the server, follow these steps:

1. Do either of the following:
 - From the menu bar, click on the Transfer menu and select the Receive File command.
 - Click on the Receive button from the Toolbar.

The Receive File Name dialog box appears.



2. Enter the path where the files are located in the Full path name of remote file entry box and then click on OK. The File Receive Status dialog box appears.
3. Notice that the OK button remains grayed until the transfer of file(s) is completed. To stop the transfer of file(s) or to disregard the operation that has been performed previously, click on Cancel.

If the file(s) already exist, a message box prompting you to confirm the replacement of the files will appear. Click on Yes to confirm the replacement of the file that is currently being transferred. Click on Yes to All to confirm the replacement of all the common files. Click on No if you do not want to replace the file.

4. When the file transfer is finished, click on the OK button to close the Receive Status dialog box.



Note: The maximum file size that can be transferred is 18 MB.

Refreshing the screen

To "refresh" the screen, you can either click on the Agent menu from the menu bar and select the Refresh Screen command, or click on the Refresh Screen button from the Toolbar. This automatically updates the RDM Console screen.

Running the talk utility

The Talk utility allows the user at the RDM Console to directly communicate with the user at the server site via PC. Users at both sites can send messages by simply typing in the text.

To run the Talk utility, follow these steps:

1. Do either of the following:
 - From the menu bar, click on the Agent menu and select the RDM Talk command.
 - Click on the Talk button from the Toolbar.

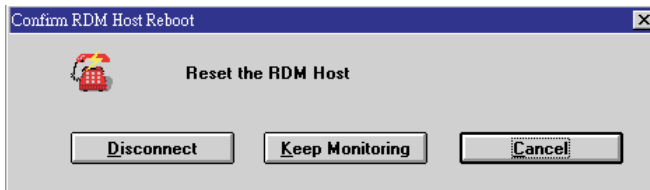
The Talk Utility screen appears both on the server site and on the local site monitors.
2. Type in the messages that you want to send. The messages from the server site appear in the upper portion of the screen, while the messages from the RDM Console appears in the lower portion
3. To exit this utility, the user at the RDM Console must press `Ctrl + X` keys.

Rebooting the server

To reboot the server, follow these steps:

1. Do either of the following:
 - From the menu bar, click on the Agent menu and select the Reboot Agent command.
 - Click on the Reboot button from the Toolbar.

The Confirm RDM Server Reboot dialog box appears.



2. Click on the Disconnect button to disable RDM and reboot the server to normal mode. Click on the Keep Monitoring button to simply reboot the server. If you suddenly decide not to reboot the server, click on Cancel.
3. After making your choice, the dialog box disappears from the screen and the selected reboot option is performed.

► SCO OpenServer, UnixWare and Internet FastStart Installation

This appendix describes how to do a fresh installation of the SCO OpenServer, UnixWare and Internet FastStart while preserving the RDM hidden partition.

SCO OpenServer 5

The default option for Hard Disk Setup is Unix only: Bad blocking 0 FF. Do NOT accept this default option. This will overwrite the RDM partition.

Follow these steps to install SCO OpenServer 5:

1. Boot the system with the SCO OpenServer boot diskette and the SCO OpenServer CD-ROM loaded in their respective drives.
2. Follow all onscreen instructions until you reach the Hard Disk Setup entry.
3. Choose Interactive fdisk/divvy.
4. Choose either Use the Rest of the Disk for Unix for allocating the remaining space to Unix, or Display Partition Table to customize it.
5. Continue to follow all onscreen instructions to complete the installation.



.....

Note: If you are using the SCO OSR 5 Easy Install on the Startup CD, it will automatically detect and preserve the existing RDM partition in the system. If you are doing the manual installation, you must perform steps 2 through 4 to ensure that you do not overwrite the RDM hidden partition.

SCO UnixWare

Follow these steps to install SCO UnixWare:

1. Boot the system with the SCO UnixWare installation diskette and the SCO UnixWare CD-ROM loaded in their respective drives.
2. Follow all onscreen instructions until you reach either of the following:
 - Destructive Installation step - if you have not yet installed UnixWare in your system. From the Destructive Installation options listed, select Display a Screen to View/Change Current

Disk Configuration. The installation program proceeds to the Disk Partition step (see Step 3).



.....

Caution: Do not select Use the ENTIRE DISK for UnixWare 2.1 (Erases ALL Partitions). This option will overwrite all existing partitions on the disk (including the RDM hidden partition).

- Nondestructive Installation step - if you have previously installed UnixWare. In this step, the installation program will not require you to create a partition for UnixWare; instead, it will keep your previous partitions and overwrite the previously installed Unixware in your system. Skip Step 3 and proceed to Step 4.
3. Create an active Unix partition by editing the disk partition table shown on the screen.



.....

Important! The Disk Partition screen not only allows you to create new partitions, but also displays information on the existing partitions on the disk. By default, the RDM hidden partition information appears as the first entry in the partitions list. This partition is detected by the UnixWare installation program as Others. Therefore, when creating a UnixWare partition, DO NOT select Others. Doing so allows UnixWare to overwrite the RDM hidden partition.

4. Continue to follow all onscreen instructions to complete the installation.

SCO Internet FastStart

The default option for Hard Disk Setup is Unix only: Bad blocking 0 FF. Do NOT accept this default option. This will overwrite the RDM partition.

Follow these steps to install SCO Internet FastStart:

1. Boot the system with the FastStart v1.0 boot diskette and the SCO Internet Family Release 1.0 CD-ROM loaded in their respective drives.
2. Follow all onscreen instructions until you reach the Hard Disk Setup entry.
3. Choose Interactive fdisk/divvy.
4. Choose either Use the Rest of the Disk for Unix for allocating the remaining space to Unix, or Display Partition Table to customize it.



.....

Note: You must perform steps 2 through 4 to ensure that you do not overwrite the RDM hidden partition.

5. Continue to follow all onscreen instructions to complete the installation.

► Troubleshooting

This section lists the common problems that you may encounter during RDM operation, followed by the possible corrective action(s).

ASM Pro Server Agent troubleshooting

1. The RDM Work Mode parameter is grayed out.
Check the RDM module and make sure that it is properly plugged into its socket.
2. The message "No RDM Hidden Partition" appears.
Do the following:
 - a. Enter the BIOS Setup.
 - b. Set the Hidden Partition to Enabled.
 - c. Exit the BIOS Setup and save your changes.
 - d. Make sure that you have created the hidden partition. Refer to section 2.2.3 for instructions. In case you need to recreate the RDM hidden partition, do not forget to back up all important files before you proceed. RDM partition creation destroys all data on the hard disk due to the requirement that the RDM hidden partition must be the first partition on the primary hard disk.

RDM Console manager troubleshooting

1. When running any DOS application that requires ALT + hotkey, RDM Console cannot transmit key to the agent site due to the Windows operating system interception.
Instead of just pressing ALT + hotkey, press Shift + F1 followed by the hotkey.
2. Shadows appear on the screen.
Do either of the following:
 - Click on the Refresh button to refresh the screen.
 - Click on the Hang-up button to disconnect.

Modem troubleshooting

The RDM program does not run properly. Check the baud rate of your modem. The recommended baud rate is 57600 Kbps.

Hidden partition troubleshooting

If there are bad sectors or other damage in the hidden partition, do the following:

1. Insert a bootable diskette into the diskette drive.
2. Enter the BIOS Setup and set the Hidden Partition parameter in the RDM BIOS to Enabled.
3. After the system boots from the diskette drive, use the Disk Repair tool to troubleshoot the partition.

BIOS messages

The following table lists the BIOS status and error messages that you might encounter when using RDM.

BIOS Message	Description
RDM Enabled But Modem Not Ready	RDM Work Mode is set to Reboot or Waiting; however there is no modem available for the RDM module. Check if there is a modem connected to serial port 2. Make sure that it is ON.
RDM Dialing Out. Please Wait...	RDM Console function has been enabled. BIOS will dial out to connect to the RDM Console. This process will take a couple of minutes.
Connect Fail: Serial 2 Disabled	Serial 2 is disabled. Enter the BIOS Setup, select the System Security option, and set an I/O port for serial 2.
Connect Fail: Modem Off	Modem is OFF. Check if modem is connected to serial 2. Make sure that it is ON.

BIOS Message	Description
Connect Fail: Modem Initial Command Fail	The default modem initial command failed. Consult your modem's manual. The BIOS default command is AT&F1&C1V0X0M1L2S7=120
Connect Fail: No Dial Tone	Modem cannot detect a dial tone. Make sure that the telephone is working properly.
Connect Fail: Line Busy	RDM Console is busy now. Wait for a few minutes, then try reconnecting.
Connect Fail: No Answer	No response from the RDM Console. Make sure that the RDM Console phone number is correct.
Connect Fail: No Telephone to Dial	RDM Console is enabled, but no RDM Console phone number is set. Enter the BIOS Setup, select the Remote Diagnostic Configuration option, and enter the RDM Console number in the Remote Console parameter screen.
Connect Fail: User Stop Dialing Out	The key is pressed during the RDM dialing out process. Do not press while RDM is dialing out unless you want to stop the connection process.
No RDM Hidden Partition	RDM hidden partition is enabled, but no hidden partition is created on the hard disk. Enter BIOS Setup, select the Remote Diagnostic Configuration option, and disable the Hidden Partition parameter. This returns your system to its normal booting process.

15 ASM Pro Web-based Manager

ASM Pro Web-based Manager (AWM) allows you to manage your network systems on the Internet using any existing browser. Thus, allowing you to conveniently monitor servers on your network without sacrificing efficiency. AWM uses the function and feature of ASM Pro Console with some differences in GUI design and item layout.

► Installing AWM and Microsoft Internet Information Service (IIS)



.....

Note: You have to install Microsoft IIS before installing AWM. If your system already have Microsoft IIS installed then AWM automatically configures IIS. Skip the “Setting up Microsoft IIS” section if this is the case.

System requirements

- Intel 486 or higher processor
- 64MB of RAM
- 10MB free hard disk space
- Windows NT Server 4.0 or Windows 2000 with the following:
 - Microsoft Internet Information Server 2.0 or later (5.0 is recommended)
 - Microsoft Active Server Pages (ASP)
 - SNMP Service
- Ethernet card
- Modem

Setting up Microsoft IIS



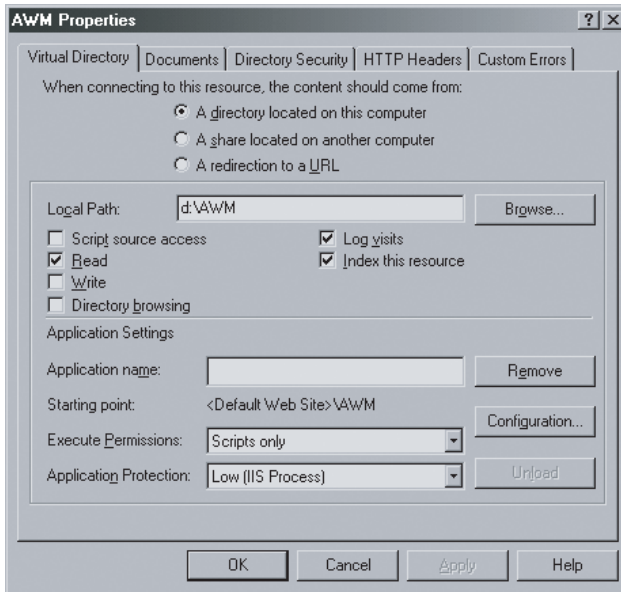
.....

Note: If you have IIS version 5.0 the directory is automatically added.

To set up Microsoft IIS:

1. Open your IIS configuration program and check the virtual directory setting. The IIS setup program is located in the Windows NT Server Optional CD or you can also download it from the Microsoft Website.

2. Check the virtual directory. If there is no virtual directory for AWM, create one and name it AWM. Point it to the directory where the AWM main files are installed (e.g. D:/AWM).



3. After adding the virtual directory, click **OK** to save changes and exit.

Installing AWM



Note: AWM and ASM Console can not be installed in the same system.

To install AWM:

1. Insert the management CD into the CD-ROM drive on your system.
2. Click Applications button.
3. In Applications lists, select "ASM Pro Web-based Manager V4.50 (AWM)".
4. Click "**Setup**" button.
5. Follow the installation wizard.

6. Click finish to complete the installation.



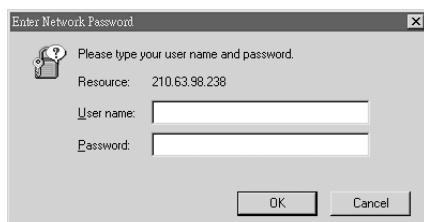
Note: For Windows NT 4.0, AWM will automatically install WbEM core or WbEM SNMP Provider if not installed. For Windows 2000, the WbEM core is built-in. AWM will only install the WbEM SNMP Provider if it is not yet installed. After installing either of these components, the system needs to reboot.

Running AWM

Type this address in your browser:

`http://{IPADDRESS}:9999/AWM`

The password window appears prompting for authentication as shown below.



To access AWM, enter your user name and password and then click **OK**.

AWM confirms the user name and password and displays the main page.

AWM doesn't provide security features itself. All the security issue relies on the web server. If your AWM is installed in IIS 5.0, AWM will choose NTLM authentication by default.

normally there are three ways to authentication the user: Basic authentication, SSL, and NTML authentication.

- Basic authentication is the standard method defined in HTTP protocol, nearly all the web server and browser support this authentication. But the user name and password are transferred in almost clear text. Sometimes it is a big threaten to security.
- SSL is a protocol which can provide a security transport layer for HTTP. It is now supported by nearly all the web server and browser. But in order to make it work, you must first obtain a server certificate from a CA (Certificate Authority). and the user which want to use AWM must also get a client certificate.
- NT authentication is only supported by Microsoft products. That means you must use IIS as the web server, and IE as the browser. The

advantage of NTLM authentication is that it can facilitate the NT authentication system. You don't need another user account database.

For more detailed information, please refer to IIS's documents.

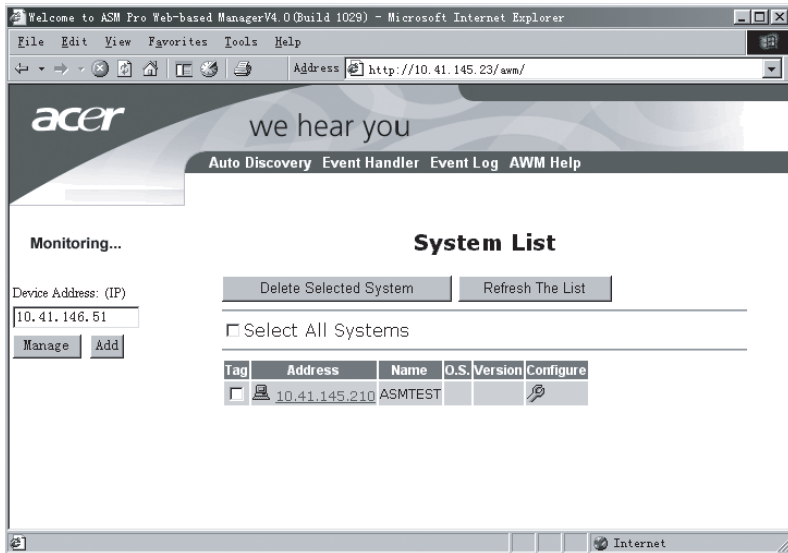
Changing the security configuration in IIS 5.0

1. open the IIS management application, select the awm virtual directory;
2. Click "Properties" button in the toolbar, a property sheet will display;
3. Click the "Directory Security" page.
4. Click "Edit" to change the configuration.

You can choose any of the above methods to protect your web application.

► AWM user interface

AWM's user interface includes a series of web pages that displays system information and configuration. The pages are designed so that each time you click on a function it displays in a new window allowing you to view multiple pages at a time. Shown below is the main page of AWM.



Item	Description
Auto Discovery	<p>Shows the current state of network devices allowing you to view different portions of your network. It also displays the gateways and subnets in your network system. If you are using AWM for the first time, AWM automatically discovers devices on your network.</p> <p>Note: The Network views described here are drawn by a Java Applet. If your browser does not support applets or if there is an intervening firewall that prevents the applet from connecting to AWM, this view may not show up. However, you will still be able to manage your network using the mechanism described in page 394.</p>
Event handler	Configures event actions that should be taken when an event occurs. Currently supporting three kinds of actions: browser notify, send mail, and call pager
Event log	Records event information and saves them to file for future reference
System Help	If you don't know what to do...
Alarm/Monitoring	<p>Allows you to change the event information as you see fit. All events are classified by types and listed in the left frame in tree view.</p> <p>Displays history of events as they occur. This feature is useful as a warning mechanism. It flashes an icon on the main page to inform you if an event occurs</p>
Device Address (IP or Name)	Type the name or the IP address of the device or click the pull down menu to choose from an existing list of devices
Add	Click this check box if you want to include the device name or address in the Device Address box
Manage	Opens a management window for the specified device
Delete selected system	Delete the selected system in the system list

Item	Description
Refresh the list	Updates the system list
Select all system	Select all the system in the system list

Deleting a device from the system listing

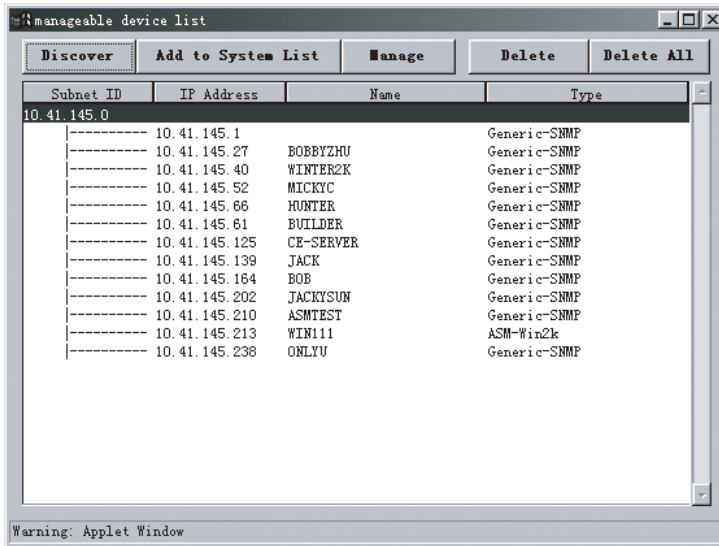
Too many unused device in AWM slows down system operation. it also males the database too large wasting valuable disk space. To make the system more efficient, you can delete unused devices in the database.

To delete a device, select the device to be deleted and then click the **Delete selected system** button.

To delete all devices, click the **Select all system** checkbox and then click the **Delete selected system** button again.

► Auto Discovery

The Auto Discovery window displays a list of manageable network devices (left panel) and its respective properties. It also functions like a navigation panel to your network topology. From this list you can choose which device to manage.

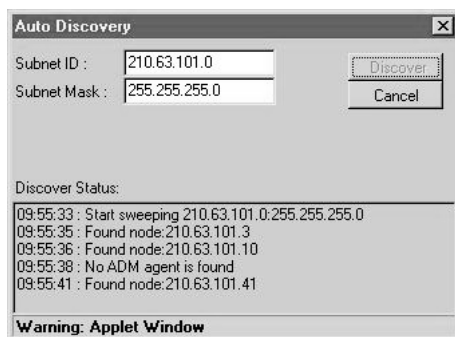


Using Auto Discovery to add a network device

The Auto Discovery function automates the search process for manageable network devices. It recognizes a variety of devices such as routers, printers, gateways, etc. The process may take some time depending on the size of your network.

Auto Discovery undergoes two processes. First, it identifies live nodes on the subnet and then check if the node have IP Forwarding. Then it fetches the name, number of the interface of the node. Second, it fetches the IP table for all Gateways (IP Forwarding nodes). AWM then builds a list of the network from the information gathered by the discovery process.

To access the Auto Discovery function, click on the **Discovery** button. The Auto Discovery dialog box appears.



To start the discovery process:

1. Enter the subnet ID and Mask and then click the **Discover** button. The process might take some time depending on the size of your network.
2. After Auto Discovery finish detecting manageable network devices, the Cancel button will change to Close.
3. Click the **Close** button to exit. The discovered devices displays in the left panel of the Dynamic Network View window.

Adding a device to the system listing

To add a device to the system listing:

1. In the Auto discovery window. Select the device you want to add to the system listing.
2. Click the **Add to system** button. The device is then listed in the system listing in the main window.

► Management pages

To open management pages, click on the device in the main AWM page. You can also do this through the Auto Discovery page - after retrieving a node, select a device and then click the **Manage** button.

The management pages allows you to view device information. To obtain this information, select an option from the menu tree located on the left of the page. The options of the Information menu vary, depending on which of the subagents is selected.

