

Advanced System Manager Pro
(ASM Pro) version 4.3
User's guide

Copyright © 2000 Acer Incorporated
All Rights Reserved.

Advanced System Manager Pro
(ASM Pro) version 4.3

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	1
Features	3
1 Getting started	7
Welcome	9
Features	10
System requirements	12
ASM Console	12
ASM Server and Desktop agents	12
System setup	13
Installing ASM Console	13
Installing ASM Server Agent	13
Installing the Novell NetWare Server Agent	13
Installing the SCO OpenServer Agent	15
Installing the SCO UnixWare Server Agent	17
Installing the Microsoft Windows NT Server Agent	18
2 Quick tour	21
ASM 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 Console	49
Launching ASM Console	51
Initializing and changing the password	51
ASM 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

Contents

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
BIOS event log	107
MIB-II information	108
System	108
Interface	109
AT (Address Translation)	113
IP (Internet Protocol)	113
ICMP (Internet Control Message Protocol)	116
TCP (Transmission Control Protocol)	118
UDP (User Datagram Protocol)	121
SNMP (Simple Network Management Protocol)	122
Redundant power supply	125
Uninterruptible Power Supply (UPS)	125

UPS information	126
Fault management	128
Threshold settings	128
Hardware errors	129
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 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_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 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 Local Console	193
Basic system information	195
Physical and partition information	196
Accessing physical storage device information	196
Accessing partition information	197
LAN adapter, TCP/IP, and modem setting	199
LAN (Local Area Network)	199
TCP/IP (Transmission Control Protocol/ Internet Protocol)	200
Modem	200
System performance information	201
CPU utilization	201
Virtual memory manager	202
Swap file	202
File system	202
System health status	204
Fan	204
Temperature	204
Voltage	205
CPU, memory, and onboard chips	206

Processor	206
Memory	207
Onboard device	207
System resource	208
I/O device information	209
7 ASM MIB Browser	211
Installing ASM 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 MIF	
Browser	237
Installing ASM 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 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
RDM agent	334
RDM station	334
RDM connectivity	334
RDM features	334
Remote management features	335
RDM station features	335
RDM installation	336
System requirements	336
RDM server requirements	336
RDM Station requirements	336
RDM server setup	337
Installing RDM module	337
Connecting communication peripherals	339
Installing RDM agent software	340
RDM station setup	342
Installing the RDM station software	342
Uninstalling the RDM station software	343
Configuring the RDM server	344
RDM operation modes	344
RDM local mode	344
RDM remote mode	344
RDM runtime mode	344
RDM BIOS	345
Entering the RDM BIOS	345
RDM 4.3 BIOS version	346
Console redirection	346
Hidden partition	346
Communication protocol	347
COM port baud rate	347
Remote Console phone number	347

Dial out retry times	348
Modem initial command	348
RDM work mode	348
Waiting mode password	349
Paging	349
System critical paging numbers	350
Paging times	350
Setting RDM operation modes	351
RDM local mode	351
RDM remote mode	351
RDM runtime mode	353
Using the RDM station	357
Running the RDM station	357
Starting the RDM station	357
Connecting to the RDM server	357
EMP (emergency management port) console	358
EMP console buttons	359
EMP console functions	361
RDM reboot options	362
RDM station options	364
RDM station utility	364
RDM station utility menus	365
RDM station toolbar buttons	367
RDM station functions	368
Viewing a snapshot file	368
Clearing the screen	369
Saving a log file	369
Disabling the saving log file function	370
Configuring RDM station settings	370
Setting the font properties	371
Creating a new RDM agent	372
Sending files	374
Receiving files	376
Refreshing the screen	377
Rebooting the server	377
SCO OpenServer, UnixWare and	
Internet FastStart Installation	379
SCO OpenServer 5	379
SCO UnixWare	379
SCO Internet FastStart	380
Troubleshooting	382
RDM agent troubleshooting	382
RDM station manager troubleshooting	382
Modem troubleshooting	383

Hidden partition troubleshooting	383
BIOS messages	383
15 Advanced Web-based Manager	385
Installing AWM and Microsoft IIS	387
System requirements	387
Installing AWM	387
Setting up Microsoft IIS	387
Running AWM	389
AWM user interface	390
Network topology	393
Using Auto Discovery to add a network device to the Dynamic Network View	393
Changing device properties	394
Adding a device	395
Removing a device	396
Managing network devices	397
Managing devices using the Network Topology	397
Managing devices using the Manage Device Form	398
Dynamic graphing	399
Management pages	400
ASM Management Pages	400
Basic System Information	400
Operating system	401
Hardware environment	403
DMI BIOS Information	404
I/O peripheral information	408
Network information	408
System resource information	409
Storage information	411
Utilization	413
Polling interval	413
Processor utilization	413
PCI bus utilization	414
Memory utilization	416
Storage utilization	417
MIB-II configuration information	417
System information	417
Interface	419
AT (Address Translation)	422
IP (Internet Protocol)	422
ICMP (Internet Control Message Protocol)	425
TCP (Transmission Control Protocol)	427

UDP (User Datagram Protocol)	429
EGP (Exterior Gateway Protocol)	431
SNMP (Simple Network Management Protocol)	432
Event action configuration	434
Event actions	435
Event information configuration	436
Real time monitoring	437
Event log view	438
Setting automatic refresh interval	439
A Troubleshooting	441
General ASM troubleshooting	443
ASM agent for SCO OpenServer troubleshooting	449
ASMSMUXD	449
ASMCONFIG	452
BPBSMUXD	452
BPBCONFIG	452
IPMSMUXD	453
ASM Agent for SCO UnixWare troubleshooting	454
ASMSMUXD	454
ASMCFG	455
BPBSMUXD	456
IPMSMUXD	457
XASMMON	457
ASM Windows NT troubleshooting	459
Hardware common part troubleshooting	467
C RAID utilities	469
ASM Mylex RAID utility	471
Mylex RAID controller monitor	471
Controller tab	471
Disk tab	471
Controller statistic tab	472
Disk statistic tab	473
Physical disk statistic graph tab	473
Logical disk statistic graph tab	474
ASM DPT RAID utility	475
HBA (Host Bus Adapter) tab	475
Bus tab	477
Device tab	478
Array tab	480
Statistic tab	481
Graph tab	482

AcerAltos 3102RS utility	484
AcerAltos 3102 RAID Controller monitor window	484
Controller tab	484
Channel tab	484
Drive tab	485
Controller statistic tab	486
Controller statistic graph tab	486
Disk statistic tab	487
Physical disk statistic graph tab	487
Logical disk statistic graph tab	488
	488
D APC UPS system utility	489
Information tab	491
Battery tab	493
Control tab	497
E ASM Adaptec CI/O utility	501
Adaptec CI/O monitor window	503
Controller tab	503
Device tab	505
Bus port tab	507
Volume tab	508
Statistic tab	509
F Management system snap-in modules	511
CA Unicenter TNG	513
HP OpenView	515
Intel LDCM	515
MMC (Microsoft Management Console)	517



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 management system include the following:

- **ASM Console**

ASM 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 Console through the Management Information Base (MIB) Object ID get/set requests from the ASM 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 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 Server Agent Utilities**

The ASM sever 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 MIB Browser (customized version only)**

ASM MIB Browser is an MIB (Management Information Base) file browsing tool included with the ASM 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 MIF Browser (customized version only)**

ASM MIF Browser is an MIF (Management Information Format) file browsing tool included with the ASM 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 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

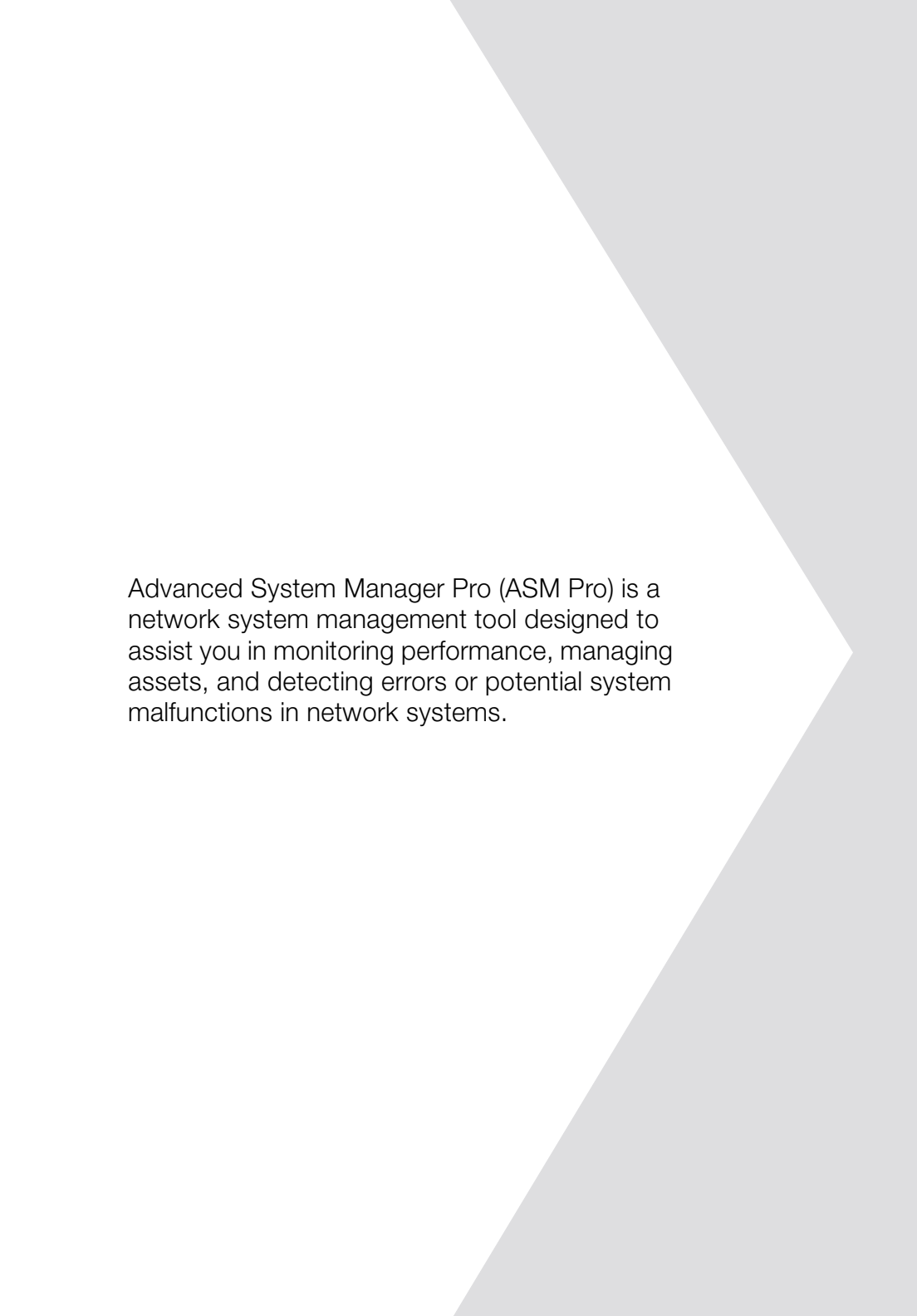
The Alert via LAN (Land Area Network) function of ASM enables administrators to easily monitor and reconfigure local systems via a network.
 - Remote Console

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 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 package consists of the following software components:

- ASM Console

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

ASM Console supports systems running on Windows 95, Windows 98, Windows NT, or Windows 2000.

- ASM Server Agent

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

ASM 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 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 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 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 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 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 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 Console

- Intel Pentium or higher processor
- 64MB of RAM (128MB recommended)
- 20MB free hard disk space
- Microsoft Windows 95, Windows 98, Windows NT, or Windows 2000 operating system
- Ethernet card
- Modem

ASM Server and Desktop agents

- 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 Console

To install ASM Console:

1. Insert the Resource CD into the CD-ROM drive on your system.
2. Click on the Startup icon.
3. Click on Software Installer, and select ASM Console.
4. Follow the Installation Wizard.
5. Click Finish to complete the installation.



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

Installing ASM Server Agent

ASM 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, 4.11
- SCO OpenServer 5.0
- SCO Unixware 7.x
- Microsoft Windows NT 4.0 Server
- Linux RedHat 6.2
- Microsoft Windows 2000 (Server and Advanced Server)

Installing the Novell NetWare Server Agent



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

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

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

```
load snmp control=public
```

If you load SNMP.NLM before ASM 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. Use the diskette maker utility on the Startup Resource CD to create your NetWare installation diskette.
2. Insert the diskette into the NetWare server's drive.
3. At the NetWare server console, type:
Load A: setup
4. You are asked if you want to install the ASM 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 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 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 drivers.



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

Follow these steps to install the SCO Server Agent:

If the ASM installation diskette is already available, go to Step 2. Otherwise, perform Steps 1 to make the ASM installation diskette from the diskette image file on the ASM package CD-ROM.

1. Use the Diskette Maker utility on the Startup Resource CD to create your SCO OpenServer installation diskette.
2. If you are in the desktop window, click on the Software Manager icon. If you are at the UNIX shell prompt, type "custom" and press Enter.
3. From Software Manager or the custom program, select Software and then Install New.
4. The "Begin Installation" screen appears. Follow the onscreen instructions. Click on Continue to accept the defaults.
5. When the Select Media screen appears, highlight Floppy Disk Drive 0 and select Continue.
6. At the Install Preferences menu, select Full. The *asmconfig* screen appears.



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 Console system. (You can run `asmconfig` at a later time to add or change the ASM Console IP address. See the ASM 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.

The installation process adds the ASM agent driver to the SCO operating system, and the following message appears before the kernel relinks.

Adding device to system configuration files. . .

When the installation is complete, the following message appears:

Installation Complete.

9. Exit Software Manager or the custom program, and reboot the system.

Configuring ASM Server Agent for SCO OpenServer

You may disable the password if you are installing ASM 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 Console to remotely change or set any values for the agent.

Refer to the ASM 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 installation diskette from the DD file on the ASM 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 installation diskette into your floppy drive and, at the shell prompt, execute this command to begin ASM installation:

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

The installation process copies the ASM 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 Server Agent can be manually started by executing the command:

```
# /usr/asm/asmsmuxd
```

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



Before starting ASM SMUX Agent asmsmuxd, execute the ASM Agent Configuration Utility asmcfg to configure at least "SNMP", "ASM_Password" and other parameters. Refer to "Chapter 4 - ASM Server Agent Utilities" in the ASM Pro manual for detailed instructions on using the ASM Configuration Utility.

Installing the Microsoft Windows NT Server Agent



Before installing the ASM 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 installation CD-ROM into your drive after booting NT and logging in as the system administrator.
2. Click on the Start button and select Run. A dialog box appears that allows you to specify the setup program in the NT directory of the installation CD.
3. Verify the path and click OK. The Welcome screen appears.
4. Click Next. You are asked to stop SNMP service.
5. Click Yes. You are prompted to choose a destination directory. If you only want to install ASM SNMP agent and Remote Console, you can choose Typical. If you want to choose more components, click Custom. There are five components in ASM agent:
 - SNMP agent
 - DMI
ASM Pro agent defines a proprietary ASM.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 Mangement Console.
6. 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 Server Agent solely for the purpose of utilizing UPS and/or RDM functions.

7. Enter a password and click OK. A password is required when using the ASM 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 Console tries to change or set these values.
8. Enter the IP address of the ASM 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).
9. Click Yes to save your changes. The view readme file dialog box appears.
10. Click Yes to view, No to continue.
11. Click Finish to exit setup.

2 Quick tour

This quick tour is a step-by-step tutorial that helps you get started with setting up and customizing ASM 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 Console, please refer to “Chapter 2 ASM Console” on page 15.