AWM management pages can be classified into two categories:

- ASM Pro management pages for Server devices that have ASM Pro agent installed
- MIB-2 browser pages for Generic SNMP devices that support SNMP RFC1213 MIB



.....

Note: The left hand side of the web pages are management commands. When you click on each function, the command subtitle shows and only when you click on each subcommand (the one with the big orange dot in front) that AWM shows its data on the right side of the page.

ASM Pro Management Pages

Basic System Information

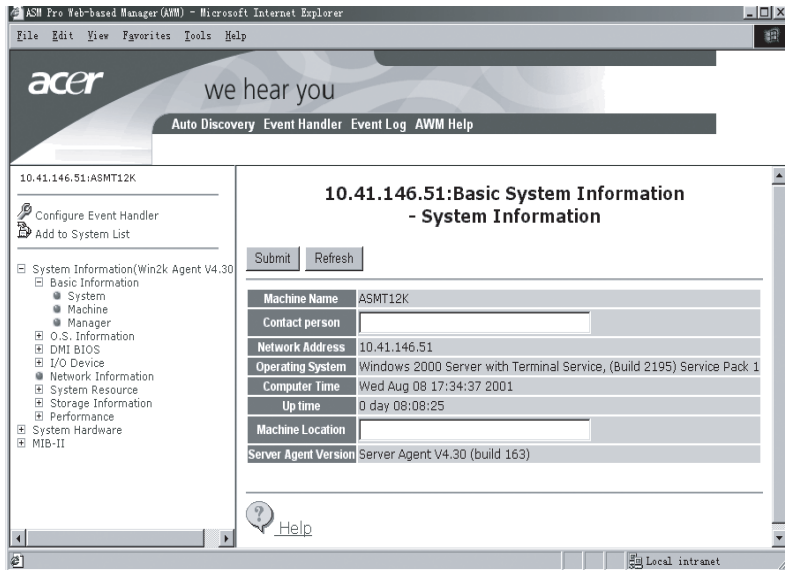
System page

Click the **System page** to view general information about the system. This page also shows the system's contact person, network address, and System Agent version.



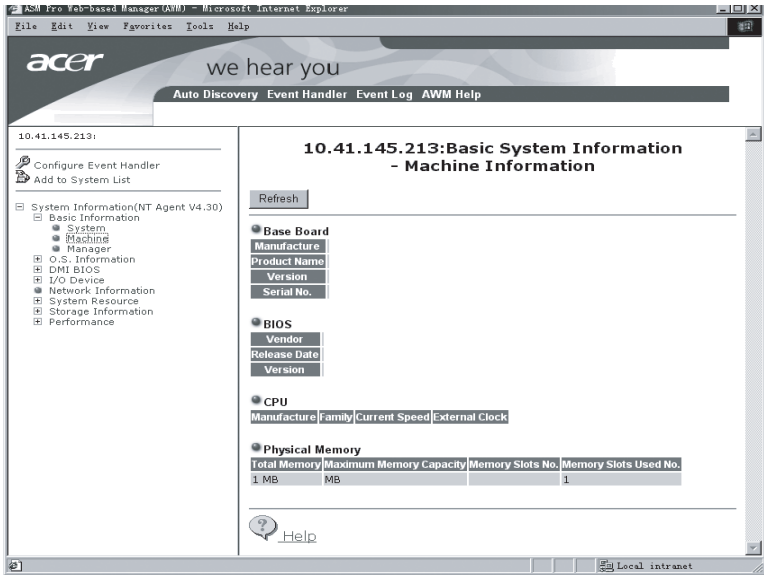
.....

Note: If agent is password protected, the **Submit** button will be shown. Also, an additional item, Machine Name, will be displayed.



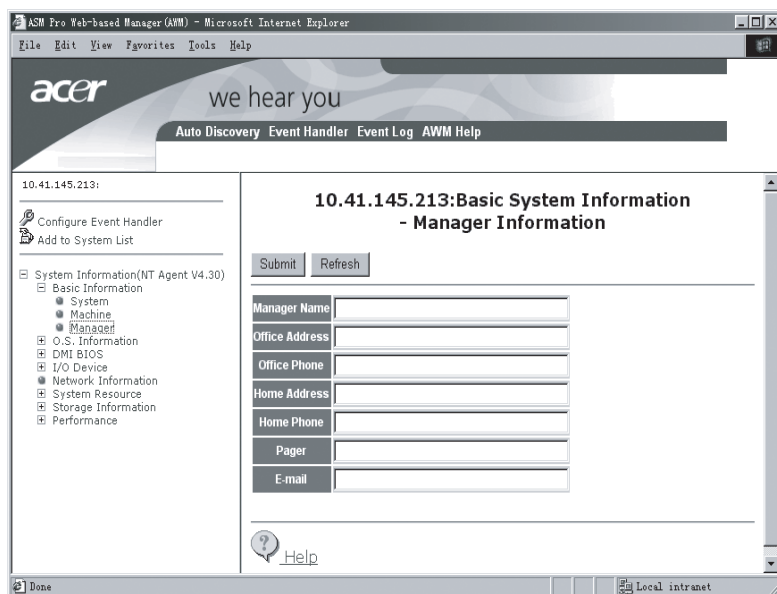
Machine page

Click the **Machine** page to view general information about the system's components, such as: Base Board, CPU, BIOS, and Physical Memory.



Manager page

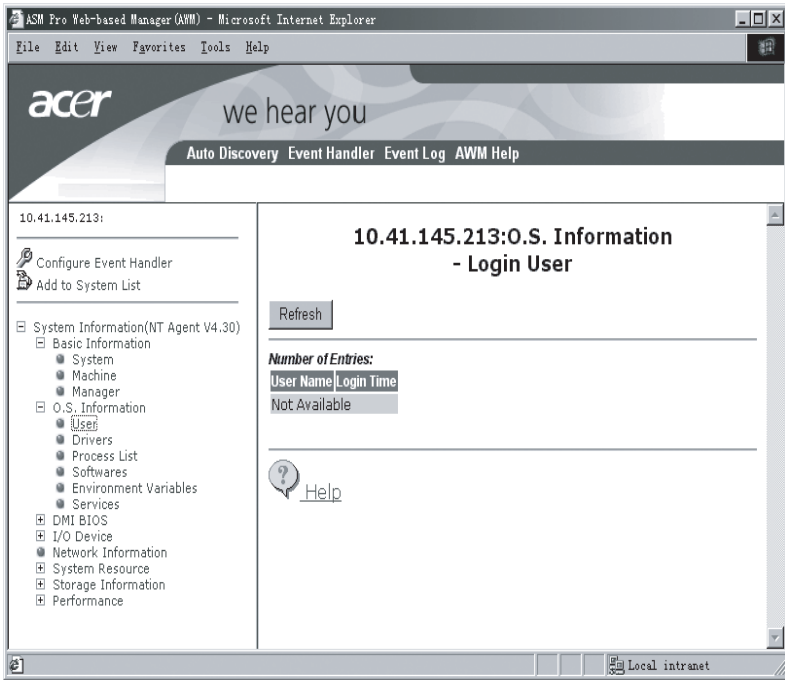
Click the **Manager** page to view information about the person in charge of the system.



O.S. information

User page

The **User** page displays the number of users currently logged on to the server.



Drivers

The **Drivers** page displays all the device drivers installed in the server.



Process list

The **Process list** page displays the programs and DLL libraries that are currently running on the system. To terminate a process in the list, select the process and click the **Kill** button.

10.41.146.51:ASMT12K

Configure Event Handler
Add to System List

System Information(Win2k Agent V4.30)

- Basic Information
 - System
 - Machine
 - Manager
- O.S. Information
 - User
 - Drivers
 - Process List
 - Software
 - Environment
 - Process List
 - Files
- DMT: BIOS
- I/O Device
- Network Information
- System Resource
- Storage Information
- Performance
- System Hardware
- MIB-II

10.41.146.51: O.S. Information
-Process List

Refresh

Number of Entries: 33

Process Name #	ID	Start Time
AFileTrans	636	Wed 09:26:54 Aug 08 2001
Agent32	688	Wed 09:26:54 Aug 08 2001
Agent32Srv	652	Wed 09:26:54 Aug 08 2001
csrss	204	Wed 09:26:42 Aug 08 2001
DESKMENU	2976	Wed 16:12:00 Aug 08 2001
dfsSvc	1460	Wed 09:27:00 Aug 08 2001
dllhost	3032	Wed 09:30:05 Aug 08 2001
explorer	3308	Wed 09:27:50 Aug 08 2001
Idle	0	N/A
inetinfo	3928	Wed 14:20:39 Aug 08 2001
IpMipAgent	696	Wed 09:26:54 Aug 08 2001
lsassrv	720	Wed 09:26:55 Aug 08 2001
lsass	268	Wed 09:26:45 Aug 08 2001
lsrv	1004	Wed 09:26:58 Aug 08 2001
mdm	3428	Wed 09:27:53 Aug 08 2001
msdtc	516	Wed 09:26:52 Aug 08 2001
mstask	808	Wed 09:26:56 Aug 08 2001
RcServer	792	Wed 09:26:56 Aug 08 2001
RcSvc	764	Wed 09:26:55 Aug 08 2001
regedit	972	Wed 09:39:29 Aug 08 2001

javascript: onTopicClick('root_asm_os_proc', 'asm_pages/win/asm_os_proc.asp?ip=10.41.146.51') Local intranet

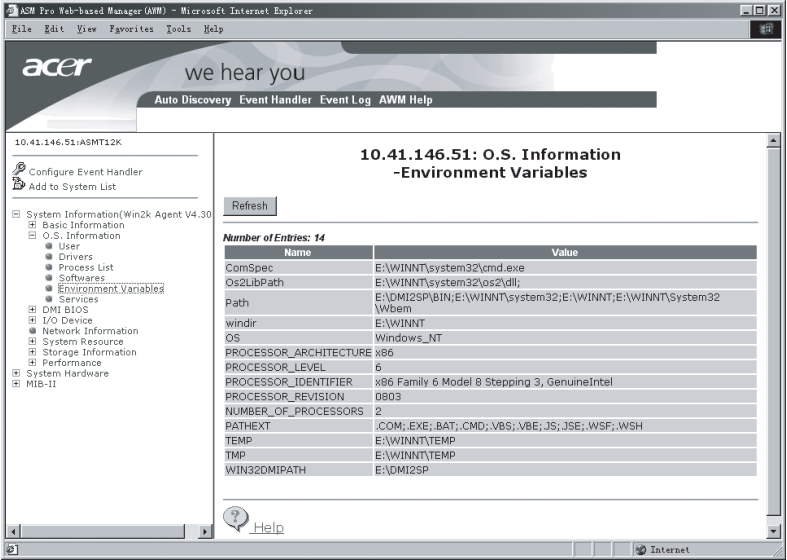
Softwares

The **Software** tab displays the software packages currently installed on the server.



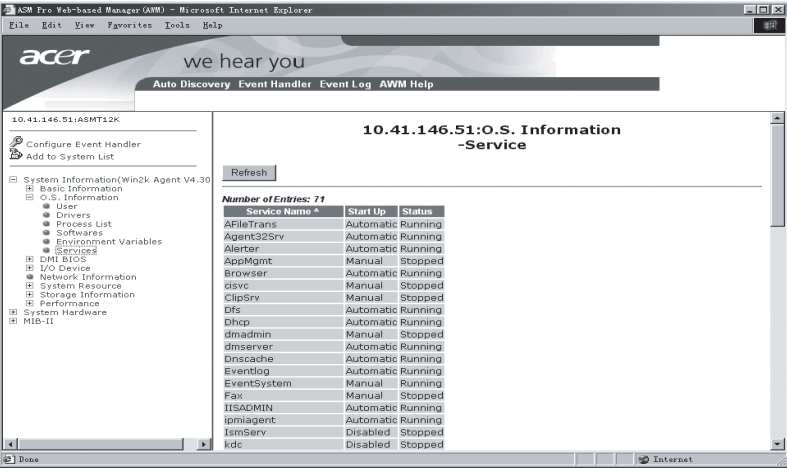
Environment variables

The **Environment Variables** tab displays the contents of the initialization file of the operating system.



Service

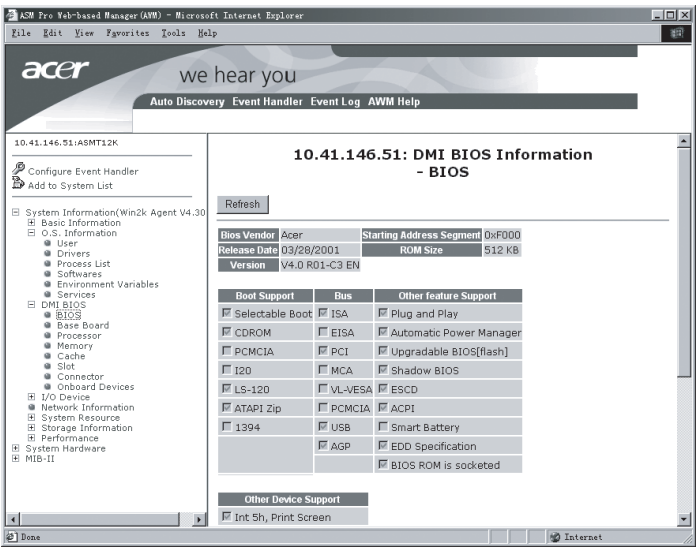
The **Service** tab displays the number of services currently active in the server.



DMI BIOS Information

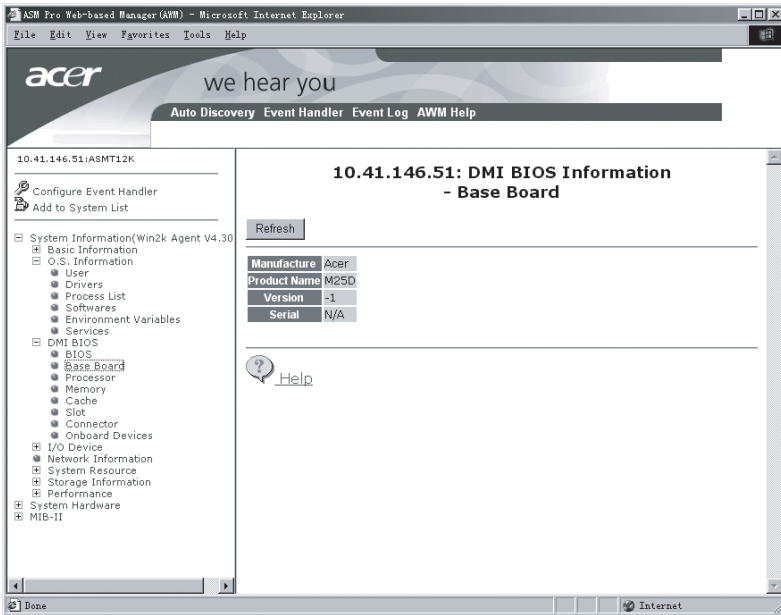
BIOS

The **BIOS** page displays general information about the BIOS version installed in the system. It also shows the type of hardware supported by the BIOS. The check marks show the supported bus, function, boot device, int13 floppy status, and other services based on the DMI specification used.



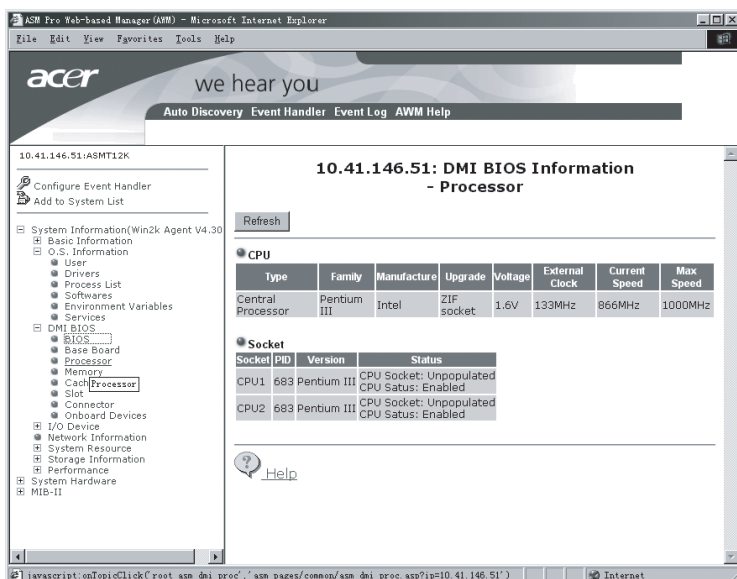
Base board

The **Base Board** page shows the manufacturer, product name, version and serial number of the base board.



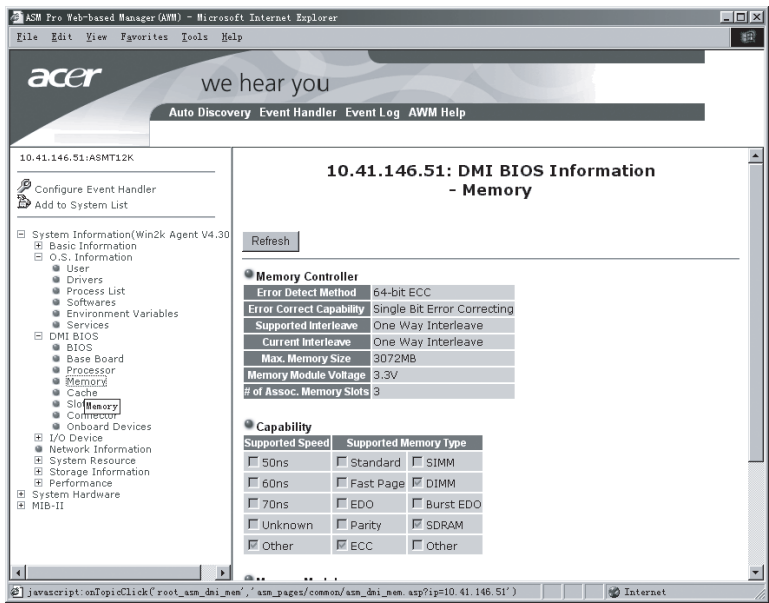
Processor

The **Processor** page shows the type, speed, version number, and other information about each CPU on the server.



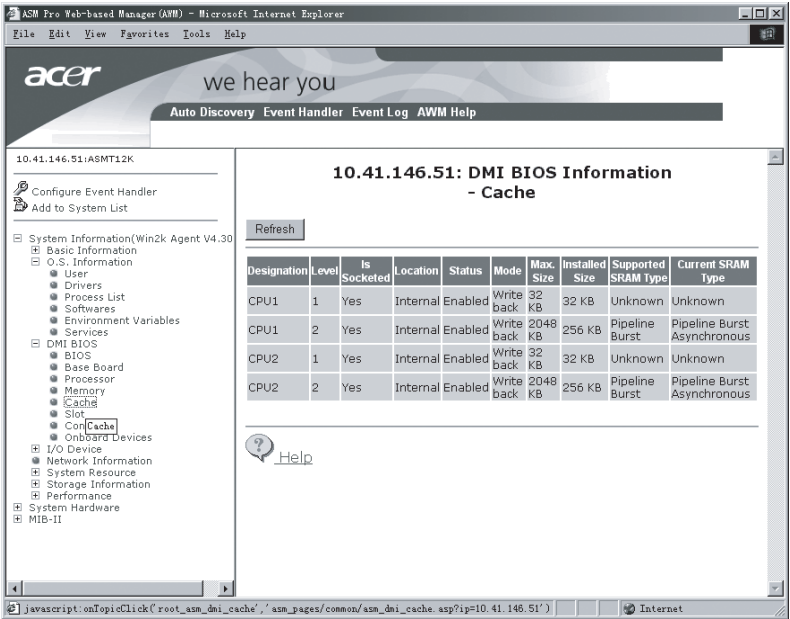
Memory

The **Memory** page displays information about the memory controller and the memory module.



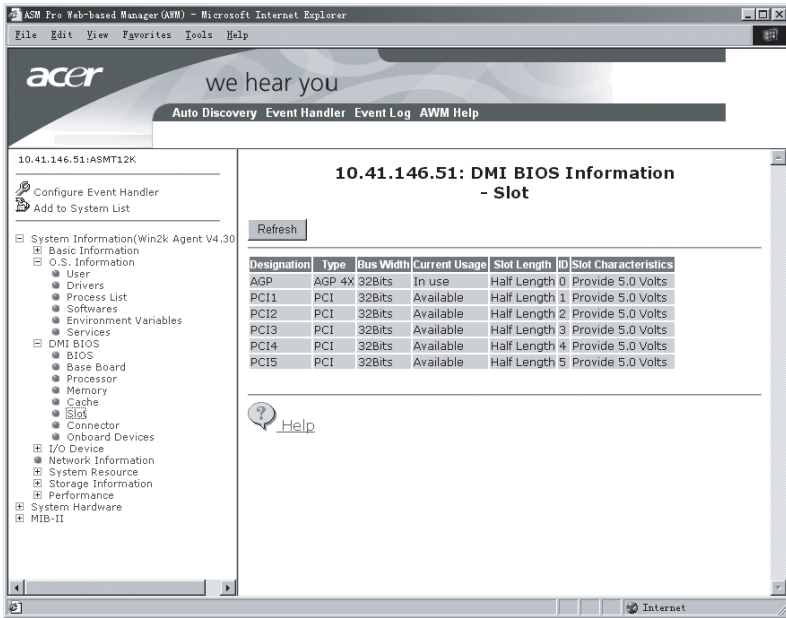
Cache

The **Cache** page displays attributes of CPU cache devices.



Slot

The **Slot** page displays information about different slots on the system board, including the type and availability of each bus. Please refer to the EISA or PCI specification for definitions of the slot IDs.



Connector

The **Connector** page displays information about the motherboard connectors.

10.41.146.51:ASMT12K

Configure Event Handler
Add to System List

System Information (Win2k Agent V4.30)

- Basic Information
- O.S. Information
 - User
 - Drivers
 - Process List
 - Softwares
 - Environment Variables
 - Services
- DMI BIOS
 - BIOS
 - Base Board
 - Processor
 - Memory
 - Cache
 - Slot
 - Connector
 - Onboard Devices
- I/O Device
- Network Information
- System Resource
- Storage Information
- Performance
- System Hardware
- MTB-IT

10.41.146.51: DMI BIOS Information - Connector

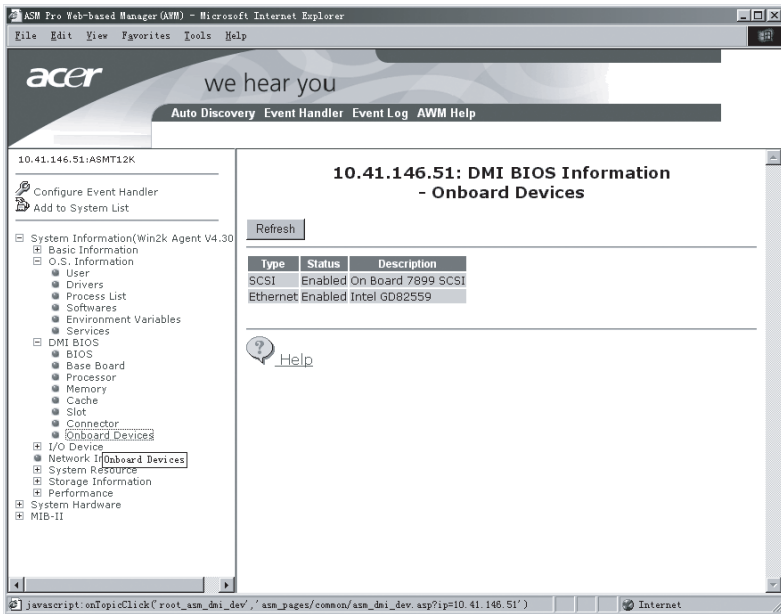
Refresh

Internal	Type	External	Type	Port Type
N/A	None	SERIAL1	D89 pin male	Serial Port 16650A Compatible
N/A	None	SERIAL2	D89 pin male	Serial Port 16650A Compatible
N/A	None	PRINTER	DB25 pin female	Parallel Port ECP/EPP
N/A	None	KEYBOARD	PS/2	Keyboard Port
N/A	None	MOUSE	PS/2	Mouse Port
N/A	None	USB1	Access BUS	USB
N/A	None	USB2	Access BUS	USB
IDE1	On board IDE		None	Other
IDE2	On board IDE		None	Other
FDD	On board floppy		None	Other

Help

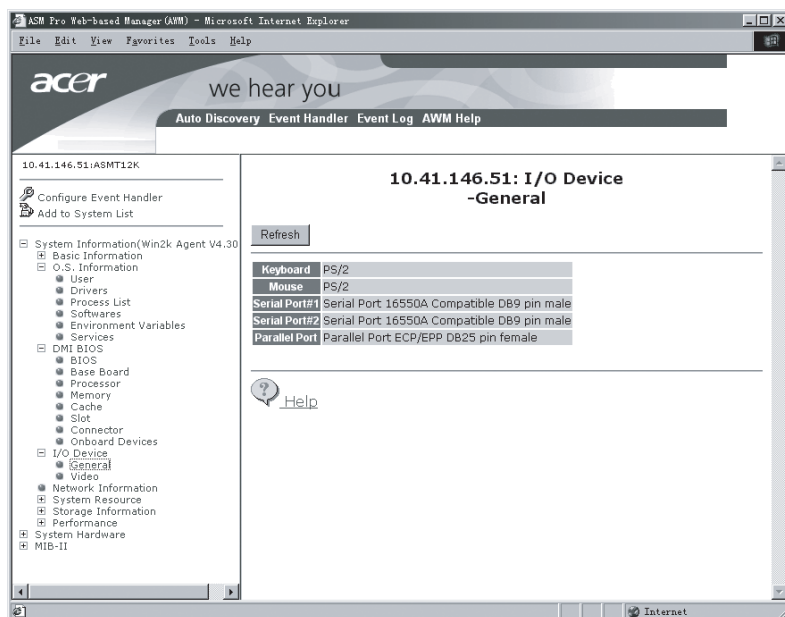
Onboard device

The **Onboard Device** page displays information about devices found on the motherboard.



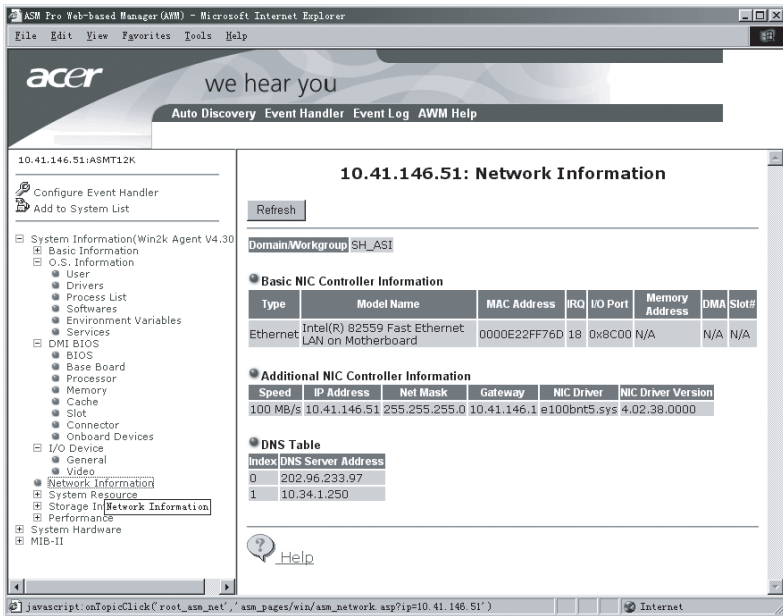
I/O device information

Displays Peripheral information like keyboard, mouse, serial ports, parallel ports, video ports, and etc.



Network information

This page displays information about some of the network interface cards; not all network cards provide this type of information.

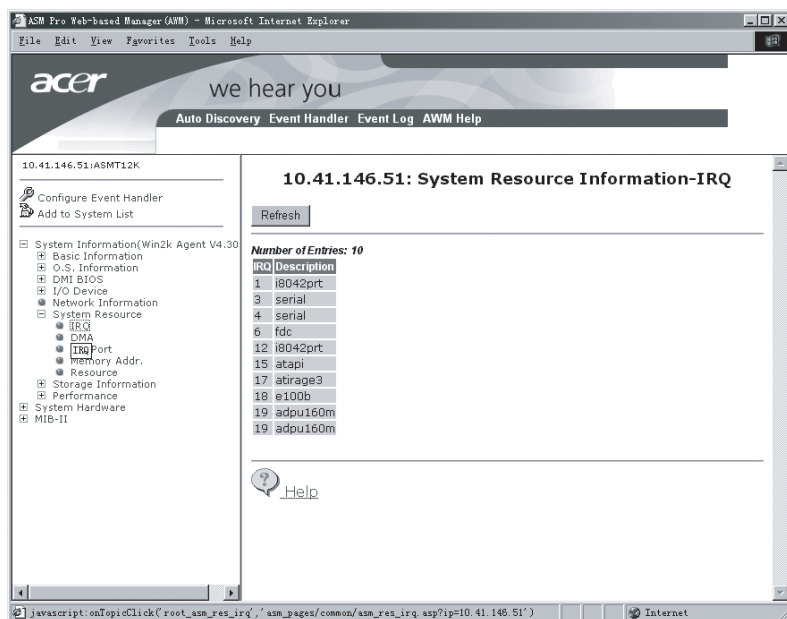


System resource information

System Resource Information consists of four pages: IRQ, DMA, I/O Port, and Memory Address. The following sections briefly describe each of these types of resource information.

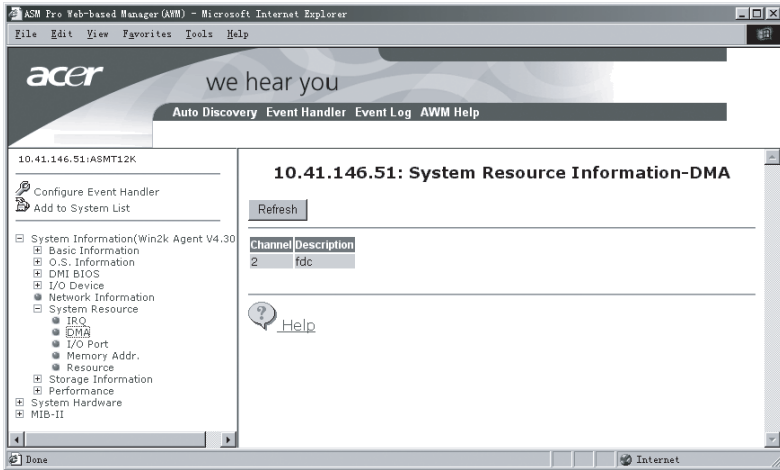
IRQ

This screen displays a list of each IRQ and its assigned usage in the system. It can be used to detect a hardware interrupt conflict.



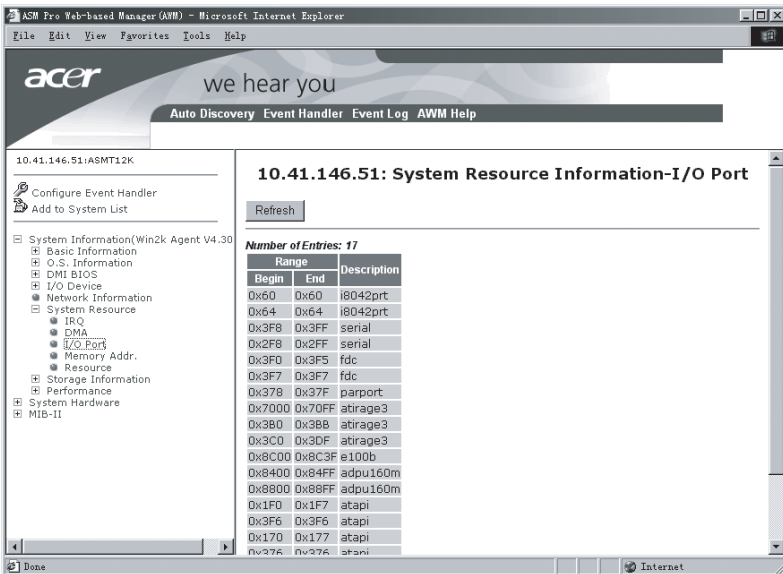
DMA

This screen displays all the DMA channels used by each device in the system.



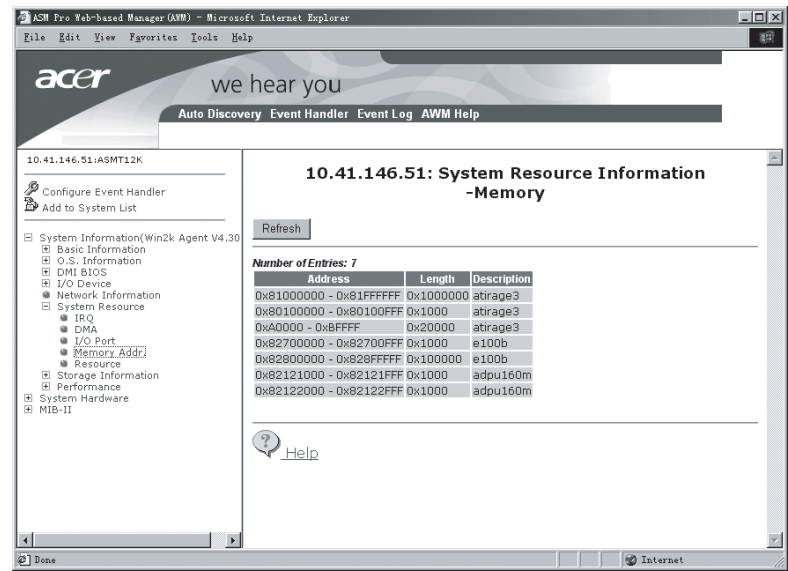
I/O port

This displays the range of port addresses occupied by the system resources.



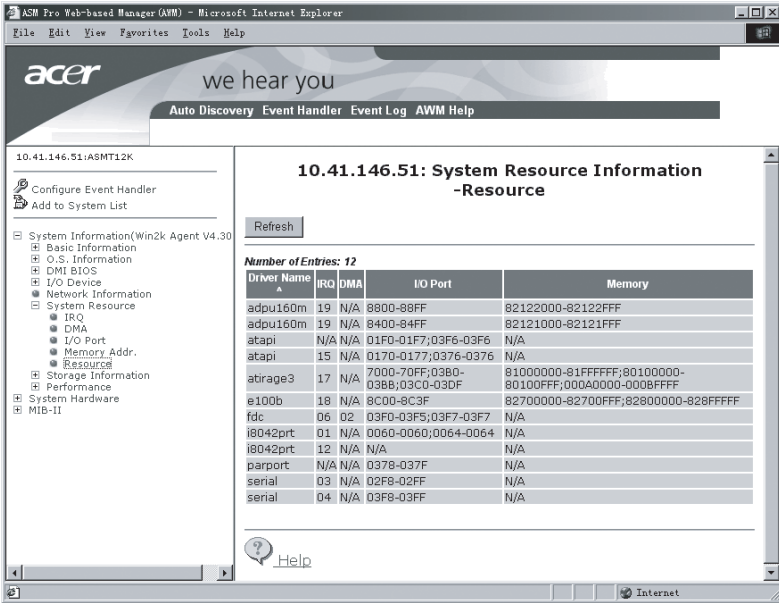
Memory address

This displays the system’s base memory usage, including the address, the length, and its description.



Resource

This displays the system resource use which includes driver-IRQ, DMA, I/O port, and memory usage.



Storage information

The Storage Information page shows information concerning the size, type, and controller of all physical and logical hard disks that are configured on the system.

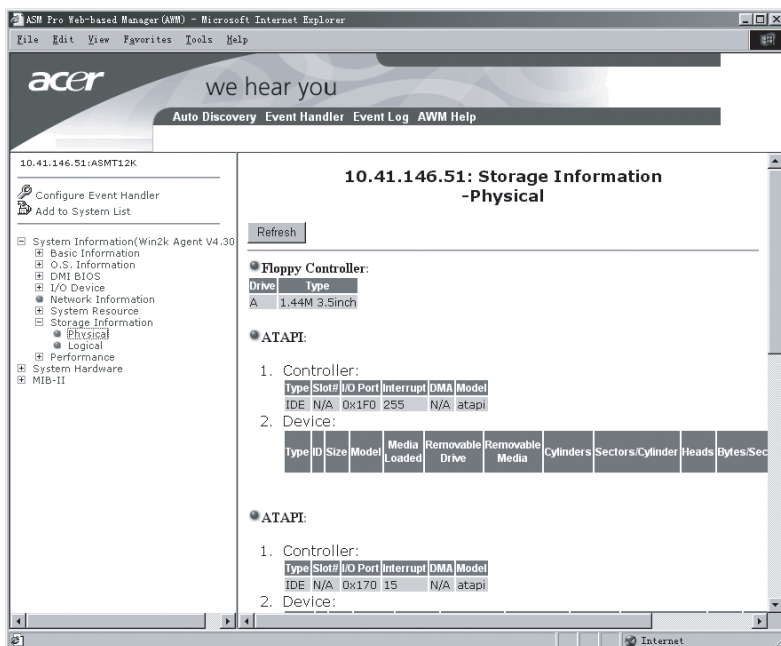
Physical disk

Physical disk indicates the number of actual hard disk drives installed in a system. Each hard disk drive is connected to an adapter that controls them.



Note: The physical disk screen for the desktop systems differ slightly from the screen shown here but the functions are the same.

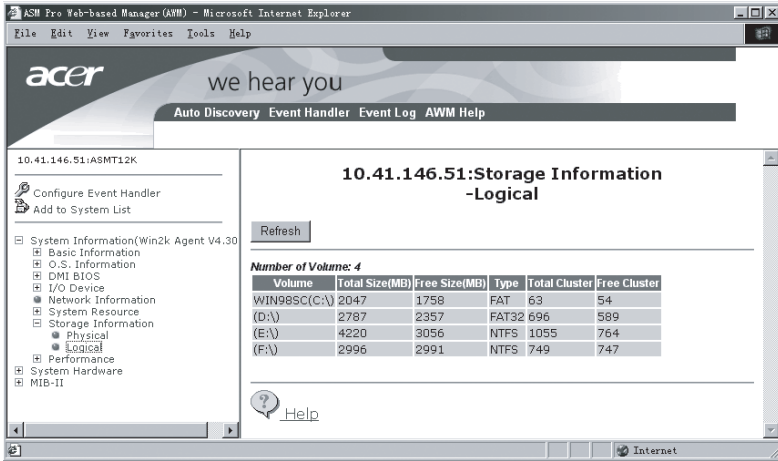
Click **Refresh** to update the information on the screen.



Logical disk

Logical disks are created when you separate a hard disk into several partitions and designate each of them as an independent logical drive. This window shows you information about each logical drive created on the hard disk drives.

Click **Refresh** to update the information on the screen.

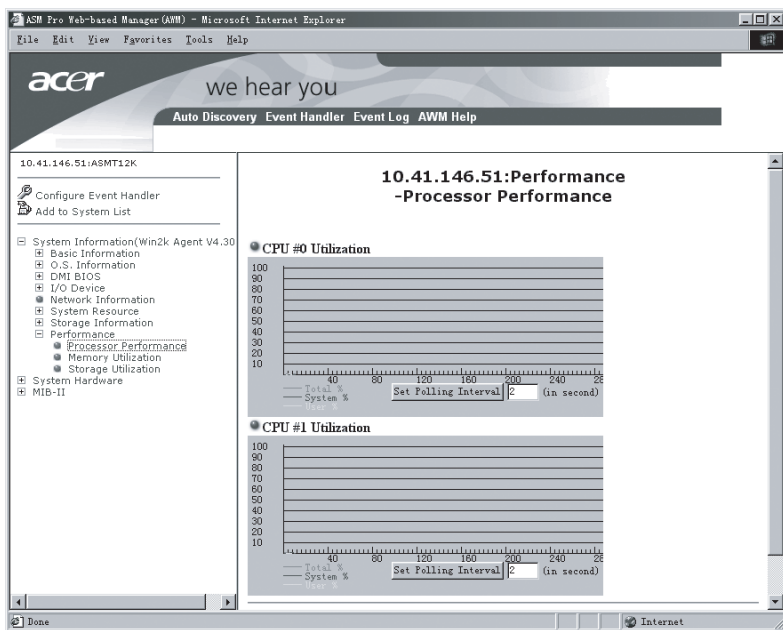


Performance

AWM monitors the performance of each agent periodically and sends this information back to the AWM. The polling interval of the Console can be configured to check the agents whenever the system administrator chooses.