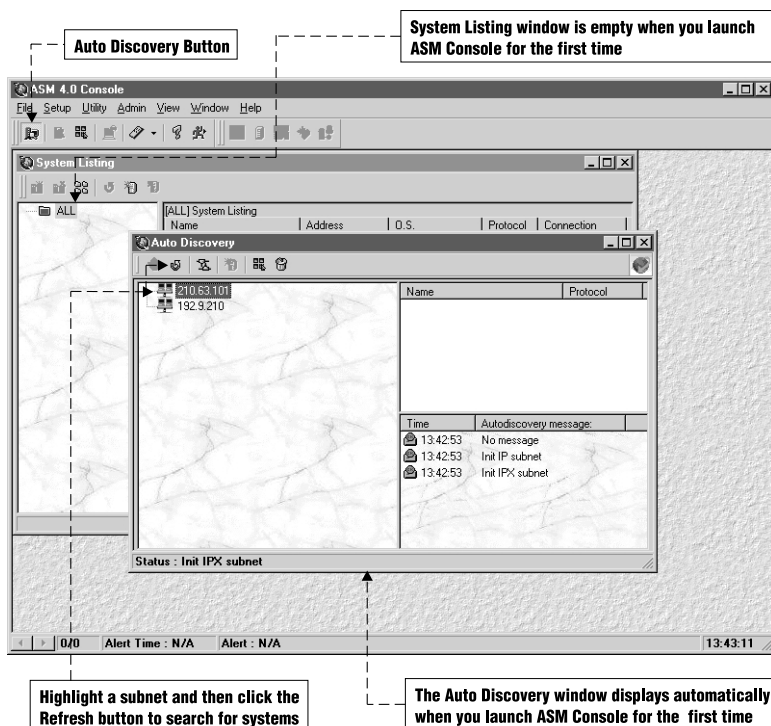
▶ ASM console

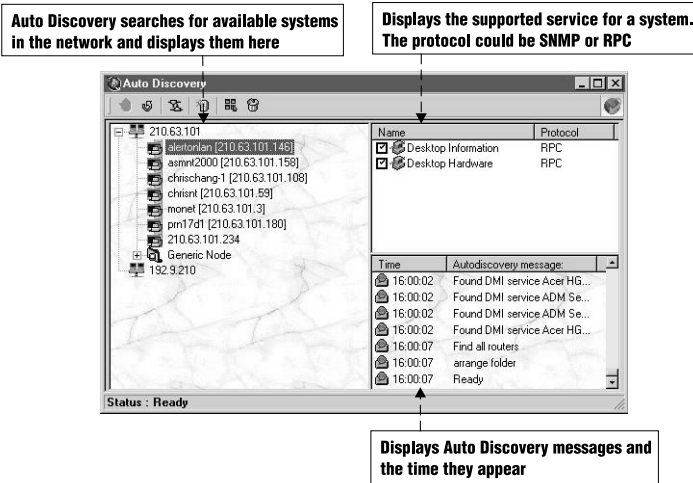
To launch ASM Console, press the Start button and then select Programs > ASM > ASM Console or you can double-click on the ASM Console shortcut icon.

If you are using ASM 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 Console.

After initializing a password, the Auto Discovery window appears:





Understanding system listing

The System Listing window is the main interface of the ASM 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" with two main tables. The top table lists systems with columns for Name, Address, O.S., Protocol, and Connection. The bottom table lists services with columns for Service, Protocol, State, and Health.

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:

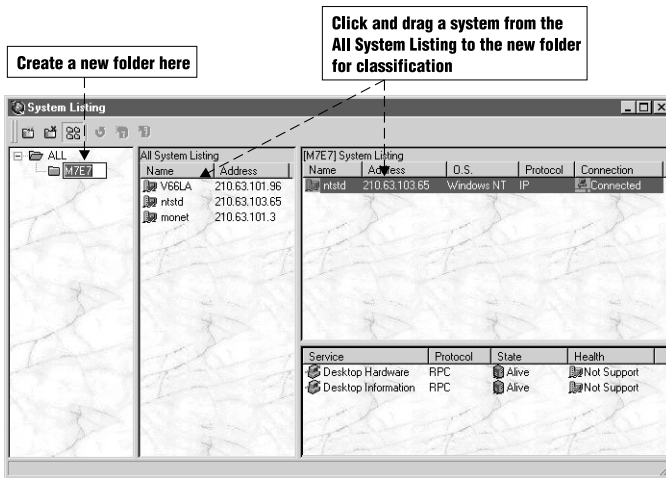
- SNMP for SNMP services
- RPC for DMI Instrumentation code

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

- Normal
- Abnormal
- Not Supported

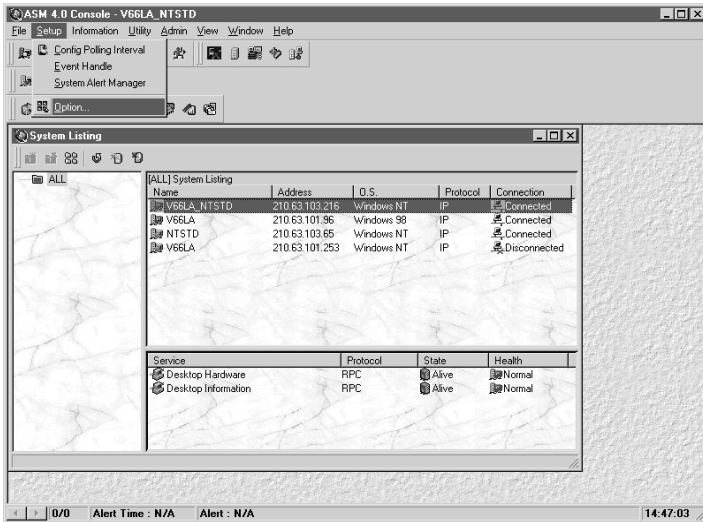
This panel indicates the state of this service. It can be:

- Alive
- Unstable
- Dead



Customizing system listing

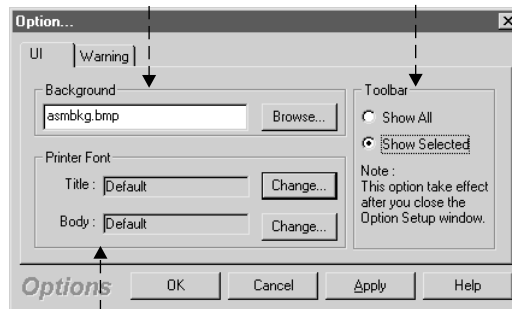
If you get bored looking at the same background graphic or if the fonts you are using now hurts your eyes, you can easily change them to fit your needs. Also, you can set the warning option to warn you before it executes a certain command. To display the Option dialog box, select Setup > Option.....



User interface (UI) tab

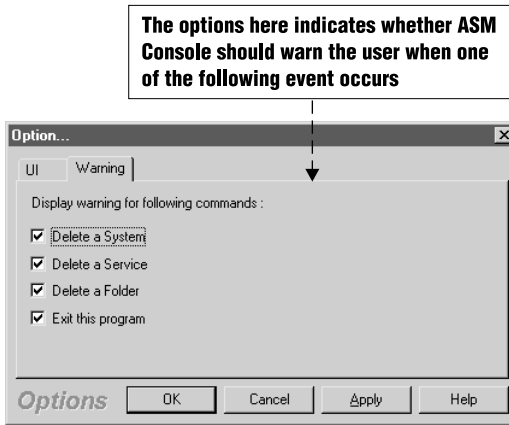
Choose a graphic to change the background display of ASM Console

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



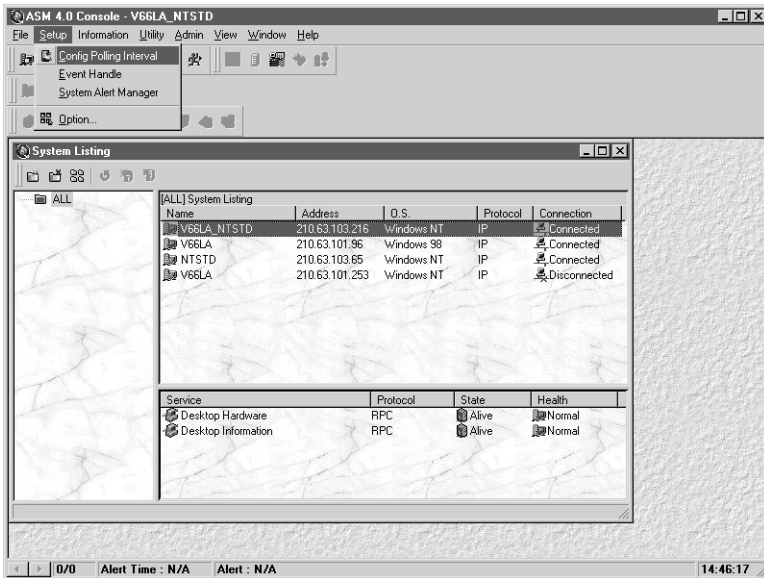
Choose a font for the title and body text of the printed material

Warning tab



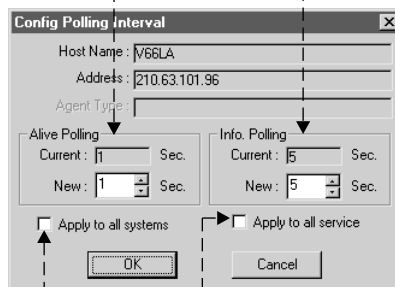
Configuring polling interval

ASM 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 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