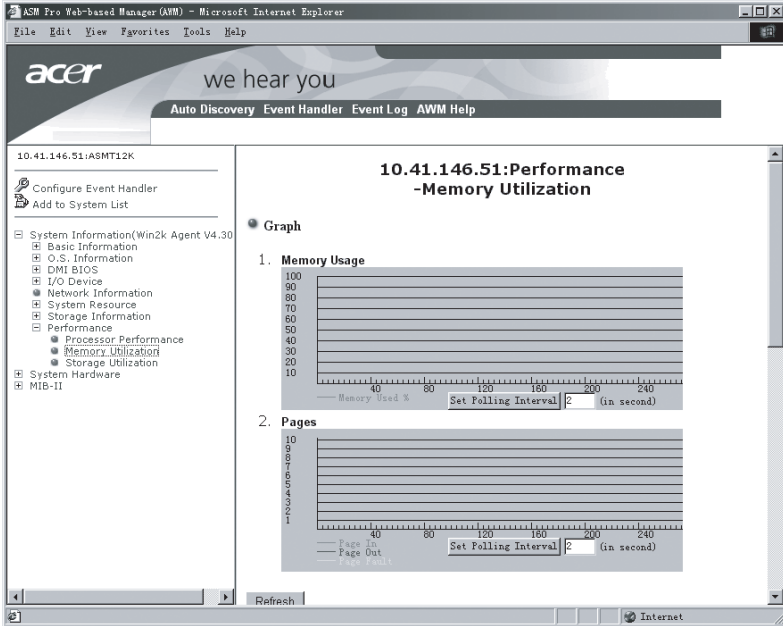
Processor performance

This page displays a line graph showing the current load of each CPU (Central Processing Unit) installed in the system. This can be used to indicate how much load the system has and how well the system's processing power is handling the load.



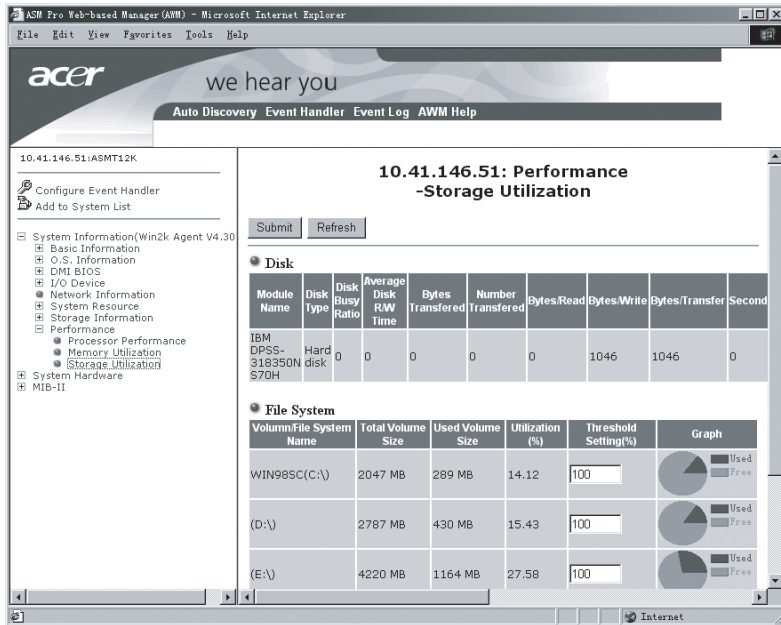
Memory utilization

The Memory Utilization page shows a graph that measures the utilization of system memory and memory paging along a time line. It also displays information like the utilization percentage of used and unused memory in a system.



Storage utilization

The storage utilization page shows the utilization information of your storage devices and file systems. For the file system utilization, you can set a threshold to warn you of excess value.

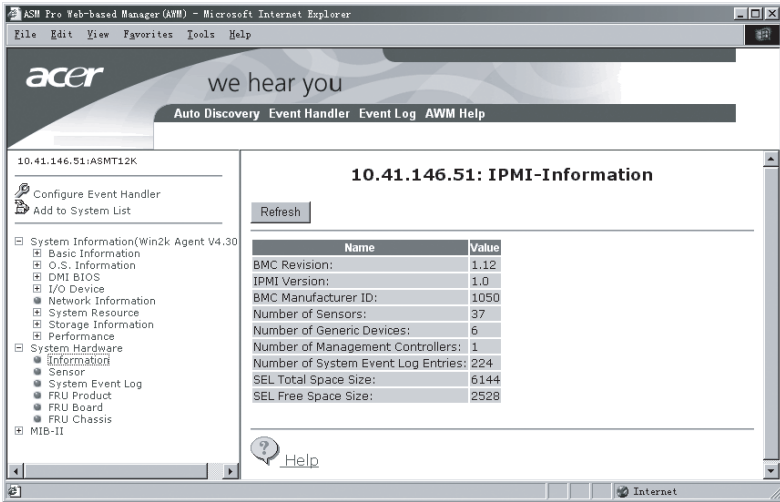


System Hardware

IPMI information

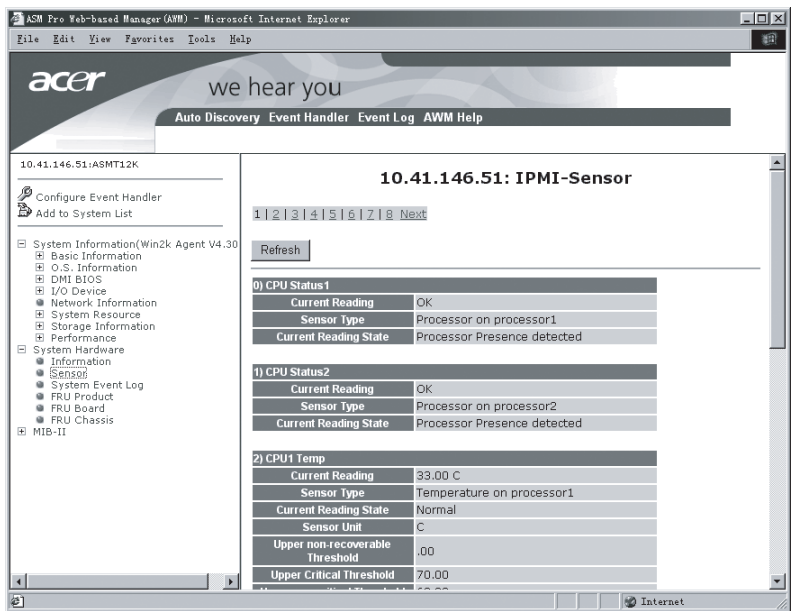
IPMI stands for intelligent Platform Management Interface. IPMI defines common interfaces to the intelligent hardware that is used to monitor the physical health characteristics of the server, such as temperature, voltage, fans, power supplies and chassis. These monitoring abilities provide information that enables system management, recovery and asset tracking.

This page shows the IPMI version, number of sensors, and other things related to IOMI. To refresh the display, click the **Refresh** button.



IPMI Sensor

This page shows the IPMI sensors and their current status. To refresh the display, click the **Refresh** button.



System event log

System event log gathers event information in the systems being monitored and saves them in the event log, click the **Event Log** link in the main page. The system event log page appears.

10.41.146.51:ASMT12K

Configure Event Handler
Add to System List

System Information (Win2k Agent V4.30)
Basic Information
O.S. Information
DMI BIOS
I/O Device
Network Information
System Resource
Storage Information
Performance
System Hardware
Information
Sensor
System Event Log
FRU Product
FRU BIOS
FRU Chassis
MIB-II

10.41.146.51: IPMI-System Event Log

Refresh

Total 224 events: 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4

Index	Time	Event Description
220	0C/E0E9 *E0A 8 17:57:0 2001 GMT	system chassis 1 Physical Security Sensor (Chassis Intrus): General Chassis Intrusion Assertion
221	0C/E0E9 *E0A 8 18:04:58 2001 GMT	system chassis 1 Physical Security Sensor (Chassis Intrus): General Chassis Intrusion Assertion
222	0C/E0EA *E0A 9 09:22:15 2001 GMT	system chassis 1 Physical Security Sensor (Chassis Intrus): General Chassis Intrusion Assertion
223	0C/E0EA *E0A 9 09:27:47 2001 GMT	system chassis 1 Physical Security Sensor (Chassis Intrus): General Chassis Intrusion Assertion

Total 224 events: 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4

Help



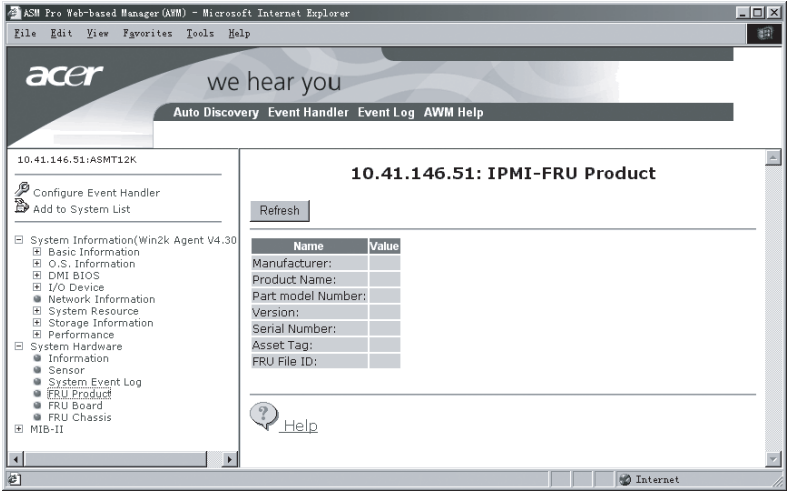
Note: You can sort the information in the table by clicking on the table heading.

To delete log files within a specific time:

1. Click the Delete Log Time Range from and to radio button and specify the date of the event logs you want to delete.
2. Click Submit to delete.

FUR product

Shows the manufacturer's information.



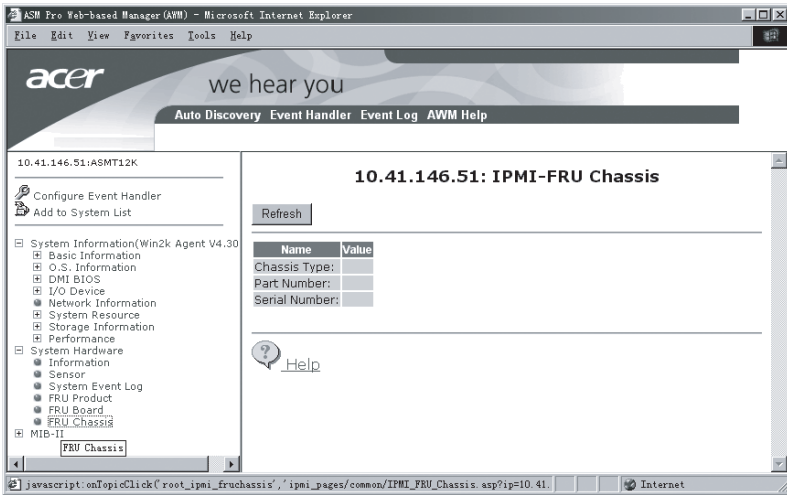
FUR board

Shows system board information.



FUR chassis

Shows chassis description.



Caution: The events described in the following sections that generate alerts are critical. If any of them occur, correct the problem immediately, as damage to your system may result if the problem is not corrected.

MIB-II configuration information

This section includes specifications about MIB-II (Management Information Base), a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allow any SNMP and RMON tools to monitor any device defined by an MIB. For more information about each network working group, please refer to RFC1213.

RMON is a network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it.

The following sections describe the Information menu options that display when an MIB-II subagent is selected in the System Listing window.

System information

Implementation of the system group is mandatory for all systems. If an agent is not configured to have a value for any of these variables, a string of length 0 is returned.

The screenshot shows the ASM Pro Web-based Manager (AWM) interface in a Microsoft Internet Explorer browser window. The interface has a top navigation bar with the Acer logo and the slogan "we hear you". Below this is a menu bar with "Auto Discovery", "Event Handler", "Event Log", and "AWM Help". The main content area is titled "10.41.146.51: MIB-II System". On the left, there is a tree view showing the system hierarchy: "System Information (Win2k Agent V4.30)" > "System Hardware" > "MIB-II" > "System" > "Interface" > "Address Table" > "IP Group" > "Generic" > "Address Table" > "Routing Table" > "Net To Media Table" > "ICMP" > "TCP" > "TCP Statistics" > "TCP Connection Table" > "UDP" > "UDP Statistics" > "UDP Listener Table" > "SNMP". The main content area displays the following information:

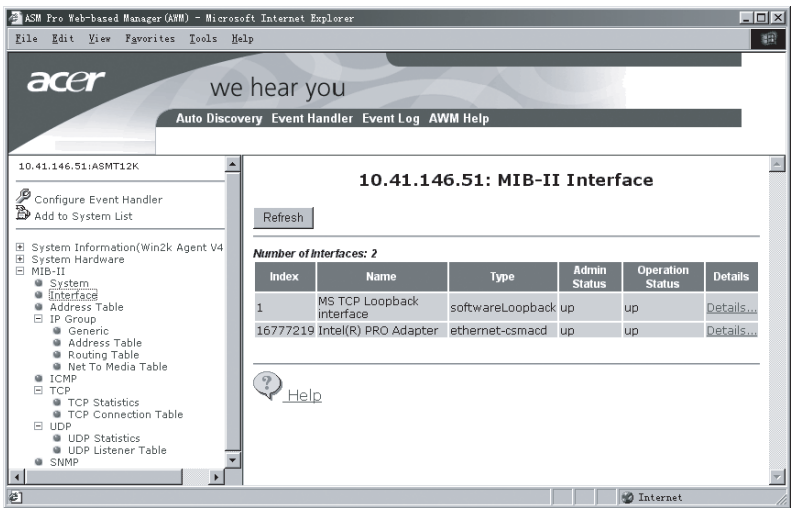
10.41.146.51: MIB-II System	
[Submit] [Refresh]	
System Description	Hardware: x86 Family 6 Model 8 Stepping 3 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)
System Object Identifier	1.3.6.1.4.1.311.1.1.3.1.2
System Up time (time since last reboot)	0days 3:37:56.28
System Contact person	
System name	ASMT12K
System Location	
System services	<input checked="" type="checkbox"/> Application Layer <input type="checkbox"/> Presentation Layer <input type="checkbox"/> Session Layer <input checked="" type="checkbox"/> Transport Layer <input checked="" type="checkbox"/> Network Layer <input type="checkbox"/> Data Link Layer <input type="checkbox"/> Physical Layer

The browser status bar at the bottom shows "Done" and "Internet".

Parameter	Description
System Description	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software
System Object Identifier	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Jayson, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Ann Router'
System Up Time	The time (in hundredths of a second) since the network management portion of the system was last re-initialized
System Contact Person	The textual identification of the contact person for this managed node, together with information on how to contact this person
System Name	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name
System Location	The physical location of this node (e.g., 'telephone closet, 3rd floor')
System Services	A value which indicates the set of services that this entity primarily offers. Layer functionality: 1 - physical (e.g., repeaters) 2 - datalink/subnetwork (e.g., bridges) 3 - Internet (e.g., IP gateways) 4 - end-to-end (e.g., IP hosts) 7 - applications (e.g., mail relays)

Interface

Implementation of the Interface group is mandatory for all systems. Click the **Details** link to display the Details Interface Information page.



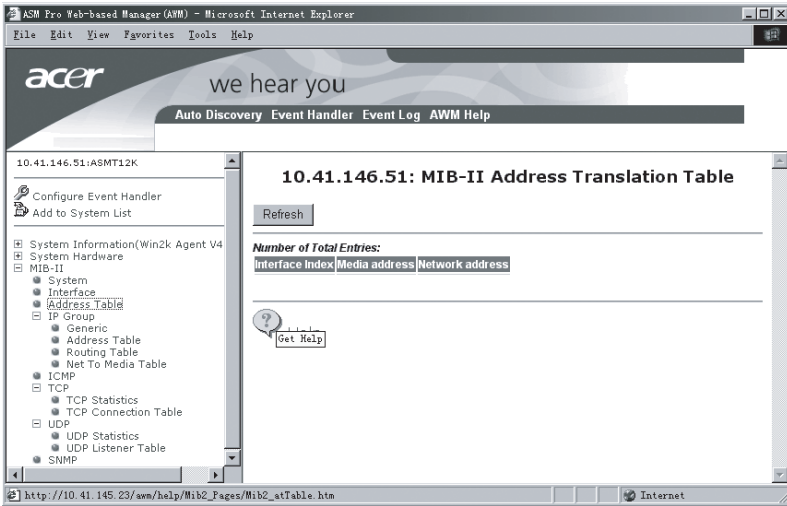
Parameter	Description
Description	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface
Media Type	The type of interface, distinguished according to the physical/link protocol(s) immediately 'below' the network layer in the protocol stack
Administrative Status	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name
Operational Status	The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed
MTU	The size of the largest datagram which can be sent/ received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface

Parameter	Description
Speed	The desired state of the interface. The testing (3) state indicates that no operational packets can be passed
Media Address	The interface's address at the protocol layer immediately 'below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length
Status Last Change	The value of sysUp Time at the time the interface entered its current operational state. If the current state was entered prior to the last re - initialization of the local network management subsystem, then this object contains a zero value
Input: Bytes Received	The total number of octets received on the interface, including framing characters
Input: Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol
Input: Non-Unicast Packets Received	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol
Input: Discard Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space
Input: Received Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Input: Unknown Protocol Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol
Output: Bytes Sent	The total number of octets transmitted out of the interface, including framing characters

Parameter	Description
Output: Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Output: Non-Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent
Output: Discard Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space
Output: Transmit Error	The number of outbound packets that could not be transmitted because of errors
Output: Queue Length	The length of the output packet queue (in packets)
Media Specific MIB OID	A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an Ethernet, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and conformant implementation of ASN.1 and BER must be able to generate and recognize this value

AT (Address Translation)

Implementation of the Address Translation group is mandatory for all systems. Note, however, that this group is deprecated by MIB-II. That is, it is being included solely for compatibility with MIB-I nodes, and will most likely be excluded from MIB-III nodes. From MIB-III and onwards, each network protocol group contains its own address translation table.

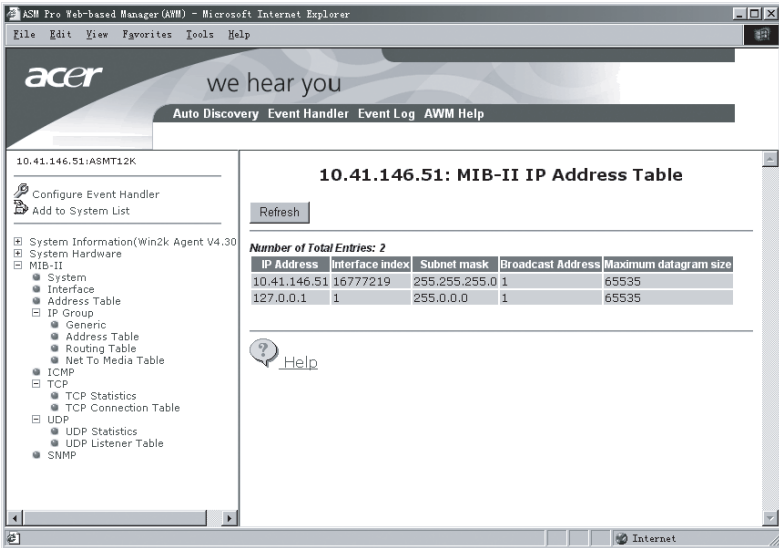


The Address Translation group contains one table which is the union across all interfaces of the translation tables for converting a Network Address (e.g., an IP address) into a subnetwork-specific address. This document refers to such a subnetwork-specific address as a 'physical' address.

Parameter	Description
Media Address	The media-dependent 'physical' address
Network Address	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent 'physical' address

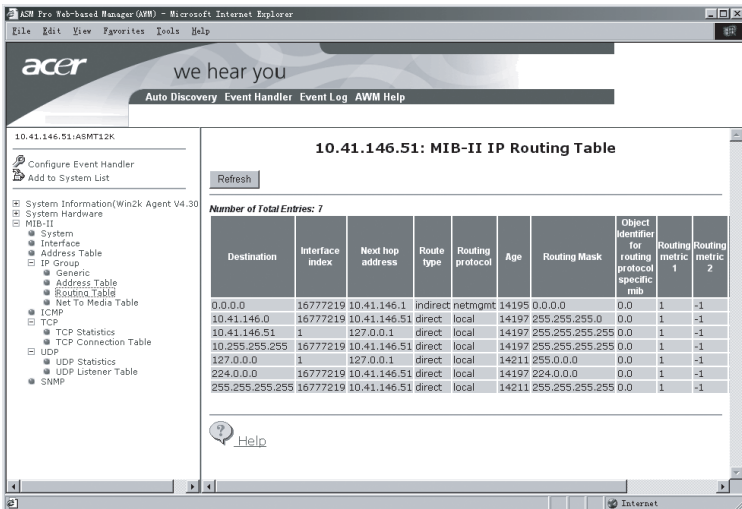
IP (Internet Protocol) group

Implementation of the IP group is mandatory for all systems.

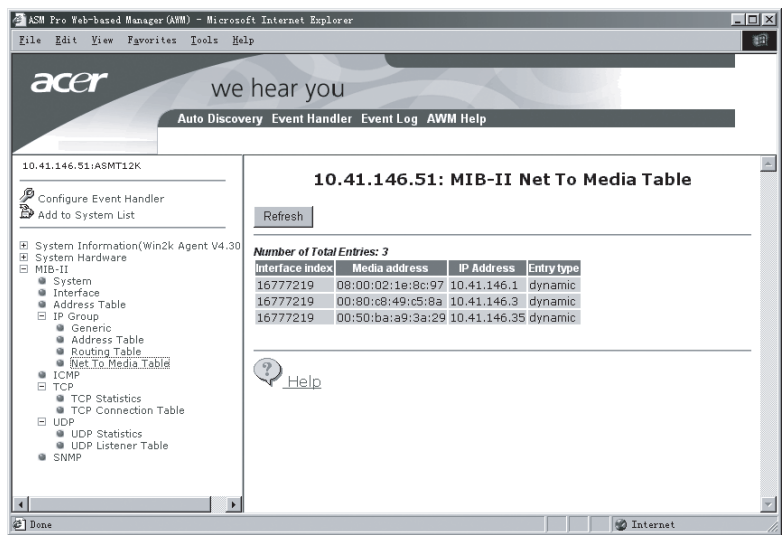


Routing table page

The IP routing table contains an entry for each route presently known to this entity.

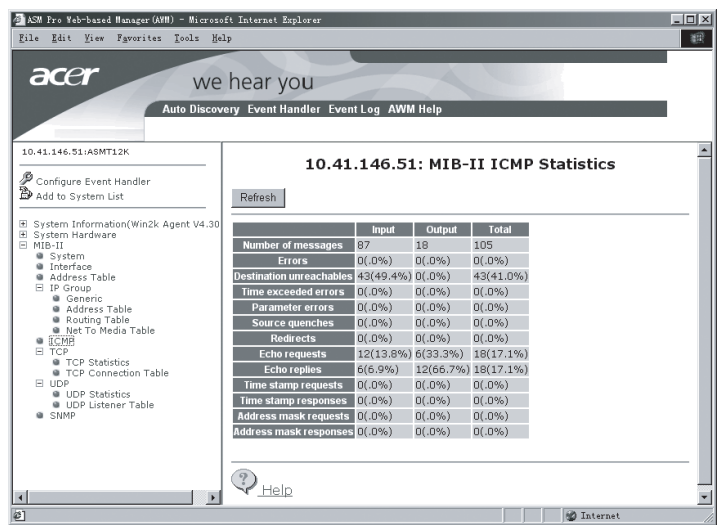


Net to media page



ICMP (Internet Control Message Protocol)

Implementation of the ICMP group is mandatory for all systems.



Parameter	Description
Number of Messages	The total number of messages which the entity received/sent. Note that this counter includes all those counted by InErrors.
Errors	The number of messages which the entity received/sent but determined as having -specific errors (bad checksums, bad length, etc.).
Destination Unreachables	The number of Destination Unreachable messages received/sent.
Time Exceeded Errors	The number of Time Exceeded messages received/sent.
Parameter Errors	The number of Parameter Problem messages received/sent.
Source Quenches	The number of Source Quench messages received/sent.
Redirects	The number of Redirect messages received/sent.
Echo Requests	The number of Echo (request) messages received/sent.
Echo Replies	The number of Echo Reply messages received/sent.
Time Stamps Requests	The number of Timestamp (request) messages received/sent.
Time Stamp Replies	The number of Timestamp Reply messages received/sent.
Address Masks Requests	The number of Address Mask Request messages received/sent.
Address Mask Replies	The number of Address Mask Reply messages received/sent.

TCP (Transmission Control Protocol)

The TCP connection table contains information about the entity's existing TCP connections.

Note that instances of object types that represent information about a particular TCP connection are transient; they persist only as long as the connection in question.

TCP statistics page

The screenshot shows the ACM Pro Web-based Manager (AWM) interface in a Microsoft Internet Explorer browser window. The interface has a top navigation bar with the Acer logo and the slogan "we hear you". Below this is a menu bar with "Auto Discovery", "Event Handler", "Event Log", and "AWM Help". The main content area is titled "10.41.146.51: MIB-II TCP Statistics" and includes a "Refresh" button. A table displays various TCP statistics, including retransmission timeouts, connection counts, and segment counts. A left sidebar shows a tree view of system information, with "TCP Statistics" selected. A "Help" button is located at the bottom right of the main content area.

10.41.146.51: MIB-II TCP Statistics

Refresh

TCP retransmission timeout algorithm	vanj
Minimum retransmission timeout	300 ms
Maximum retransmission timeout	240000 ms
Maximum number of connections	Dynamic
Connections actively opened	44
Connections accepted	64
Connection establishment failures	2
Connection resets	0
Current established connections	0
Input segments	1420
Output segments	1352
Retransmissions	0

Help

Parameter	Description
TCP retransmission timeout algorithm	The algorithm used to determine the timeout value used for re-transmitting unacknowledged octets.
Minimum retransmission timeout	Retrans Min - the minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. Retrans Max - the maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds
Maximum retransmission timeout	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1
Maximum number of connections	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value-1
Connections actively open	The number of times TCPconnections have made a direct transition to the SYN-SENT state from the CLOSED state
Connections accepted	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state
Connections established failures	The number of times TCPconnections have made a direct transition to the CLOSED state or the SYN-REVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state
Connections resets	The number of TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSED-WAIT state
Current established connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT

Parameter	Description
Input segments	The total number of segments received, including those received in error. Those count includes segments received on currently established connections
Output segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets
Retransmissions	The total number of segments retransmitted-that is, the number of TCP segments transmitted containing one or more previously transmitted octets
Input errors	The total number of segments received in error (e.g., bad TCP checksums)
Output errors	The number of TCP segment sent containing the RST flag

TCP Connection table page

The TCP connection table contains information about this entity's existing TCP connections.

The screenshot shows the ASM Pro Web-based Manager (AWM) interface in a Microsoft Internet Explorer browser. The page title is "10.41.146.51: MIB-II TCP Connection Table". The interface includes a navigation pane on the left with a tree view showing the following structure:

- 10.41.146.51/ASMT12K
 - Configure Event Handler
 - Add to System List
 - System Information (Win2k Agent V4.30)
 - System Hardware
 - MIB-II
 - System
 - Interface
 - Address Table
 - IP Group
 - Generic
 - Address Table
 - Routing Table
 - Net To Media Table
 - ICMP
 - TCP
 - TCP Statistics
 - TCP Connection Table**
 - UDP
 - UDP Statistics
 - UDP Listener Table
 - SNMP

The main content area displays the "10.41.146.51: MIB-II TCP Connection Table" with a "Refresh" button. Below the title, it states "Number of Total Entries: 21". The table has five columns: Status, Remote Address, Remote port, Local Address, and Local port. The data is as follows:

Status	Remote Address	Remote port	Local Address	Local port
listen	0.0.0.0	43239	0.0.0.0	21
listen	0.0.0.0	34817	0.0.0.0	25
listen	0.0.0.0	59572	0.0.0.0	135
listen	0.0.0.0	26744	0.0.0.0	445
listen	0.0.0.0	18440	0.0.0.0	1028
listen	0.0.0.0	10280	0.0.0.0	1032
listen	0.0.0.0	59436	0.0.0.0	1033
listen	0.0.0.0	43133	0.0.0.0	1037
listen	0.0.0.0	43094	0.0.0.0	1041
listen	0.0.0.0	10309	0.0.0.0	1066
listen	0.0.0.0	2192	0.0.0.0	3372
listen	0.0.0.0	2160	0.0.0.0	3389
listen	0.0.0.0	2160	0.0.0.0	5000
listen	0.0.0.0	10316	0.0.0.0	5001
listen	0.0.0.0	51385	0.0.0.0	6157
listen	0.0.0.0	18654	0.0.0.0	9907
listen	0.0.0.0	2240	0.0.0.0	9908

Parameter	Description
Status	The state of this TCP connection
Remote Address	The remote IP address for this TCP connection
Remote port	The remote port number for this TCP connection
Local Address	The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used
Local Port	The local port number for this TCP connection

UDP (User Datagram Protocol)

The UDP listener table contains information about the entity's UDP end-points on which a local application is currently accepting datagrams. The tables following the figures describe the functions of the two pages in the MIB-II UDP window — System and Table.

UDP Statistics page

10.41.146.51:ASMT12K

Configure Event Handler
Add to System List

- System Information(Win2k Agent V4.30)
- System Hardware
- MIB-II
 - System
 - Interface
 - Address Table
 - IP Group
 - Generic
 - Address Table
 - Routing Table
 - Net To Media Table
 - ICMP
 - TCP
 - TCP Statistics
 - TCP Connection Table
 - UDP
 - UDP Statistics**
 - UDP Listener Table
 - SNMP

10.41.146.51: MIB-II UDP Statistics

Refresh

Input datagrams	7608
No receiver on port	1094
Input errors	0
Output datagrams	1859

[Help](#)

Parameter	Description
Input Datagrams	The total number of UDP datagrams delivered to UDP users
No Receiver on Port	The total number of received UDP datagrams for which there was no application at the destination port
Input Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port
Output Datagrams	The total number of UDP datagrams sent from this entity

UDP Listener page

The UDP listener table contains information about this entity's UDP end-points on which a local application is currently accepting datagrams.

The screenshot shows the ASM Pro Web-based Manager (AWM) interface in a Microsoft Internet Explorer browser window. The page title is "10.41.146.51: MIB-II UDP Listener Table". The interface includes a navigation pane on the left with a tree view showing the following structure:

- System Information(Win2k Agent V4.30)
 - System Hardware
 - System
 - Interface
 - Address Table
 - IP Group
 - Generic
 - Address Table
 - Routing Table
 - Net To Media Table
 - ICMP
 - TCP
 - TCP Statistics
 - TCP Connection Table
 - UDP
 - UDP Statistics
 - UDP Listener Table**
 - SNMP

The main content area displays the "10.41.146.51: MIB-II UDP Listener Table" with a "Refresh" button. Below the title, it states "Number of Total Entries: 13". The table has two columns: "Local Address" and "Local port".

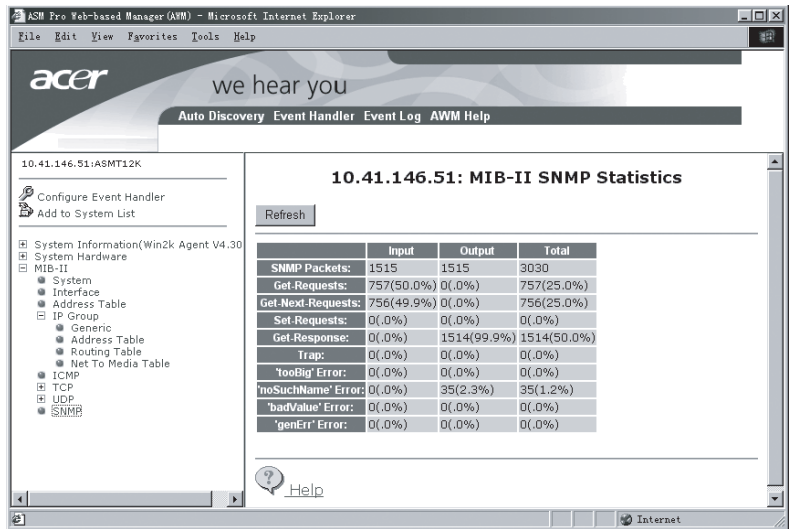
Local Address	Local port
0.0.0.0	135
0.0.0.0	161
0.0.0.0	445
0.0.0.0	1031
0.0.0.0	1034
0.0.0.0	1040
0.0.0.0	1060
0.0.0.0	3456
0.0.0.0	5002
0.0.0.0	9907
10.41.146.51	137
10.41.146.51	138
10.41.146.51	500

At the bottom of the page, there is a "Help" link with a question mark icon. The browser's status bar shows "Done" and "Internet".

Parameter	Description
Local Address	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used
Local Port	The local port number for this UDP listener

SNMP (Simple Network Management Protocol)

Implementation of the SNMP group is mandatory for all systems which support an SNMP protocol entity. Some of the objects defined below will be zero-valued in those SNMP implementations that are optimized to support only those functions specific to either a management agent or a management station. In particular, it should be observed that the objects below refer to the SNMP entity, and there may be several SNMP entities residing on a managed node (e.g., if the node is acting as a management station).



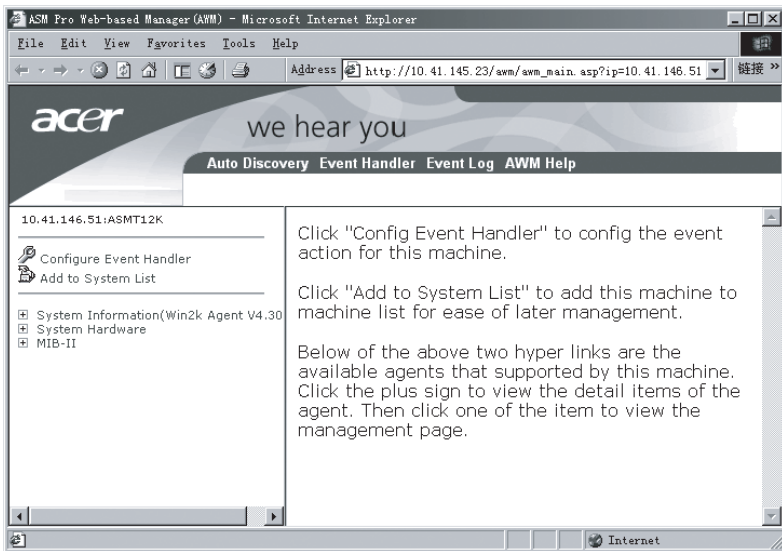
Parameter	Description
SNMP packets	The total number of Messages delivered to the SNMP entity from the transport service
Get-Requests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity
Get-Next-Requests	The total number of SNMP Get-Next-Request PDUs which have been accepted and processed by the SNMP protocol entity
Set-Requests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity
Get-Responses	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity
Traps	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity
'tooBig' Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'tooBig'
'noSuchNames' Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'noSuchName'
'badValues' Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'badValue'
'genErr' Errors	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'genErr'

► Configuring event handler

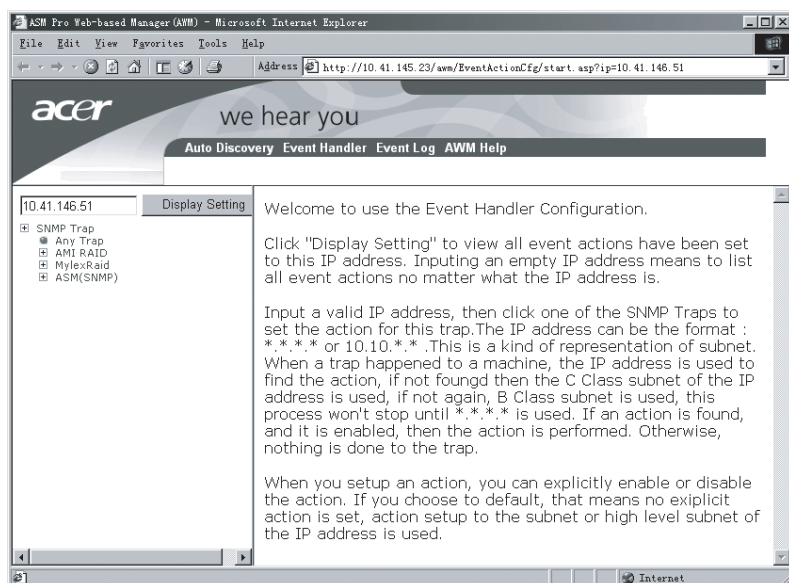
The event action configuration page helps you set what action to take when a specific system generates a specific event.

To set event actions:

1. In the main screen, click the **Configure Event Handler** link to access the Event Handler configuration page.



2. On the left frame, type the IP address of the device and then click on the SNMP traps that you want to set.



3. Click **Display setting** to display the current settings.
4. Enable or disable event actions as you like.

You can also do this:

1. In the main screen, type the device address in the device address textbox and then click the **Event Handler** link to access the Event Handler Configuration page.
2. Enable or disable event actions as you like.



Note: you can use wild cards (*) , when typing IP addresses. To do so, simply replace the byte number with an asterisk. For example, to look for all the IP addresses in the network type ".*.*.*". To look for IP addresses beginning with 172, then type "172.*.*" so on and so forth.

Event actions

ASM Pro Web-based Manager (AWM) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://10.41.145.23/asm/EventActionCfg/start.asp?ip=10.41.146.51

acer we hear you

Auto Discovery Event Handler Event Log AWM Help

10.41.146.51 Display Setting

SNMP Trap
Any Trap
AMI RAID
MylexRaid
ASM(SNMP)

Event Handler Setup For:
10.41.146.51 - Any Trap

Submit Refresh

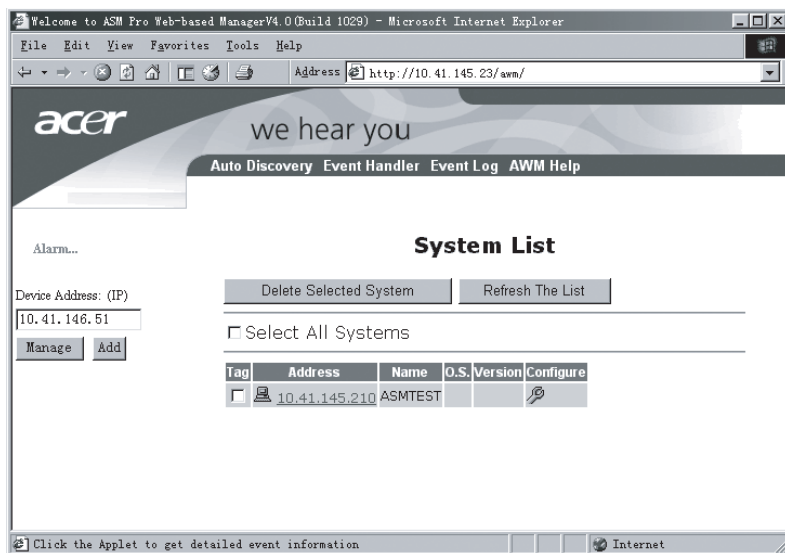
Browser Notify:
☐ Enable ☐ Disable ☒ Default

Send E-Mail:
☐ Enable ☐ Disable ☒ Default
SMTP Server: 263.net *
Mail From: webmaster@company.com *
Mail To: webmaster@company.com *
Subject: [AWM Event notification] *

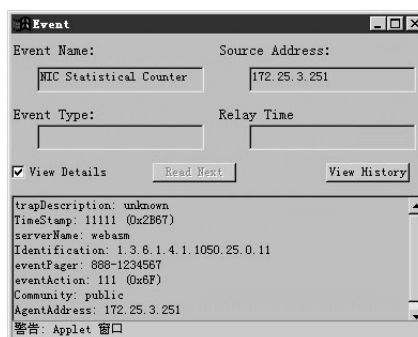
Call Pager:
☐ Enable ☐ Disable ☒ Default
Telephone Number: 88888888 *
Message Code: 1234# *

- Browser notify - notifies the administrator through the browser. Click the **Enable** radio to activate.
- Send E-Mail - sends an E-Mail to the administrator when an event occurs. Click the **Enable** radio button and fill out the form.
- Call Pager - sends a message through the administrator's pager when an event occurs. Click the **Enable** radio button and fill out the form.

► Real time monitoring

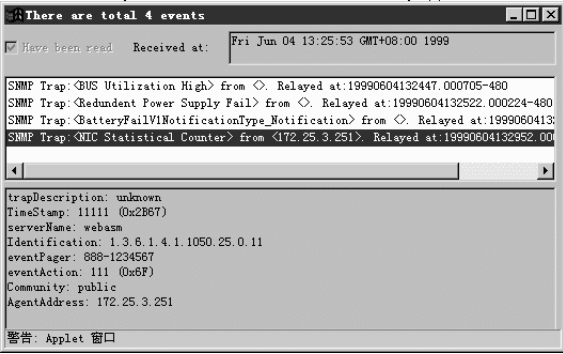


An icon flashes in the main page whenever a new event occurs. To view the detail event information, click on the flashing icon. The Real Time Event Monitoring window appears.



It includes information such as event name, event type, source address, and relay time. To view details, click the View Details checkbox.

To view the event history, click the **View History** button. The View History window displays.



A Troubleshooting

This chapter contains tables that describe some basic troubleshooting techniques you can use to work around specific problems in ASM Pro.