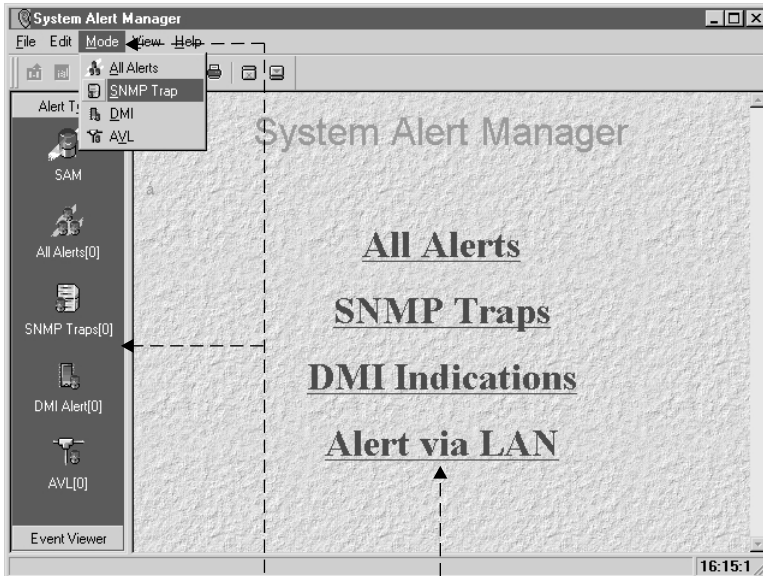
Information Polling determines how frequently the Console polls the Agent to update its data. Polling interval must be from 01 to 60



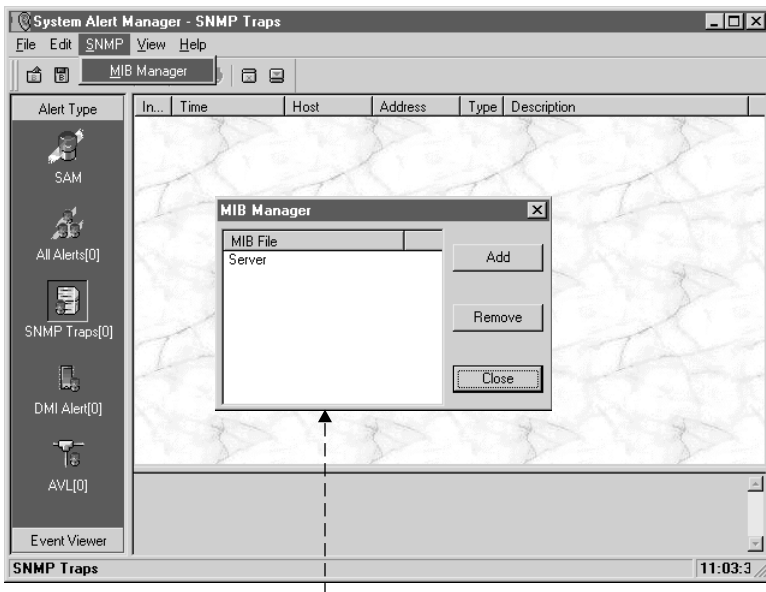
You can set the interval to all systems or to all services

► 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.

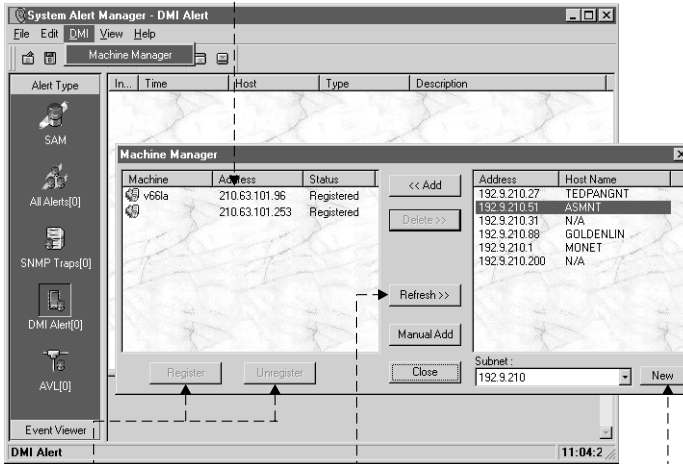


You can view SNMP Traps, DMI Indications, and AVL Packets by clicking any one of these



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



Click these buttons to Register and Unregister a system respectively

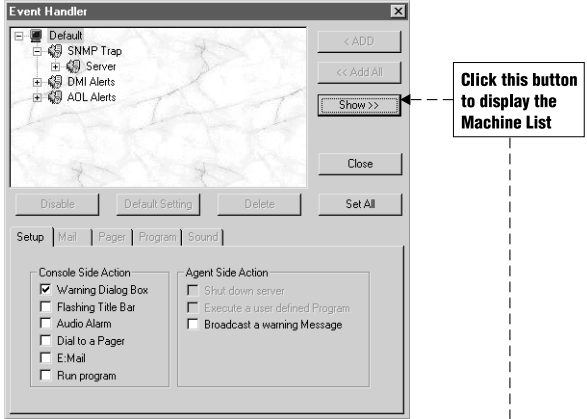
Click this button to refresh the list and add a new system or click the Manual Add button to add a system

Click this button to view a new subnet. The systems found in the new subnet will be displayed in the right panel

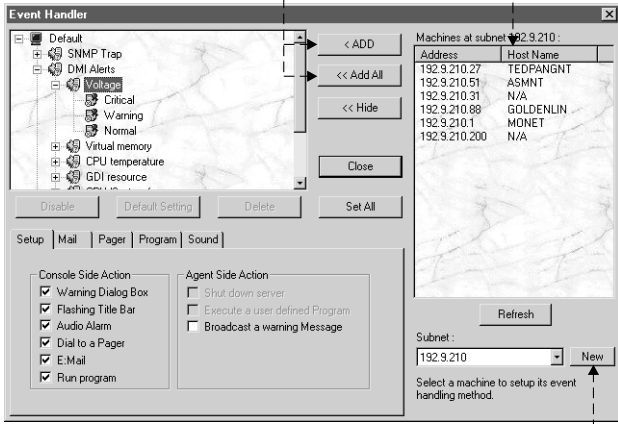
Assigning event handler

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 these buttons to add specific systems to handle and define different settings



Click this button to apply the current settings to all sub items under the currently selected item. Example, select Voltage Indication and click Set All, the sub items, critical, warning, and normal, takes the current settings

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

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

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

Event viewer

Event Viewer gathers information about events in the system being monitored by the ASM 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

System Alert Manager - v66la_ntstd

File Edit Operation View Help

Alert Type

Event Viewer

v66la [3]

NTSTD

v66la [3]

v66la_ntstd [84]

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 in normal condition.
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 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%

v66la_ntstd

By Server By Type

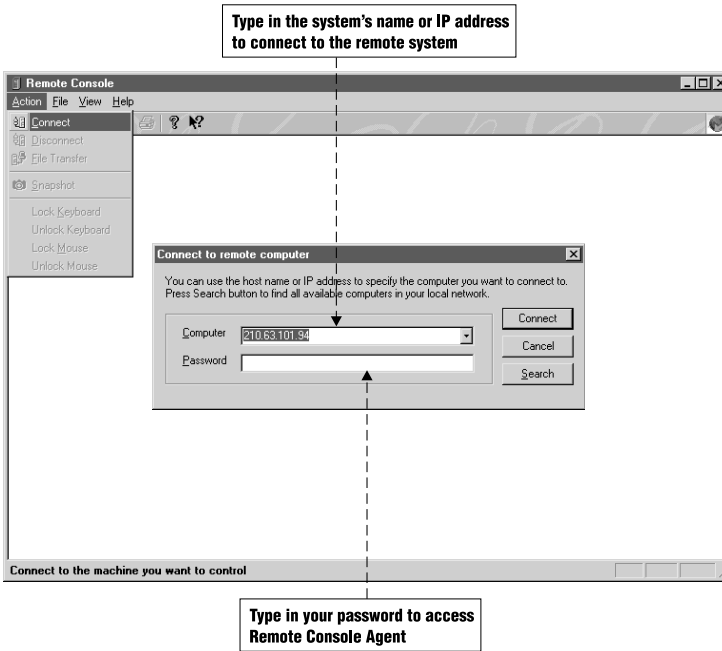
Pie Bar 2D

v66la_ntstd 11:16:5

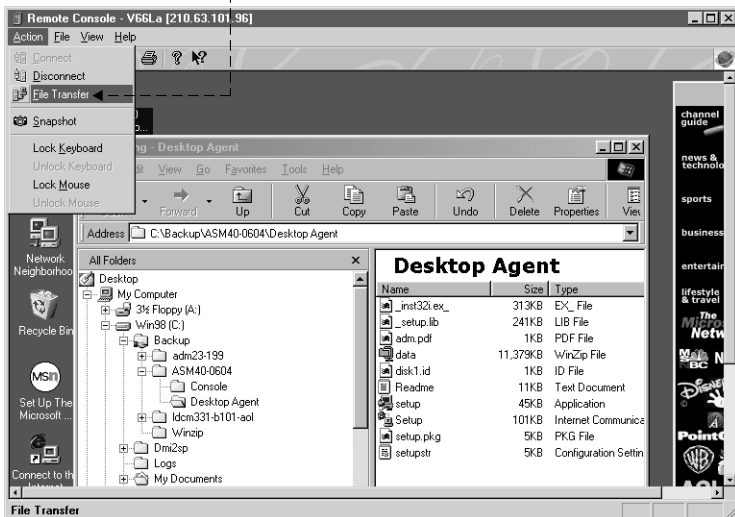
Lists the systems found in the System Listing of ASM Console