► General ASM Pro troubleshooting

The following table describes the error message for different functions in ASM Pro. It also provides a description of the error message and the action to take to correct the error.

Function	Message	Description	Action
Hardware Information/ Event log Information	Open file Fail	Fails to open a file to save event log	
Hardware Information/ Event log Information	Setting Event Threshold Failed	Fails to set a threshold	Make sure: 1. Agent allows remote setting configurations 2. Network connection is OK
Hardware Information/ Event log Information	Invalid threshold	Threshold is invalid	Don't set the threshold higher than 100
File System	Setting File System Threshold Failed		Make sure: 1. Agent allows remote setting configurations 2. Network connection is OK
Server Information/ Basic Information	Setting Manager Information Failed		Make sure: 1. Agent allows remote setting configurations 2. Network connection is OK

Function	Message	Description	Action
Server Information/ Basic Information	Setting Server Location Failed		Make sure: 1. Agent allows remote setting configurations 2. Network connection is OK
ASM Pro Console	Modem Initialization Failed		Set up the modem from the control panel.
Station	Com Port Initialization Failed	Fail to initialize Com port	
Station	Failed to initialize (COM1 to COM4)	Fail to initialize Com port	
Utility/CMOS Setup	Timeout. It waited too long to get the setup password from XXX		Check network connection
Utility/CMOS Setup	Socket Initialize failed		Check network connection
Utility/CMOS Setup	The client machine doesn't support to setup CMOS remotely		The setup password does not exist. Check BIOS version
Utility/CMOS Setup	Getting setup password error		Check network connection
Utility/CMOS Setup	The setup password is not correct		Input a correct password
Utility/CMOS Setup	Open WriteParams file error	Cannot open a file to write	Don't write parameters into a existed and read-only file
Utility/CMOS Setup	Failed to set password	Failed to set password	Check BIOS version

Function	Message	Description	Action
Utility/CMOS Setup	Cannot open the driver ADMCMOS.SYS	Cannot open the driver ADMCMOS.SYS	Check if Admcmos.sys is existent
Utility/CMOS Setup	Write CMOS data error	Cannot write CMOS data	Check BIOS version
Utility/CMOS Setup	Failed to open VxD file PROXY.VxD	Cannot open VxD file PROXY.VxD	Check if PROXY.VxD is existent
Utility/CMOS Setup	Failed to read VxD file PROXY.VxD	Cannot read VxD file PROXY.VxD	Check if PROXY.VxD is existent
Utility/CMOS Setup	Failed to write VxD file PROXY.VxD	Cannot write VxD file PROXY.VxD	Check if PROXY.VxD is existent
Utility/CMOS Setup	Get CMOS data error	Cannot get CMOS from target machine	Check BIOS version
Utility/CMOS Setup	Get BIOS version error	Cannot get CMOS version from target machine	Check BIOS version manually at target machine
Utility/CMOS Setup	Save CMOS data error	Cannot put CMOS data into target machine	Check BIOS version
Utility/CMOS Setup	Load ADMMISC.DLL Error	Cannot load admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Get GetSysProductNa me Address Error	Cannot get GetSysProductNa me Address from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Call GetSysProductNa me Error	Cannot call GetSysProductNa me from admmisc.dll	Check if admmisc.dll is existent

Function	Message	Description	Action
Utility/CMOS Setup	Get GetBiosVersion Address Error	Cannot get GetBiosVersion Address from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Save CMOS data error	Cannot put CMOS data into target machine	Check BIOS version
Utility/CMOS Setup	Load ADMMISC.DLL Error	Cannot load admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Get GetSysProductNa me Address Error	Cannot get GetSysProductNa me Address from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Call GetSysProductNa me Error	Cannot call GetSysProductNa me from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Get GetBiosVersion Address Error	Cannot get GetBiosVersion Address from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Timeout waits too long to get the CMOS data from XXX		Check network connection
Utility/CMOS Setup	Timeout waits too long to get the CMOS data from XXX		Check network connection
Utility/CMOS Setup	Timeout waits too long to save the CMOS data of XXX		Check network connection

Function	Message	Description	Action
Utility/CMOS Setup	Cannot find this machine :(IP address)		Check if this machine exists
Utility/CMOS Setup	The file format is not correct	The format of CMOS file is not correct.	Check if the CMOS file is correct.
Utility/CMOS Setup	The script file is not existed	Cannot find cmos.ver	Check if the file cmos.ver is existent.
Utility/Update CMOS	Fail to create socket	Cannot create socket to connect to target machine	Check network connection
Utility/Update BIOS	Winsock function error	Cannot send update BIOS job to target machine	Check network connection
Utility/Update BIOS	Invalid MAC address	MAC address is invalid	Check network connection
Utility/Update BIOS	Applied Model of package XX(XX) is not matched with machine XX(XX)	Package model does not match machine model	Check the Update BIOS package
Utility/Update BIOS	Start update service before job(s) can proceed	User can proceed to start update BIOS job	None
Utility/Update BIOS	The patch list file was not opened	Cannot find patch list file	Check if the patch list file is existed.
Utility/Update BIOS	Cannot open profile or sector XXX not found	Cannot open profile file or find sector XXX in profile file	Check the contents of the profile file.

Function	Message	Description	Action
Utility/Update BIOS	You should stop service first	When user applies the settings, if there is a service is running, it must be interrupted first.	Stop the service or give up the new settings
Utility/Update BIOS	Windows sockets initialization failed.	Cannot create socket to connect to target machine	Check network connection
Utility/Update BIOS	Cannot start BIOS update service	Starting Update BIOS service failed	Check network connection
Station	There is no response from Agent	Cannot set value to Agent	Make sure: Agent is still running Network connection

► ASM Pro agent for SCO OpenServer troubleshooting

ASMSMUXD

Message	Action
AgentAddr, out of memory	End unnecessary processes or reboot the system
Bad Inet address for param	Check /etc/snmpd.trap
Can't open /etc/mnttab	check /etc/mnttab
Can't open /etc/snmpd.trap	Verify file existence & permission
can't open /xsnmpd/portnum.dat	Verify file existence & permission
Can't read NIC	l1stat, verify NIC was found at boot
fail, gettimeofday	Check similar msg in /var/adm/syslog, try to resolve the problem according to the msg
AgentAddr, out of memory	End unnecessary processes or reboot the system
Bad Inet address for param	Check /etc/snmpd.trap
Can't open /etc/mnttab	check /etc/mnttab
Can't open /etc/snmpd.trap	Verify file existence & permission
Bad Inet address for param	Check /etc/snmpd.trap
Can't open /etc/mnttab	check /etc/mnttab
Can't open /etc/snmpd.trap	Verify file existence & permission
can't open /xsnmpd/portnum.dat	Verify file existence & permission
Can't read NIC	l1stat, verify NIC was found at boot

Message	Action
fail, gettimeofday	Check similar msg in /var/adm/syslog, try to resolve the problem according to the msg
fail, xselect	Try restart asmsmuxd or reboot
Fail to allocate	End unnecessary processes or reboot the system
Fail to malloc	End unnecessary processes or reboot the system
Fail to open /xsnmpd/asmsmuxd.cfg	Verify file existence & permission
Fail to open /xsnmpd/asmsmuxd.cfg	Verify file existence & permission
Fail to write /xsnmpd/asmsmuxd.cfg	Verify file existence & permission
Filesystem utilization exceeds threshold	“df -ik” check file system utilization percentage_clear unnecessary files
get_SCSI: cannot open /etc/conf/cf.d/mscsi	Verify SCSI card was found at boot, check SCSI card
get hardware information fail	Check /dev/asm, try reinstall
get system information fail	Check /dev/asm, try reinstall
gethostbyname fail	Verify system hostname can be found by DNS
gethostname fail to get hostname	Verify system hostname length not exceeding 32 characters
init_SMUX, out of memory	End unnecessary processes or reboot the system
malloc fail	End unnecessary processes or reboot the system
no SMUX entry for this SMUX daemon in 'peers' file	Check /etc/snmpd.peers
no syntax defined for object	Check ipmsmuxd.defs

Message	Action
open /dev/asm fail	Check whether /dev/asm installed or not
out of mem in NotifyManagers	End unnecessary processes or reboot the system
read kernel sym. fail.	Check /stand/unix & /dev/kmem
readobjects:	Verify file existence & permission
ps: /dev/kmem: cannot open	Check /dev/kmem
ps: /unix: cannot open	Check /stand/unix
ps: /unix: no namelist	Try rebuild kernel or boot with /stand/unix.old
ps: /unix: not the booted system	Try boot with /stand/unix or edit /etc/default/boot
ps: read error	Check these 2 files
ps: seek error	Check these 2 files
smux: fork	Try restart program or reboot
Unable to bind at *any* UDP port	Try restart asmsmuxd
Unknown type	Check SCSI card or try another card

ASMCONFIG

Message	Action
Can't open /etc/snmpd.trap	Verify file existence & permission
Fail to open /xsnmpd/asmsmuxd.cfg	Verify file existence & permission
Fail to write /xsnmpd/asmsmuxd.cfg	Verify file existence & permission

BPBSMUXD

Message	Action
/dev/gamdev open fail	Check /dev/gamdev installed or not
Cannot open /dev/gamdev, errno=	Check /dev/gamdev installed or no
fail, xselect	Try restart bpbsmuxd or reboot
Fail to open /xsnmpd/asmsmuxd.cfg	Verify file existence & permission
no SMUX entry for this SMUX daemon in 'peers' file	Check /etc/snmpd.peers

BPBCONFIG

Message	Action
/dev/gamedev open fail	Check whether /dev/gamedev installed or not
Backplane Board open fails	Check whether /dev/smb installed or not

IPMSMUXD

Message	Action
ERROR, ipmi.C, GetSDR(), BMCInterface() fail	Verify whether this machine supports IPMI, & IPMI is well-functioning
ERROR, ipmsmuxd, InitIPMI() fail	Verify whether this machine supports IPMI, & IPMI is well-functioning
ERROR, ipmsmuxd.c, main(), InitIPMI() fail	Check /dev/ipmidrv installed or not
ERROR, sig_alrm(), signal() fail	Try restart ipmsmuxd
ERROR, sig_PollIPMI(), signal() fail	Try restart ipmsmuxd
ERROR, trap.cpp, acer_trap(), smux_trap() fail	Verify snmpd is running, try resolve the problem according to the error msg
fail, xselect	Try restart ipmsmuxd or reboot
no SMUX entry for this SMUX daemon in 'peers' file	Check /etc/snmpd.peers
no syntax defined for object	Check ipmsmuxd.defs
smux: fork	Try restart program or reboot
smux_trap error	Verify snmpd is running, check similar msg in /var/adm/syslog

► ASM Pro Agent for SCO UnixWare troubleshooting

ASMSMUXD

Message	Description	Action
asmsmuxd: open (/dev/asmdrv) fail		Check whether /dev/asmdrv installed or not
enqueue: malloc		End unnecessary processes or reboot the system
ERROR: getsmuxEntrybyname		Check /etc/netmgt/snmpd.peers
ERROR: getutid(BOOT_TIME)		verify file existence & permission of /var/adm/utmp and wtmp
ERROR: readobjects		verify file existence & permission
ERROR: xselect		Try restart asmsmuxd or reboot
File System utilization exceeds threshold		"df -k" check file system utilization percentage, clear unnecessary files
fopen(/usr/asm/asmsmuxd.conf) fail		verify file existence & permission
get_irqDmaIoportMemTable:		verify directory existence & permission
make_daemon: fork fail		Try restart program or reboot
Memory utilization exceeds threshold	Memory utilization exceeds threshold	End unnecessary processes or reboot the system

Message	Description	Action
RRspPDU_failure	fail to register ASM Pro MIB module with the snmp agent	Try restart asmsmuxd & snmp daemon, or reboot
SMUX connection fail	fail to start smux connection	Try restart asmsmuxd & snmp daemon, or reboot
smux_register: no response received	fail to register ASM Pro MIB module with the snmp agent	Try restart asmsmuxd & snmp daemon, or reboot

ASMCFG

Message	Description	Action
ERROR: /usr/asm/asmsmuxd.conf not found	/usr/asm/asmsmuxd.conf not found	Verify file existence
make_daemon: fork fail	fork() fail	Try restart program or reboot
server: can't open event log file	fail to open /usr/asm/asmevent.log	verify file existence & permission

BPBSMUXD

Message	Description	Action
Ch# ID#, BPB# Tray#, Physical Disk Failure	Physical Disk Failure	Shutdown_check hark disks
ERROR: Launch program fail	fail to launch event handling program	Verify program existence & permission
fopen(/usr/bpb/bpbsmuxd.conf fail	fail to open /usr/bpb/bpbsmuxd.conf	Check file existence & permission
Going to Shutdown the server...	System is going down	Check previous broadcast message
make_daemon: fork fail	fork() fail	Try restart program or reboot
No other bpbsmuxd is found	No other bpbsmuxd is running	No action
open(/dev/gam) fail	fail to open /dev/gam	Check whether /dev/gam installed or not
thr_create(thr_bpb) fail	thr_create() fail	Try restart bpbsmuxd or reboot

IPMSMUXD

Message	Description	Action
ERROR, init_ipmi(), thr_create() fail	thr_create() fail	Try restart ipmsmuxd or reboot
ERROR, ipmi.C, GetSDR(), BMCInterface() fail!	InitIPMI() fail	verify whether this machine supports IPMI_ & IPMI is well-functioning
ERROR, sig_PollIPMI(), signal() fail	signal() fail	Try restart ipmsmuxd
make_daemon: fork fail	fork() fail	Try restart program or reboot
No ipmsmuxd is running	No other ipmsmuxd is running	No action
smux_trap:	smux_trap() fail	Verify snmpd is running, try resolve the problem according to the error msg
thr_create() fail	thr_create() fail	Try restart ipmsmuxd or reboot

XASMMON

Message	Description	Action
MrmFetchWidget() fail	MrmFetchWidget() fail	Try restart or reboot the system
MrmOpenHierarchy() fail	MrmOpenHierarchy() fail	Try restart or reboot the system

Message	Description	Action
MrmRegisterNames() fail	MrmRegisterNames() fail	Try restart or reboot the system
thr_create(hw_monitor) fail	thr_create() fail	Try restart or reboot the system

► ASM Pro Windows NT

troubleshooting

Function	Message	Description	Action
ASM Pro AGENT	Cannot Initialize NIC driver	NIC error	Reinstall NIC Adapter/driver
	Cannot create event for SnmpExtension Init	Snmp extended agent error	Reinstall SNMP
ASM Pro CONFIG UTILITY	Not a valid IP address or a host name	IP address or hostname format error	Use the correct format
	Start the SNMP service fail! Please manually restart the SNMP service	Cannot start SNMP by program	Start SNMP in the Control Panel
ASMCi	The Win32SL service is not running now	The service Win32SL is stopped	Start Win32SL in the Control Panel
	The mif file "ASMNT.MIF" cannot be installed into DMI Service Layer. Instrumentation code "ASMCi.EXE" will not be loaded	Win32SL service cannot load "ASMNT.MIF". ASMCi.EXE cannot be executed	Reinstall ASM Pro Agent and make sure Win32SL service is started
	Remote Console setup.iss could not be updated. Use default setup directory	Setup.iss file is missing or the file is write protected	Get the whole install package, or change the file property to Read/Write

Function	Message	Description	Action
	Remote Console setup failed. Remote Console is not installed	Setup.exe file is missing or crash	Get the whole install package
	This program requires VGA or better resolution	Resolution requires 640 x 480	Change the resolution setting
	Failed to detect HW type	HW is not supported	N/A
	Type comparison failed	HW is not supported	N/A
ASM Pro AGENT	Cannot Initialize NIC driver	NIC error	Reinstall NIC Adapter/driver
	Cannot create event for SnmpExtension Init	Snmp extended agent error	Reinstall SNMP
ASM Pro CONFIG UTILITY	Not a valid IP address or a host name	IP address or hostname format error	Use the correct format
	Start the SNMP service fail! Please manually restart the SNMP service	Cannot start SNMP by program	Start SNMP in the Control Panel
ASMCi	The Win32SL service is not running now	The service Win32SL is stopped	Start Win32SL in the Control Panel

Function	Message	Description	Action
	The mif file "ASMNT.MIF" cannot be installed into DMI Service Layer. Instrumentation code "ASMCi.EXE" will not be loaded	Win32SL service cannot load "ASMNT.MIF". ASMCi.EXE cannot be executed	Reinstall ASM Pro Agent and make sure Win32SL service is started
	Remote Console setup.iss could not be updated. Use default setup directory	Setup.iss file is missing or the file is write protected	Get the whole install package, or change the file property to Read/Write
	Remote Console setup failed. Remote Console is not installed	Setup.exe file is missing or crash	Get the whole install package
	This program requires VGA or better resolution	Resolution requires 640 x 480	Change the resolution setting
	Failed to detect HW type	HW is not supported	N/A
	Type comparison failed	HW is not supported	N/A
Asset Manager	Windows sockets initialization failed	ASM Pro console cannot initialize socket	Please reboot your console system

Function	Message	Description	Action
Asset Manager	Cannot find the asset log file.	ASM Pro agent cannot find the asset log file in server side.	Search "history.cfg" in your file system. If not, restart your server system and the asset log file will be generated again.
ASM Pro MIB Browser	No selected item	No selected query item	Select a query
ASM Pro MIB Browser	No Machine selected!	User didn't select any machine in query	Input machine name
ASM Pro MIB Browser	Please enter an integer between 1 and 60	User input invalid polling interval	Input valid polling interval
ASM Pro MIB Browser	Load Images Error	ASM Pro Browser load MIB data fail. The MIB database maybe corrupted	Initialize MIB database
ASM Pro MIB Browser	Can't view single item and table together	You want to view the single item and table together. It is not accepted in ASM Pro MIB Browser	User can choose single or table OIDs only
ASM Pro MIB Browser	Number of Table OID exceeds 128	User choose too many OIDs to view	Unselect some OIDs

Function	Message	Description	Action
ASM Pro MIB Browser	Only the single item will be added	When user add a whole subtree into select window. ASM Pro MIB Browser will add the single OIDs under this node	
ASM Pro MIB Browser	Can't delete this MIB file. The MIBs file are different.	When you want to remove a MIB-subtree by a MIB file. ASM Pro MIB Browser finds the OIDs defined in this sub-tree are different to the MIB file	Use the same MIB file.
ASM Pro MIB Browser	Can't open initial MIB file	ASM Pro MIB Browser cannot find the initial MIB file, origin.mib.	Search origin.mib and put it into the ASM Pro Console directory.
ASM Pro MIB Browser	Set Operation Fails!	User cannot set the OID value	Check if the OID is protected by password or not.
ASM Pro MIB Browser	Please leave Rotate Mode and Set Again	User cannot set the OID value in the rotated mode.	Please change to normal mode and set again.
ASM Pro MIB Browser	This OID is readonly	The access mode of this OID is read-only.	

Function	Message	Description	Action
ASM Pro MIF Browser	Cannot register XXX	ASM Pro MIF Browser cannot register to the service provider in a machine	Check if the service provider is ready in target system or the connection (network) is OK
ASM Pro MIF Browser	You reach the last row	When user access the the last row for a attributes table	
ASM Pro MIF Browser	Set Operation fails	The set operation for a attribute is failed	
ASM Pro MIF Browser	Can't view different tables together	You want to put attributes in different group to view	Select one group each time
ASM Pro MIF Browser	Can't view single item and table together	You want tp view the single and table attributes together	Select single or table only
Statistics Viewer	Different Recording Interval	You want to view two items whose polling intervals are different	Choose the items with same pooling intervals
Statistics Viewer	Statistics Operation Fails	The setup command is failed	Check if the password is correct if password is enabled
Statistics Viewer	Load Statistics Configuration Fails	Cannot load the statistic Configuration file	Check the agent side, find the statcfg.ini file

Function	Message	Description	Action
Statistics Viewer	Windows sockets initialization failed	ASM Pro console cannot initialize socket	Please reboot your console system
System Alert Manager	Can't use this service!	You want to use other service but it doesn't work. For example, DMI Alerts	Reboot the system or reinstall ASM Pro console again
System Alert Manager	Cannot connect to XXX	SAM cannot connect to the target system	Check if the target system is OK or the network is connected
System Alert Manager	You need to have a Mail Address to test this function	You want to set up a mail for event handling function. But no mail address	Input a mail address
System Alert Manager	Please check your Mail message to see if the Test Mail worked!!	After finish the test of mail setup, You must Check if the setting is OK	Check if the test mail is received
System Alert Manager	Invalid Phone Number	You want to set up a pager for event handling function. But the phone number is invalid	Input a valid phone number

Function	Message	Description	Action
System Alert Manager	You need to have a phone number to test this function	You want to set up a pager for event handling function. But no phone number	Input a valid phone number
System Alert Manager	Please check your pager to see if the dialing worked!!	After finish the test of pager setup, You must check the setting is OK	Check the pager

Hardware common part troubleshooting

Function	Message	Description	Action
ASM Pro AGENT	CPU/Housing Fan stopped	Fan stops	Replace fan
	CPU/On Board temperature exceeds threshold	Temperature is going high	Cool down or power off server
	CPU/SYSTEM: voltage sensor is out of range	Voltage is abnormal	Check Power Supply model or contact your H/W vendor
	Redundant Power supply unit failed	Redundant Power supply unit is abnormal	Check if it is power-off or unplugged. Or replacing a new one
	Redundant Power supply fan failed	Redundant Power supply fan stops	Check if it is power-off or unplugged. Or replace a new one
	Power supply failed	UPS is abnormal	Check if it is power-off or unplugged. Or replace a new one
	Power supply fan failed	UPS fan stops	Check if it is power-off or unplugged. Or replace a new one
	AC power failed	AC power is abnormal	Replace a new one
	AC power failed. Shutdown server in 1 minute	AC power is abnormal. Server will be shutdown	Replace a new one

Function	Message	Description	Action
	UPS battery failed	UPS battery is abnormal	Check battery or replace a new one
	Fuse failed	Fuse is bad	Replace the fuse or contact your H/W vendor
	ECC error	DIMM error	Replace the DIMM or contact your H/W vendor

B RAID utilities

The Redundant Array of Inexpensive Disks (RAID) combines small, inexpensive disk drives into an array of disk drives which yields performance exceeding that of a Single Large Expensive Drive (SLED). The array of drives appears to the computer as a single logical storage unit or drive. These utilities monitor the RAID Controller information and functions. The following sections give a brief description of the utilities.

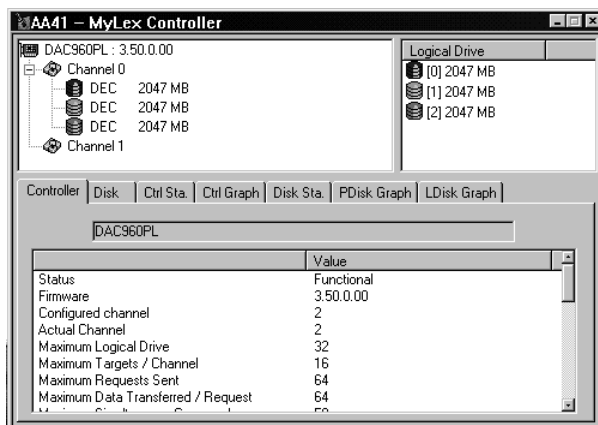
► ASM Pro Mylex RAID utility

Mylex RAID controller monitor

This window is used to monitor Mylex RAID Controller Information. The upper left window displays the hierarchical view of the controller structure, and the upper right window shows logical drive information.

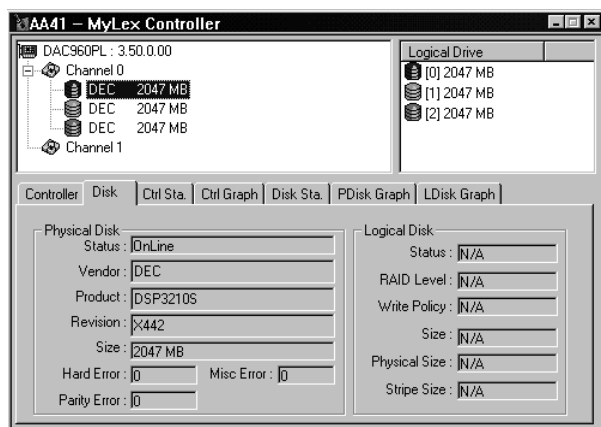
Controller tab

Click the **Controller** tab to monitor Mylex RAID Controller Information. Click on a controller to show controller information.



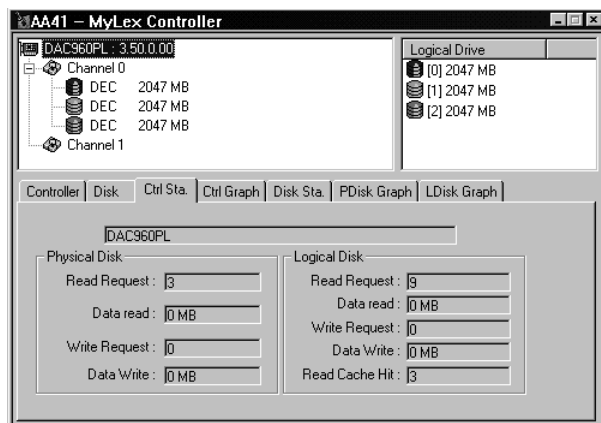
Disk tab

Click the **Disk** tab to monitor Mylex RAID Controller disk information. Highlight a hard disk to show physical disk information.



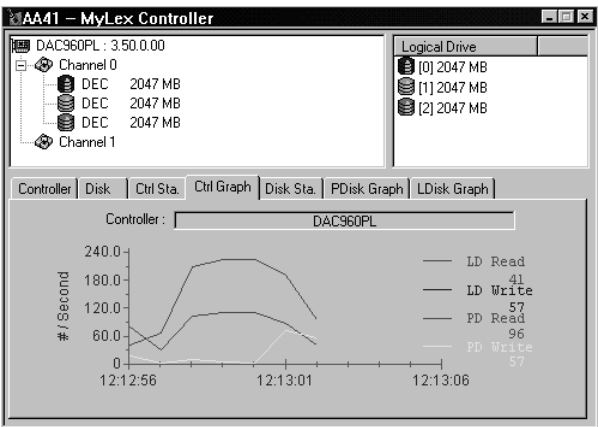
Controller statistic tab

Click the **Controller Statistic** tab to monitor Mylex RAID Controller statistics information.

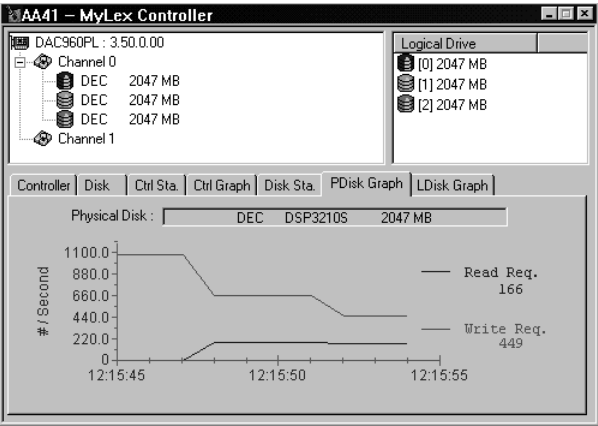


Disk statistic tab

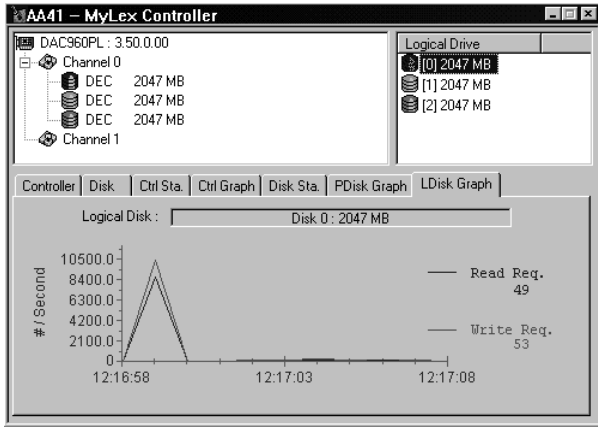
This window is used to monitor Mylex RAID Controller disk statistic information. Under this tab, the displayed information is as shown below:



Physical disk statistic graph tab



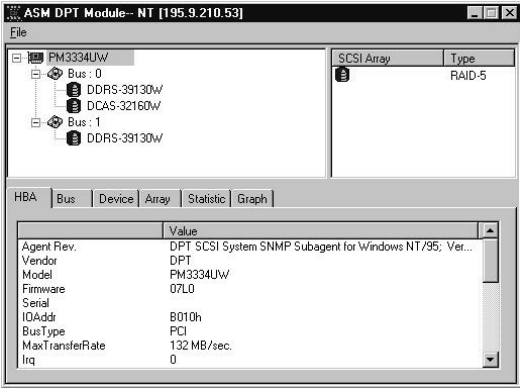
Logical disk statistic graph tab



▶ ASM Pro DPT RAID utility

This utility monitors the DPT RAID Controller information and functions. The window shown below is the main screen of the DPT RAID Controller. The upper left window displays the hierarchical view of the controller structure, and the upper right window shows the logical drive information.

HBA (Host Bus Adapter) tab

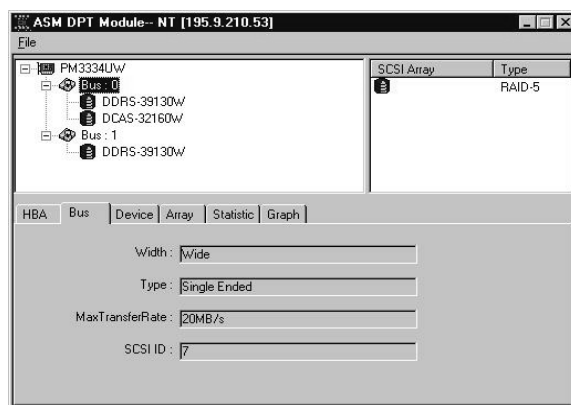


Item	Description
Agent Revision	DPT SCSI system SNMP agent revision information
Vendor	Name of the HBA vendor
Model	HBA controller model description
Firmware	HBA controller firmware version
Serial Number	HBA controller serial number
IO Address	HBA controller I/O Address (normally displayed in hex). It is a 16-bit value for ISA and EISA, and 32-bit value for PCI devices

Item	Description
Bus Type	Host bus type of the computer system to which the HBA is attached to
Max Transfer Rate	Maximum possible transfer rate in MB/seconds
IRQ	HBA controller interrupt level
IRQ Type	HBA controller interrupt type
DMA	HBA controller DMA channel. Only applicable if an ISA HBA
RAID Module	HBA Disk Array Module. With the addition of the DM4000 Disk Array Module and a caching module, HBAs can configure hard drives into RAID-0, RAID-1 and RAID-5 arrays, providing disk-fault tolerance and throughput many times those of non-arrayed disk drives
Cache Module	HBA controller caching module
Audio	Setting the value of this object to on causes an audible alarm to start beeping. Setting the value of this object to off causes the audible alarm to stop beeping
Up Time	Time elapsed (in hundredths of a second) since the HBA last booted
ECC Enabled	Shows if the ECC is enabled on the HBA. This object can set ECC to enabled or disabled
Max ReadAhead Rate	Maximum percentage of read-ahead pages brought into the HBA cache
Max DirtyPages Rate	Maximum percentage of dirty pages in the HBA cache
Write Back Delay	Write-back delay in milliseconds

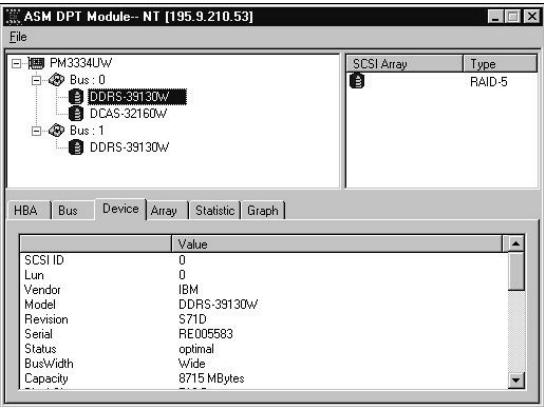
Item	Description
Temperature	Temperature as seen on the HBA
Voltage	Voltage as seen on the HBA
Bad Memory Address	The value of this object is the last faulty HBA RAM address as determined by the ECC algorithm used by the HBA

Bus tab



Item	Description
Width	SCSI Bus width
Type	SCSI Bus transceiver type
Max Transfer Rate	SCSI Bus maximum possible transfer rate in MB/s. Valid values can be 4, 5, 8, 10, 20, 40, 100, etc. depending on the SCSI technology used
SCSI ID	SCSI ID of HBA on this SCSI Bus

Device tab

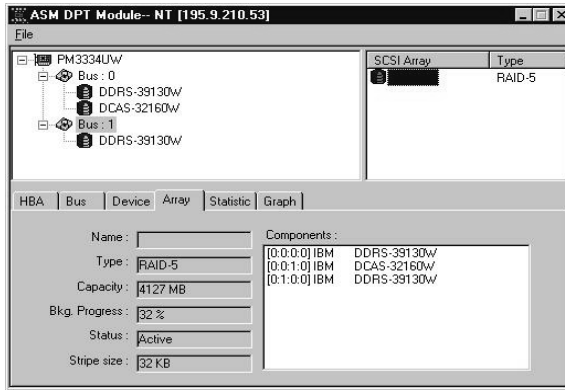


Item	Description
SCSI ID	SCSI ID for the device
LUN	SCSI Logical Unit Number (LUN) for the device
Vendor	Vendor name of the device
Model	Model name of the device
Revision	Device revision level
Serial Number	Device serial number
Status	Administrative state of the device
Bus Width	Value of this object indicates the data width of the SCSI device
Capacity	Storage capacity of the device in MBytes
Block Size	Device block size in Bytes
Max Transfer Rate	Maximum data transfer rate for the device

Item	Description
Removable	Value of this object indicates if the device is removable or not
ECC Enable	Value of this object indicates if the device has ECC enabled or disabled
SCSI Version	Value of this object indicates the SCSI specification version supported by the device
Soft Reset	Value of this object indicates if the SCSI device is soft reset capable or not
Cmd Queuing	Value of this object indicates if the SCSI device is command queuing capable or not
Linked Cmds	Value of this object indicates if the SCSI device is linked commands capable or not
Synchronous	Value of this object indicates if the SCSI device is synchronous or not
Relative Address	Value of this object indicates if the SCSI device supports relative addressing or not
SMART	Value of this object indicates if the SCSI device supports SMART specifications
SCAM	Value of this object indicates if the SCSI device supports SCAM specifications
Fast20	Value of this object indicates if the SCSI device supports Fast20 specifications
Bad Block Number	Value of this object represents the last bad block encountered on this device. It is needed in the definition of one or more traps. Value 0 means there is no error, and note that the first block starts from 1 (not zero)

Item	Description
Bad Block Count	Value of this object represents the count of the bad blocks starting at Bad Block Number encountered last time on this device. It is needed in the definition of one or more traps
Errors Above Threshold	This object indicates if the error count of this device has reached the threshold or not
Drive Locking On	This object indicates if the drive is locked or not
Last Req Sense Info	The value of this object is the request sense information and is primarily used in the definition of one or more traps
Hot Spare	This object indicates if the drive is a hot-spare or not

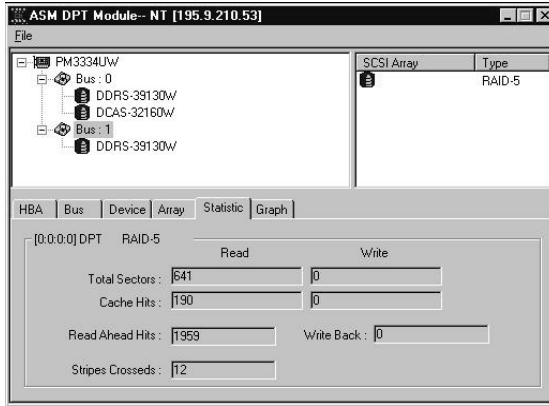
Array tab



Item	Description
Type	RAID Array Group type
Name	Name of the RAID Array Group

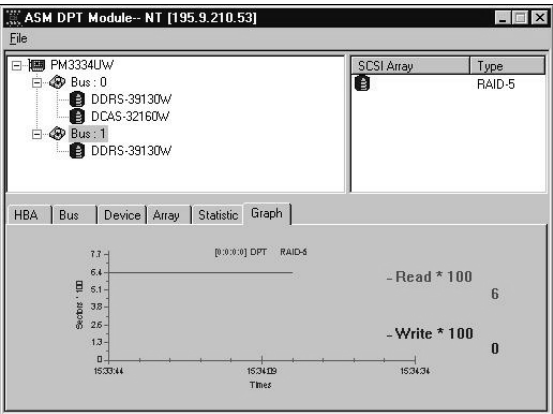
Item	Description
Capacity	Capacity of the RAID Array Group
Background Progress	The value of this object returns the percentage complete status of the outstanding background operations on this Array Group. This includes initial Build, Rebuild, Verify and VerifyFix operations. If there is no background operation, the value of this object shall be 100. The value of this object will always be 100 for non-redundant array (RAID-0)
Status	Invalid(1), 'active'(2), which indicates that the conceptual row is available for use by the managed device; 'notInService'(3), which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device; 'notReady'(4), which indicates that the conceptual row exists in the agent, but is missing information necessary in order to be available for use by the managed device; 'createAndGo'(5), which is supplied by a management station wishing to create a new instance of a conceptual row and to have it available for use by the managed device; 'createAndWait'(6), which is supplied by a management station wishing to create a new instance of a conceptual row but not to have it available for use by the managed device; and, 'destroy'(7), which is supplied by a management station wishing to delete all of the instances associated with an existing conceptual row
Stripe Size	Stripe size used on the array in KBytes. A stripe is a contiguous region of disk space. RAID distributes data evenly across component drives in an array by concatenating interleaved stripes from each drive

Statistic tab



Item	Description
Read/Total Sectors	Total number of sectors read from the device
Read/Cache Hits	Total number of data accesses in which the requested data was found in the cache
Read Ahead Hits	Total number of data accesses in which the requested data was found in the read ahead buffer
Write/Total Sectors	Total number of sectors written to the device
Write/Cache Hits	Total number of data writes to the device in which the data was written to the cache and not to the disk
Write Backs	Total number of data writes to the device in which the data was written from the cache to the disk at a time when the device would otherwise be idle
Stripes Crossed	Total number of Array Group accesses which cross stripe boundaries. Only applicable for array devices; otherwise, zero is returned

Graph tab



Item	Description
Read/Total Sectors	Total number of sectors read from the device
Write/Total Sectors	Total number of sectors written to the device

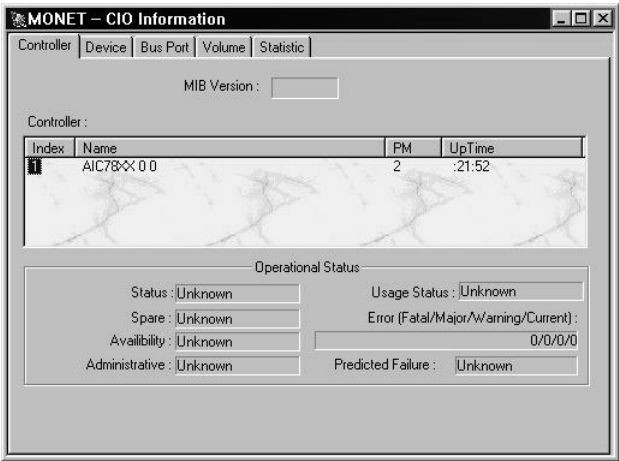
C ASM Pro
Adaptec CI/O
utility

Adaptec CI/O Array Management software is the interface to all Adaptec array solutions, simplifying array management and providing seamless scalability through a built-in upgrade path.

With Adaptec's CI/O Array Management software, network managers can monitor and manage storage either locally or remotely from any PC or workstation on the network. The management software allows network managers to see at-a-glance both physical and logical array configurations and other SCSI peripherals for any server using Adaptec array adapters and controllers.

This utility monitors status about storage devices and relative information of Adaptec controller. The sections below give a brief description of the utility.

► Adaptec CI/O monitor window



The upper left window displays the hierarchical view of the controller structure, and the upper right window shows is the logical drive information.