Remote console

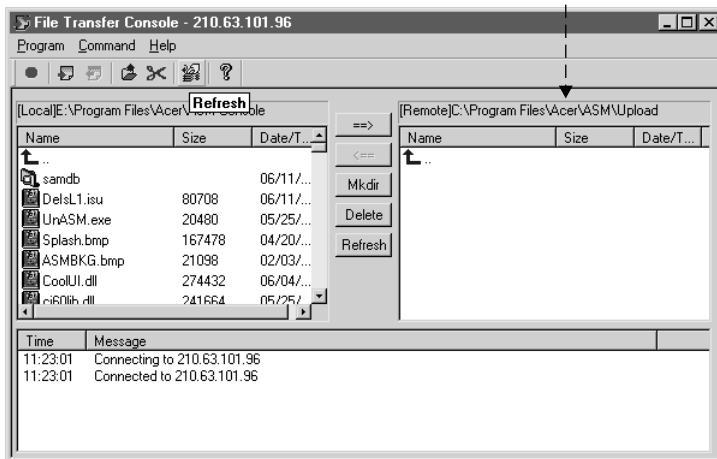
The Remote Console function of ADM allows the administrator to remotely control the local systems connected to the LAN via the server, if access is granted.



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



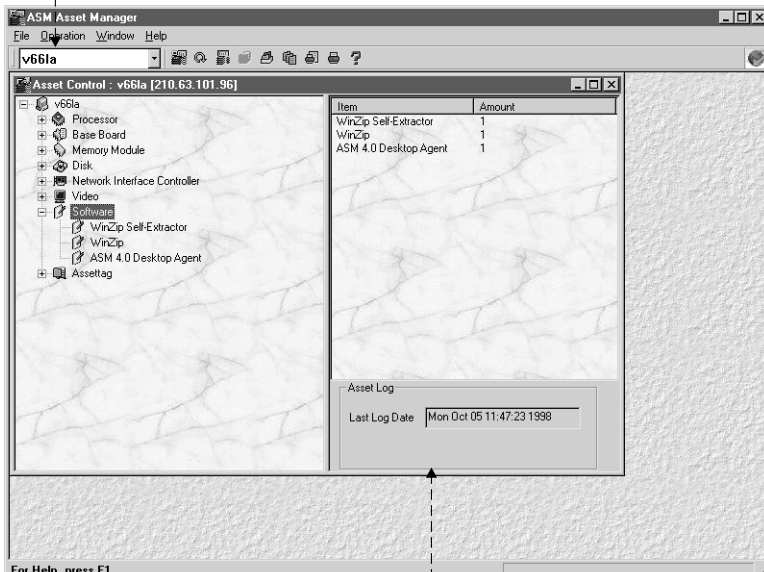
ASM Agent automatically creates a folder called "Upload" in the ASM program folder. You can only access this directory for security control



▶ Asset manager

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

Select the systems whose asset information you want to view



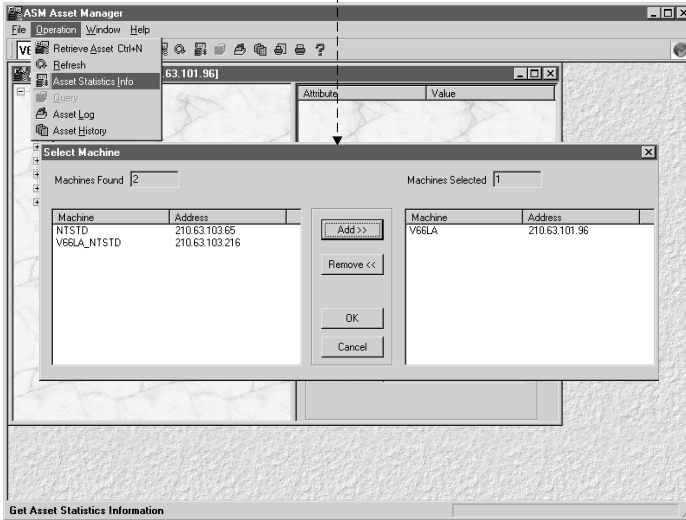
The screenshot shows the ASM Asset Manager window for system 'v661a'. The left pane displays a tree view of system components, including Processor, Base Board, Memory Module, Disk, Network Interface Controller, Video, Software, and Assettag. The right pane shows a table of assets with columns for Item and Amount. The Asset Log section at the bottom right displays the last log date as 'Mon Oct 05 11:47:23 1998'.

Item	Amount
WinZip Self-Extractor	1
WinZip	1
ASM 4.0 Desktop Agent	1

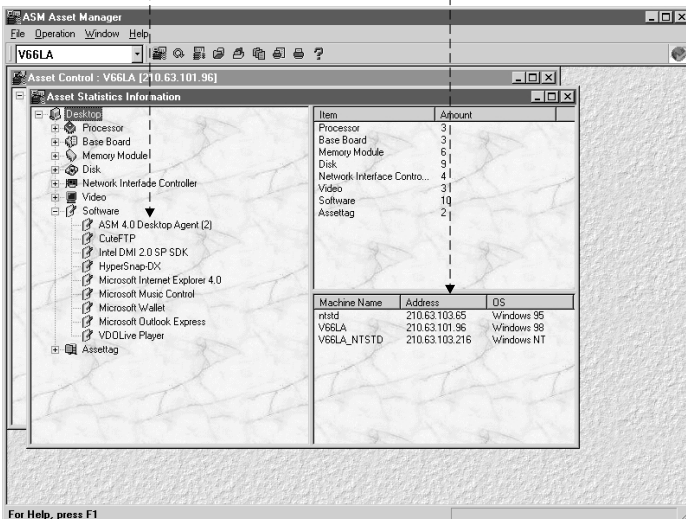
Asset Log
Last Log Date | Mon Oct 05 11:47:23 1998

Shows the log date

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



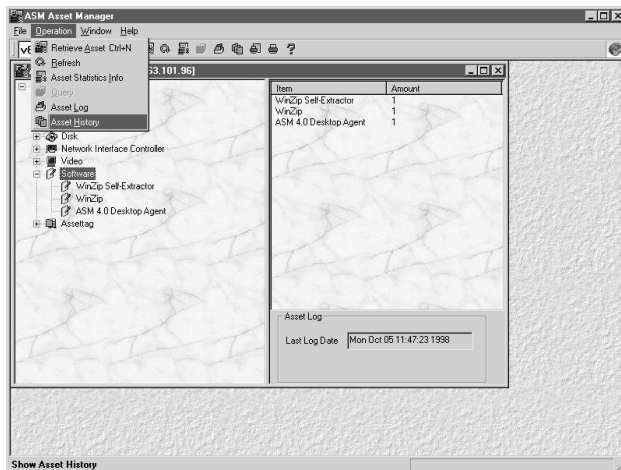
Systems found by the query is displayed here

Select the item you want to query

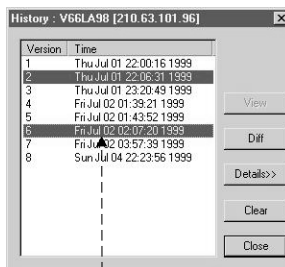
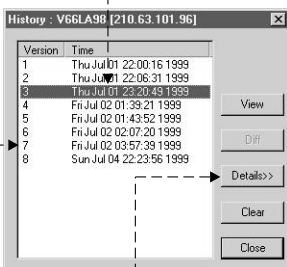
Select any value in this field to find a system

Click here to save asset log to a text file

Click here to clear asset log

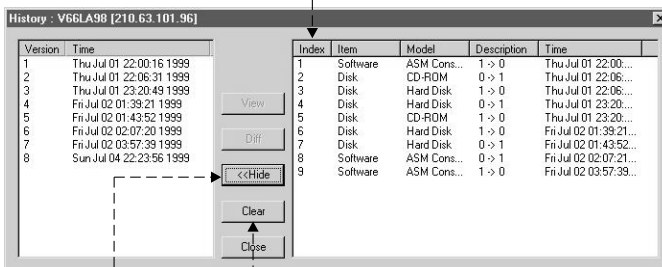


You can view old asset information



Click Details>> to view history log

Or compare the difference between two log versions

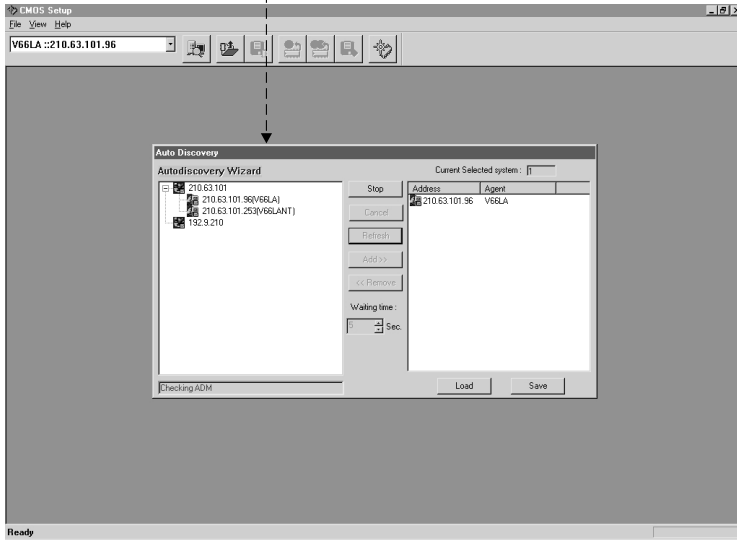


Click <<Hide to hide the history log

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

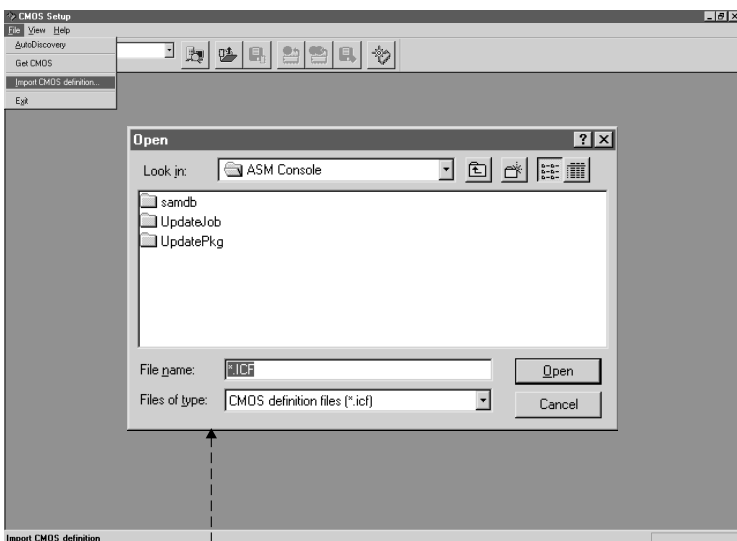
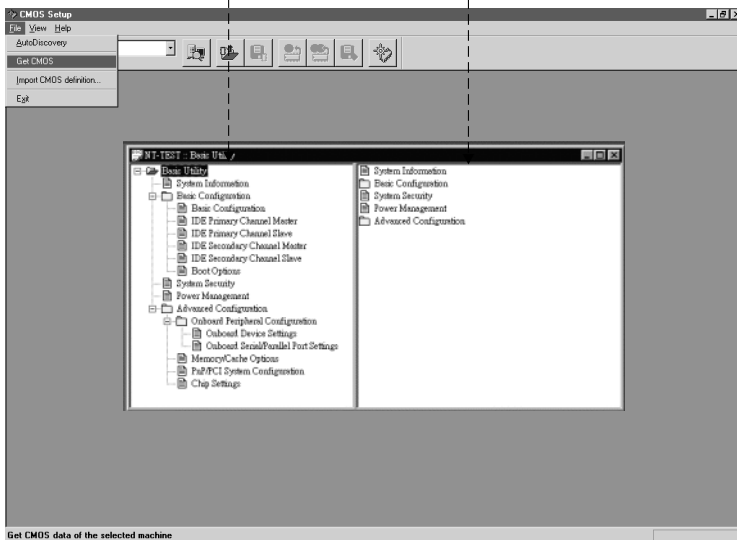
► CMOS setup manager

The Auto Discovery function helps you locate systems in the network



Click any item here to view or update

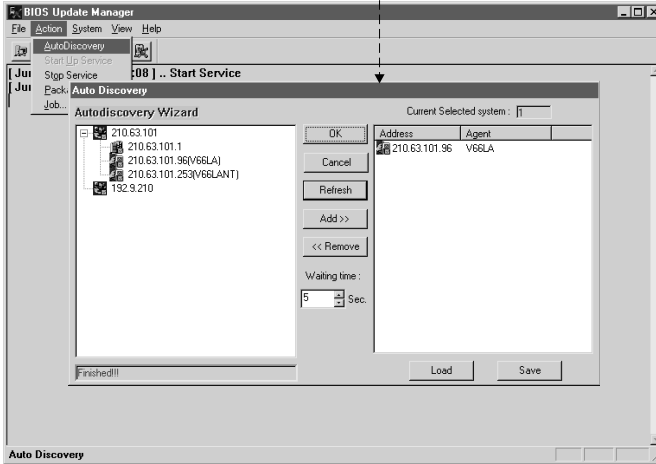
View or update in this panel



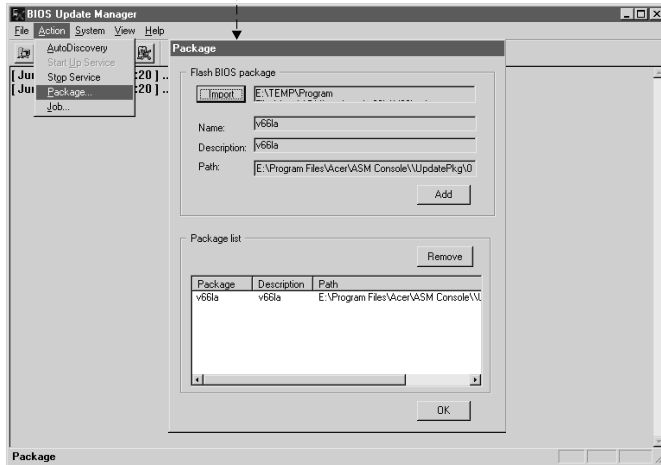
You can import CMDS definition file if the CMDS version of the target system does not match the current definition then you can setup CMDS remotely

BIOS flash manager

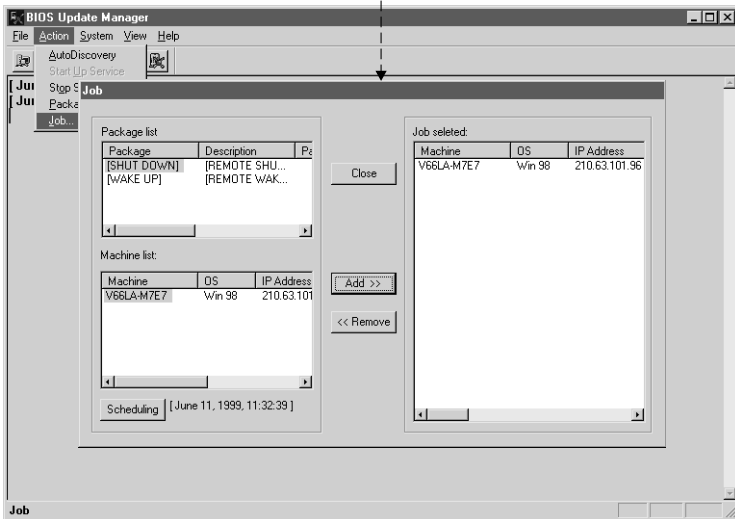
The Auto Discovery Wizard guides you to find systems in your network when you launch the BIOS Manager for the first time



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 Console

ASM 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 system agents.

▶ Launching ASM Console

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

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

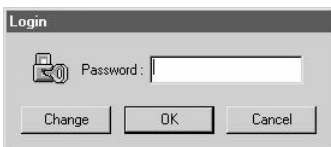
Initializing and changing the password

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 Console:



To access ASM 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. The dialog has a title bar with the text 'Change Password'. Inside, there are three text input fields: '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 Console confirms the password change by displaying a dialog box with the message "Password changed successfully."