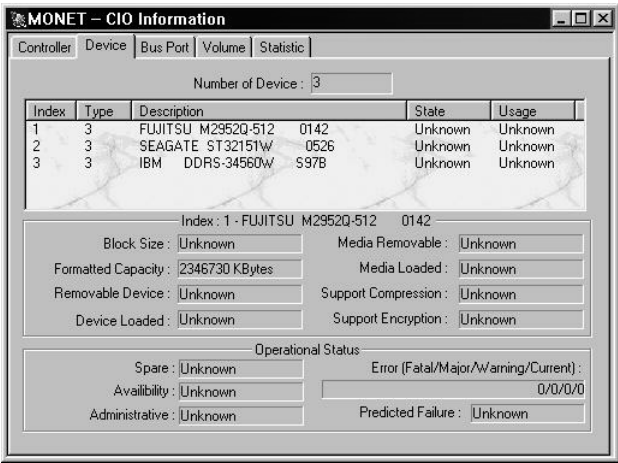
Controller tab

This window is used to monitor the Adaptec CI/O Controller Information. The information displayed is shown below:

Item	Description
MIB Version	The revision number of the CIO SNMP agent
Controller	
Index	A unique index for each storage controller
Name	Name, brand, and hardware revision level of the storage controller

Item	Description
Protection Management	Indicates whether or not the controller provides redundancy or protection against device failures
Up Time	The number of seconds that have passed since this controller was last powered on
Operational Status	
Spare	For objects which reference this operational state and which are sparing some other object this attribute describes sparing status
Availability	The availability of the object
Administrative	The administrative state of the object
Usage	The usage state of the object
Error Count Fatal,	The accumulated Fatal or Non-recoverable error count for the object
Major,	The accumulated Major or Critical error count for the object
Warning,	The accumulated Warning or Non-critical error count for the object
Current	This attribute presents the current error status for the object. The most critical error status in effect should be presented
Predicted Failure	Enumeration describing the current Device Predicted Failure Status (e.g. the S.M.A.R.T. status of the object)

Device tab

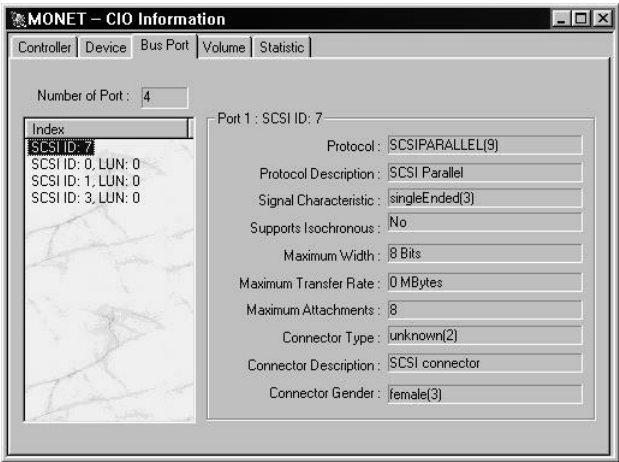


This window is used to monitor the Adaptec CI/O Device Information. Under this tab the displayed information is as shown below:

Item	Description
Number of Device	The Total number of storage devices
Index	A unique index value for each storage device beginning with 1
Type	The type of this mass storage device
Description	A longer description of the storage device
State	The operational status of the object
Usage	The usage state of the object

Item	Description
Device Status	
Block Size	The size in bytes of the data blocks used on the storage media. If the media block size is unknown or inconsistent then this value shall be zero
Formatted Media Capacity	The total size in kilobytes of this storage media after it has been formatted
Removable Device	If true, then this storage device is removable (e.g. PCMCIA device)
Device Loaded	If true, then the storage device is loaded
Removable Media	If true, then the media in this storage device
Media Loaded	If true, the media in this storage device is loaded
Support Compression	If true, the storage device supports compression
Support Encryption	If true, the storage device supports encryption

Bus port tab

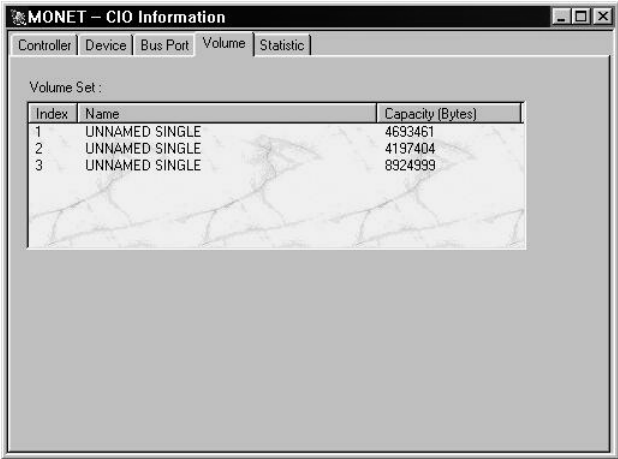


This window is used to monitor the Adaptec CI/O Controller Device information. Under this tab, the displayed information is as shown below:

Item	Description
Number of Port	Total number of ports
Port Information	
Protocol	The protocol describing the electrical characteristics of the Bus Port. If 'Other' is used, then the Protocol Description attribute shall be used
Protocol Description	Additional description of the protocol describe above
Signal Characteristics	The electrical characteristics of the Bus Port being described
Support Isochronous	Indicates whether or not the bus port supports isochronous transfers
Maximum Width	The maximum width, in bits, of this Bus Port's data path. A value of 1 should be used for serial

Item	Description
Maximum Transfer Rate	The theoretical maximum transfer rate, in millions of bytes per second, that this Bus Port is capable of achieving under ideal conditions. A value of zero should be used if the transfer rate is less than 1 million bytes per second
Maximum Attachments	The maximum number of directly addressable entities supported by this bus port's protocol
Connector Type	Describes how options (cards, devices, etc.) physically connect to this port bus. If 'Other' is used, then the connector type description attribute shall be used
Connector Description	Additional description of the connector described above
Connector Gender	Indicates the gender of the connector described above

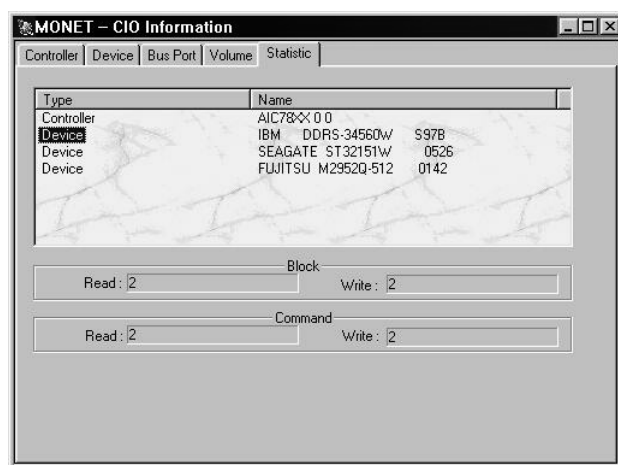
Volume tab



This window is used to monitor the Adaptec CI/O Volume information. Under this tab, the displayed information is as shown below:

Item	Description
Index	A unique index value for each volume set beginning with 1
Name	The name of the volume set
Capacity	The total size in bytes of the user data space of this volume set

Statistic tab



This window is used to monitor the Adaptec CIO Statistic information. Under this tab, the displayed information is as shown below:

Item	Description
Blocks Read	The number of 512 byte blocks read from the object
Blocks Written	The number of 512 byte blocks written to the object
Read Commands	The number of read commands issued for the object
Write Commands	The number of write commands issued for the object

D Management system
snap-in modules

This appendix describes how to install and use various Snap-in modules with the management system.

► CA Unicenter TNG



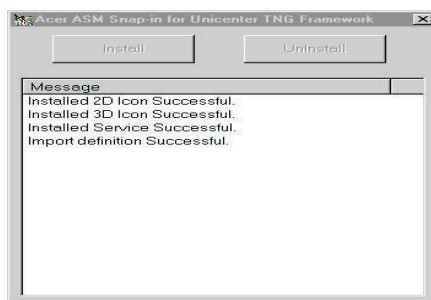
Note: Before installing the snap-in module, make sure that the CA Unicenter TNG Framework and ASM Pro Console have been installed.

To install the snap-in module, run Setup.exe from the installation CD under the directory \Console\CA\ to install/uninstall the ASM Pro snap-in module.

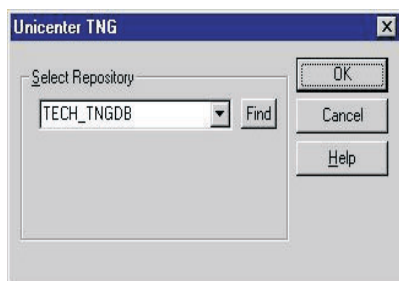
This module creates classes and objects in the repository of Unicenter TNG. The ASM Pro Agent object is created automatically when a new host is added into the repository (manually added or by auto discovery).

To launch ASM Pro Console from Unicenter WorldView:

1. Find the node you want to monitor.
2. Double-click the node's icon.



3. Right-click the ASM Pro Agent's icon and launch ASM Pro Console from the context menu.



If ASM Pro Agent is previously installed, an ASM Pro Agent's icon will appear.

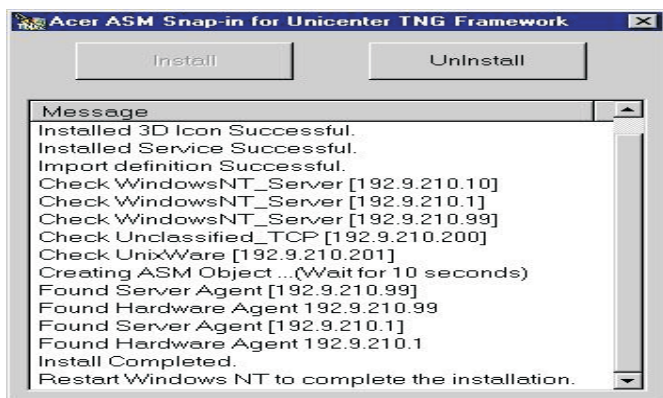
▶ HP OpenView



Note: Before installing the snap-in module, make sure that the HP OpenView Network Node Manager and ASM Pro Console have been installed.

To install the snap-in module, run Setup.exe from the installation CD under the directory \Console\OpenView\.

Launch HP OpenView Management Console and select the "Misc\ASM Pro\ADM Snap in:ASMMon" menu item to auto-discover ASM Pro machines. Select one ASM Pro machine and then click on the **Tools > ASM Pro** menu. The ASM Pro Console launches.



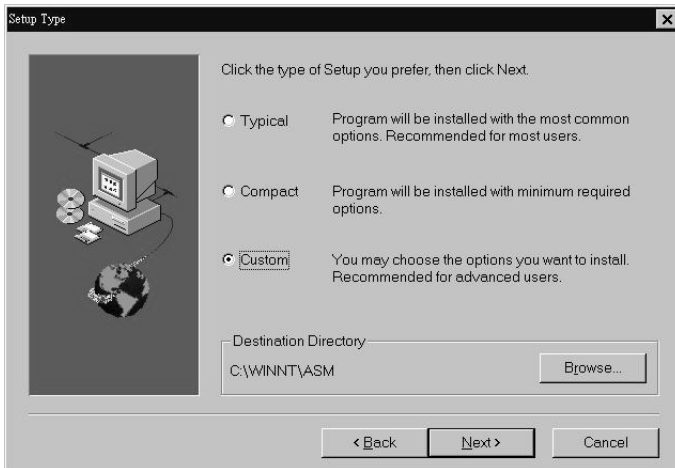
► MMC (Microsoft Management Console)

The MMC snap-in module is included in the ASM Pro Server Agent installation when installed in Windows NT servers.

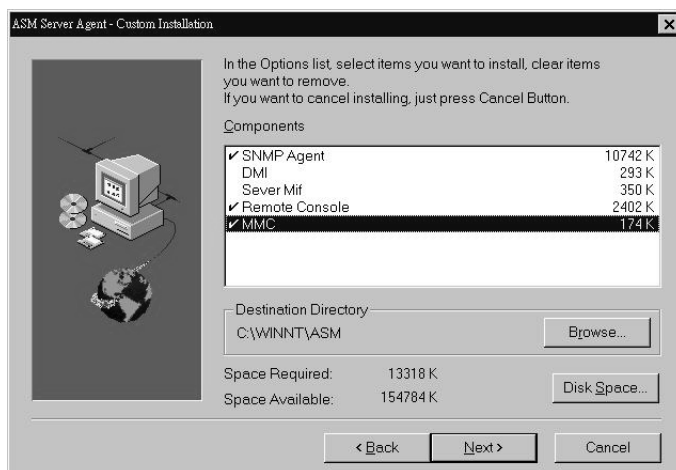
Follow the setup wizard during installation and click the **Next** button to go to the next page. You can also click the **Back** button to go back to the previous screen. Choose **MMC** when prompted to install snap-in components. A check indicates that the snap-in component will be installed into your machine.

To install and run the MMC:

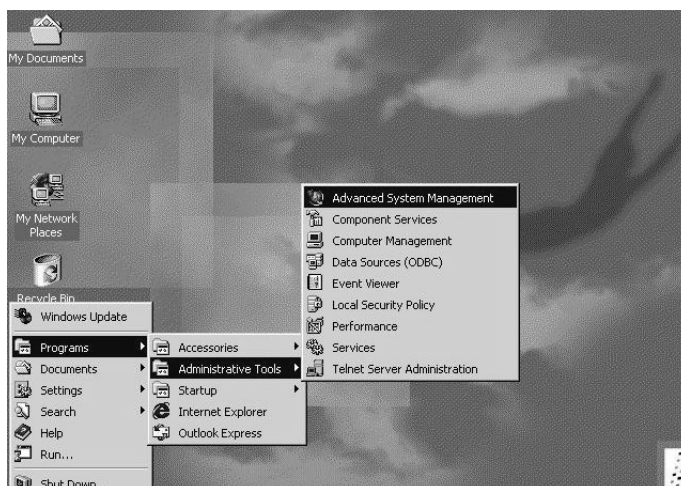
1. Choose **Custom** setup and then click **Next**.



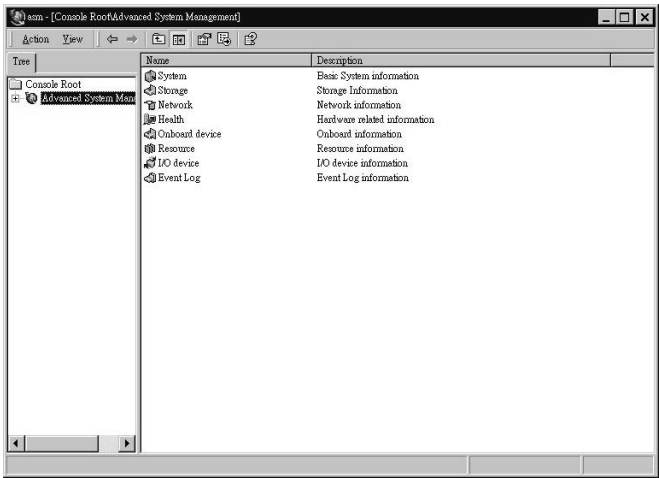
2. Click **MMC** and then click **Next**.



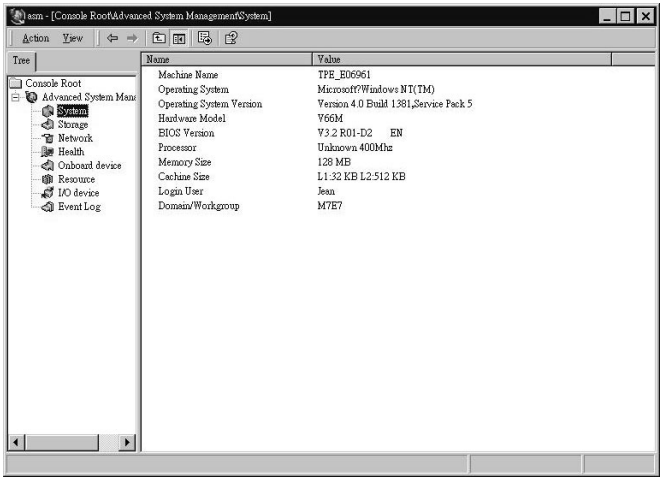
3. To run MMC, click the **Start** button in Windows NT and then choose **Programs, Administrative Tools**, and then **Advanced System Management**.



- 4. The MMC main screen appears.



- 5. Click the plus (+) sign besides Advanced System Manager to expand a list of viewable system information.



For more information about the MMC, please refer to its online help.

Index

A

- Advanced Desktop Agent
 - System Requirements 12
- Advanced Server Agent
 - System Requirements 12
- Advanced System Manager (ASM) 2
 - Add-on and Snap-in 11
 - Features 10
 - System Requirements 12
- Alert via LAN 140
- Alert via LAN Types 141
- API 3
- ASM Console
 - installation 13
 - password 51
 - What is... 9
- ASM Console User Interface 53
 - menu bar and toolbar 53
- ASM Desktop Agent
 - Basic System Information 195
 - CPU, Memory, and Onboard Chips 205
 - I/O Device Information 208
 - LAN Adapter, TCP/IP and Modem setting 198
 - Physical and Partition Information 196
 - Resource 207
 - System Health Status 203
 - System Performance Information 200
- ASM MIB Browser 10
- ASM MIF Browser 10
- ASM Server Agent
 - configuring SCO Openserver Agent 16
 - installing Microsoft Windows NT Agent 18
 - installing Novell Netware Agent 14
 - installing SCO Openserver Agent 15
 - installing SCO Unixware Agent 16
 - What is... 9
- asmcfg for NetWare 175
 - Event Handling 178
 - Manager Information 177
 - OOB 177
 - password 175
 - saving changes 181
 - Server Location 178
 - Trap Target 179

- uninstallation 182
- asmcfig for SCO UnixWare
 - Config>ASM_Password 166
 - Config>Event_Actions 168
 - Config>Manager_Info 167
 - Config>SNMP 165
 - Config>Threshold 167
- asmcfig for Windows NT 169
 - Event Action 171
 - Event Log 172
 - Manager Information 170
 - password 172
 - saving changes 173
 - Server Information 170
 - SNMP Config 169
- asmconfig for SCO OpenServer 158, 183
 - Event log 162, 188
 - Manager Information 159, 184
 - password 161, 186
 - quitting 163, 189
 - SNMP Config 158, 183
 - Threshold 161, 187
 - View Event Log 162, 188
- Asset Manager 10
- AVL Alert Types 141

C

- Configuration Information 10

D

- displaying Single Event log information 144
- DMI 4
 - definition 3

E

- event 160, 185
- Event Action 160, 185
 - handling 160, 185
 - trapping 160, 185
- Event Handler Setup 148
 - Console Action 150
 - Event Handling Method 149
- Event log file 143
 - loading 143
 - saving 143
- Event types 144
- Event Viewer 143

F

Fault Management 10, 125
 Hardware Errors 127

H

Hardware Status 100
 Health Monitor 100

L

log file
 setting 232

M

MIB 3

MIB Browser

- adding new MIB file 228
- adding OID 229
- Auto Discovery 221, 315, 323
- browsing OIDs 229
- browsing options 223
- browsing systems 221, 315, 323
- configuring community and port 224
- defining new query 225
- definition 3
- manageing MIB database 226
- menu bar and toolbar 214
- removing MIB file 229
- removing OID 229
- running 213
- selecting query 226
- SNMP Table 229
- user interface 214

MIB file

- adding 228
- removing 229

MIB-II Configuration Information 107

- ICMP 115, 437
- Internet Control Message Protocol 115, 437
- Internet Protocol 112, 434
- IP 112, 434
- Simple Network Management Protocol 121
- SNMP 121
- System 107
- TCP 117, 439
- Transmission Control Protocol 117, 439
- UDP 120, 442
- User Datagram Protocol 120, 442

Microsoft Windows NT

- installation 18

MIF 3
MIF Browser
 running 239
 what is... 3, 239

N

Network 2
Novell Netware Agent
 installation 14

O

OID
 adding 229
 enumeration display 232
 finding 235
 finding in SNMP Table 233
 recording polling information 233
 removing 229
 set operation 231
 walking 233

P

password
 ASM Console 51
Performance Monitoring 10, 92
 Changing Polling Interval 92
 Disk Utilization 96
 File System Utilization 98
 Memory Utilization 94
 NIC Utilization 98
 Processor Performance 92
polling
 setting time interval 233
protocol
 DMI 3
protocols
 SNMP 3

R

retrieving Multiple Event log information 143

S

SCO Openserver Agent
 configuring for ASM Server Agent 16
 installation 15
SCO Unixware Agent
 installation 16
SNMP
 definition 3

- SNMP Table 230
 - browsing 229
 - finding OID 233
 - rotating 233
 - saving 236
- Statistic Viewer 10
- System Alert log files 142
 - loading 142
 - saving 142
- System Alert Manager 3
- System Alert Manager (SAM) 10
- System Alert Types
 - DMI Indication Types 140
 - DMI Indications 138
- System Alert types 135
- System Information 10, 70
 - Basic Information 70
 - DMI BIOS Information 72
 - I/O Device Information 78
 - Storage Information 79, 417
- System Informaton
 - System Resource Information 88
- System Lisitng
 - customizing 68
- System Listing
 - adding a subnet 62
 - Auto Discovery 60
 - Manually adding a system 64
 - Removing a system 64
 - specifying options 63
 - symbols 67
 - System organizer 67
 - User interface 65

T

- Trap Types 135