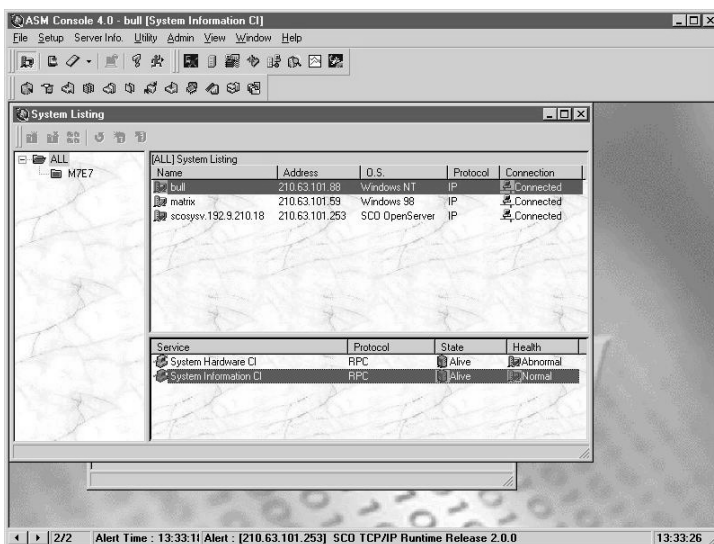
.....

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

▶ ASM Console user interface

The primary interface for ASM 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 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 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 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 Console

- The Setup Menu contains commands that allow you to specify the systems to be managed by ASM 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 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 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 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 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.

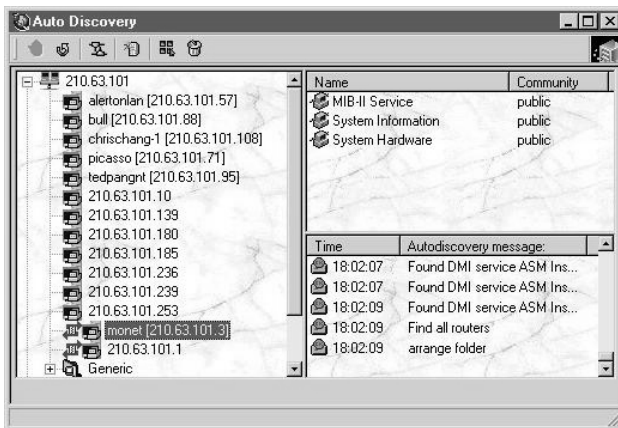
The upper right panel of the auto discovery window displays the services of the system highlighted in the left panel. This information includes the name and OID of the services, if any exist. These services typically include one or more of the following:

- Hardware, System, or Management Information Base-II (MIB-II) for server systems
- Desktop Information and Desktop Hardware for desktop 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
- 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 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 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, SCO OpenServer, and SCO UnixWare operating systems.



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

ASM Console detects 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 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 Console searches all addresses in the specified with different protocols to find the agent. For all of the ASM 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.

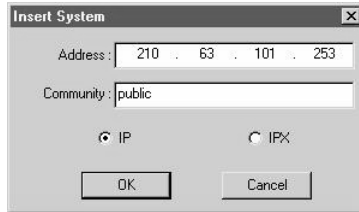


To add a new SNMP community, click on New and type in the community name. To remove a SNMP community name, highlight the community name and click Remove. The list of agents may vary depending on how you installed ASM Console.

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.

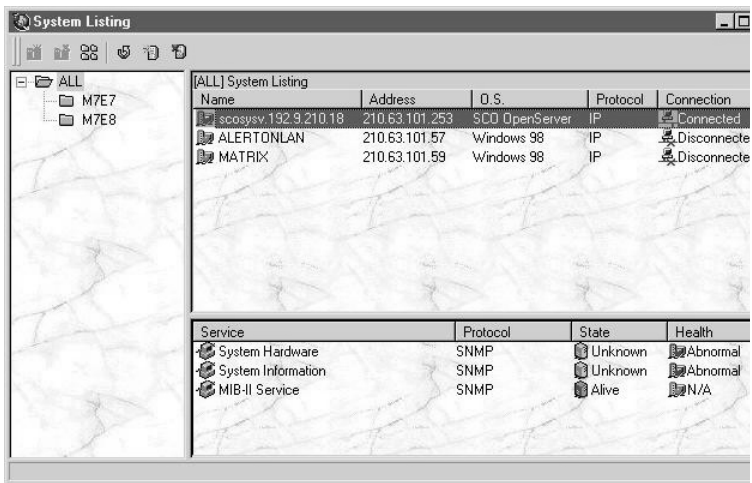
Removing a system from the list

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 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 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.



.....

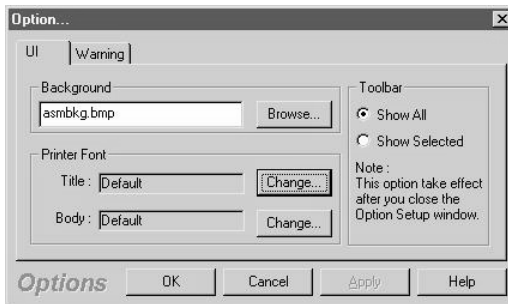
Note: If the status of the selected system is red (question mark), all toolbar buttons are disabled (grayed out). Only the Auto Discovery button is available.

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.

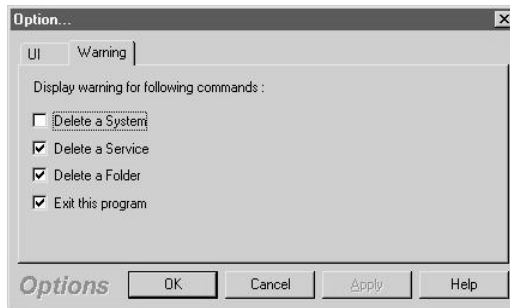
To personalize the wallpaper of the Console, click Browse and choose a graphic file, then click OK.

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 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 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

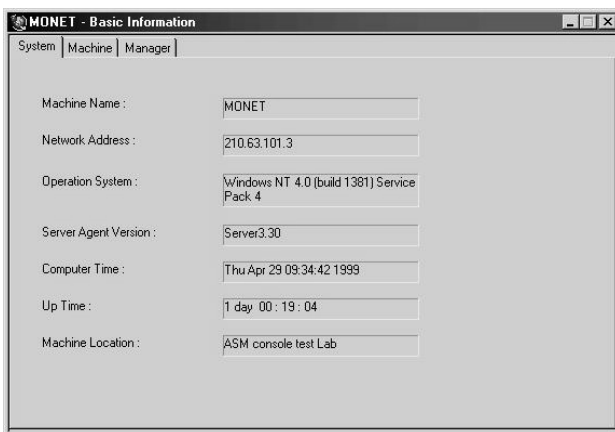
The following sections describe the Information menu options that appear when a System Information service is selected in the System Listing window.

Basic information

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

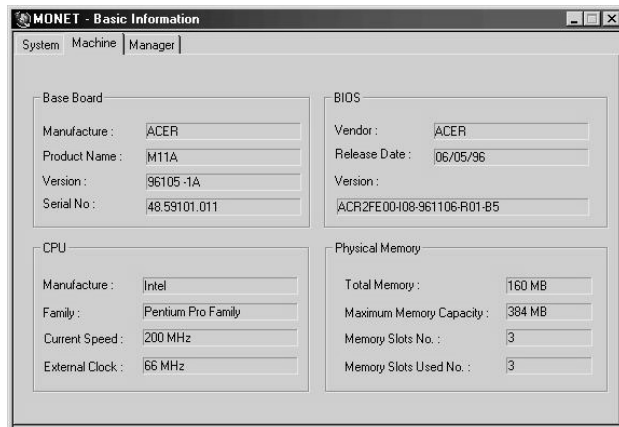
System tab

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.



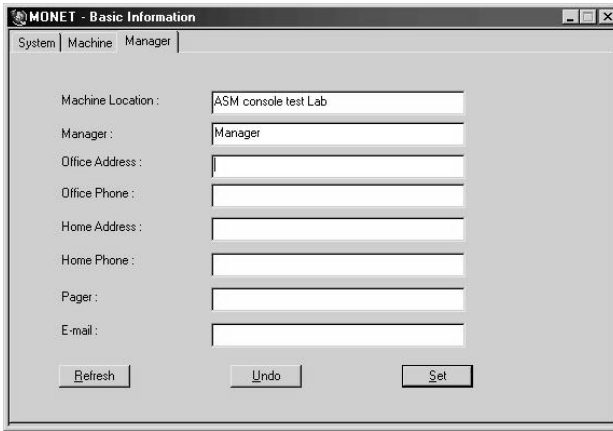
Machine tab

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



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 Server Agent system using the `asmcmfig` 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 :

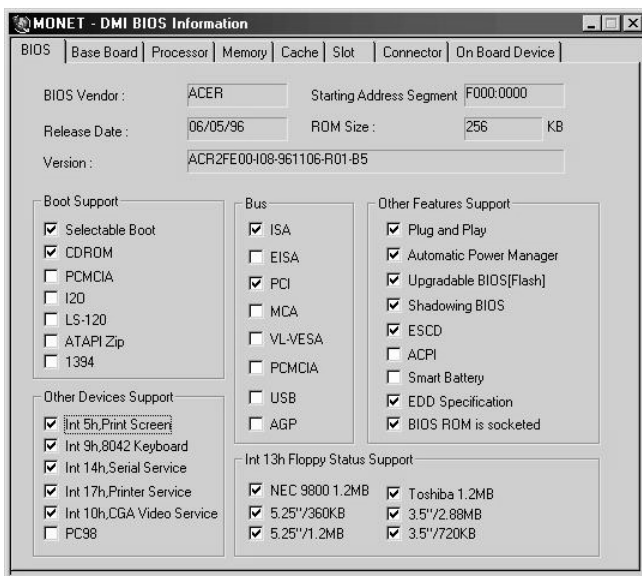
Refresh Undo Set

DMI BIOS information

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

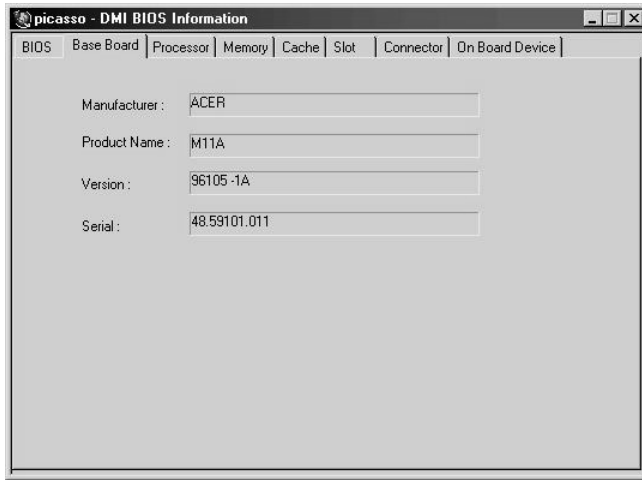
BIOS

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.



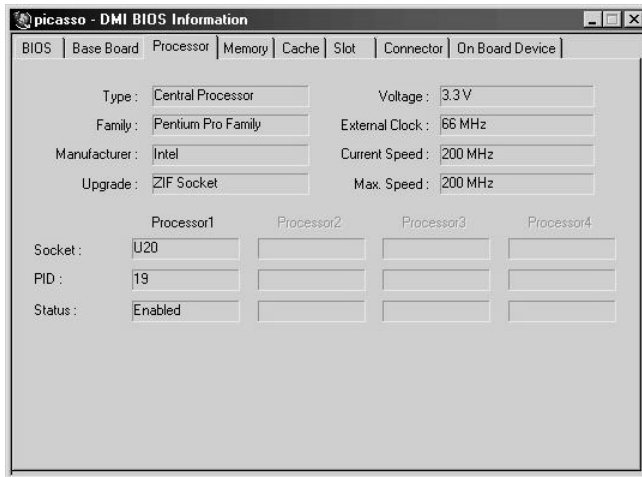
Base board

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



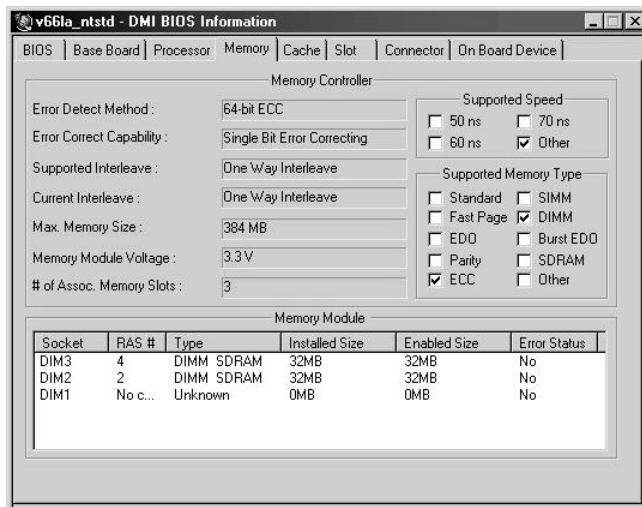
Processor

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

picasso - DMI BIOS Information							
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

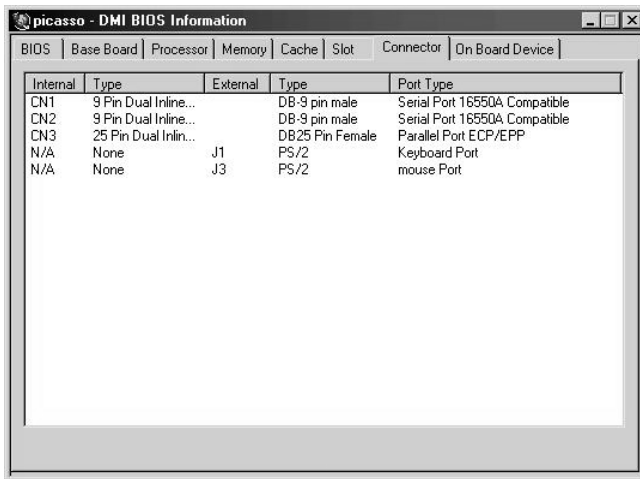
Slot

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.

picasso - DMI BIOS Information						
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

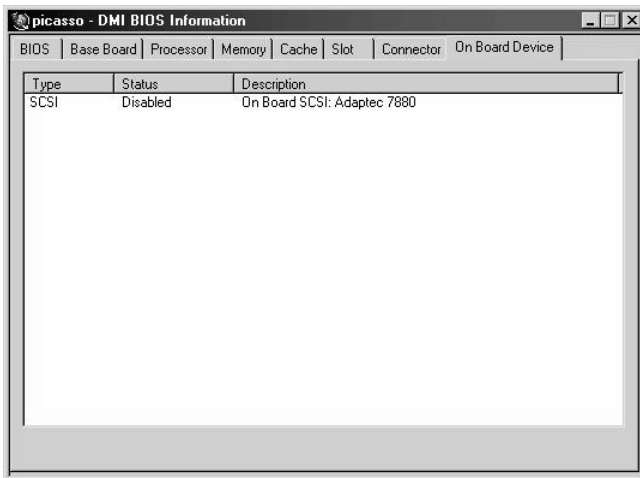
The Connector tab displays information about the motherboard connectors.



Internal	Type	External	Type	Port Type
CN1	9 Pin Dual Inline...		DB-9 pin male	Serial Port 16550A Compatible
CN2	9 Pin Dual Inline...		DB-9 pin male	Serial Port 16550A Compatible
CN3	25 Pin Dual Inlin...		DB25 Pin Female	Parallel Port ECP/EPP
N/A	None	J1	PS/2	Keyboard Port
N/A	None	J3	PS/2	mouse Port

Onboard device

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



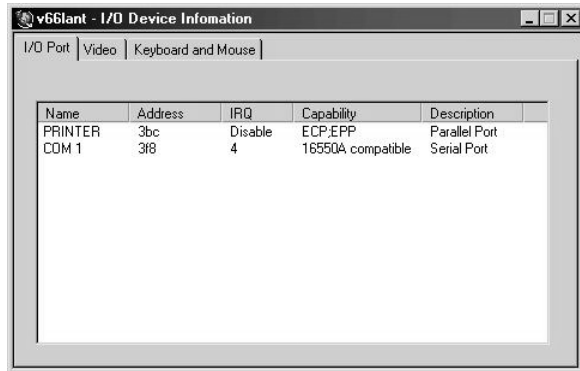
Type	Status	Description
SCSI	Disabled	On Board SCSI: Adaptec 7880

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

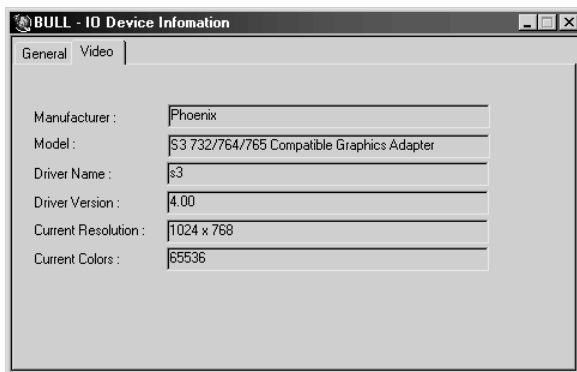
The I/O Port tab displays information about the system's input/output devices and ports.



Name	Address	IRQ	Capability	Description
PRINTER	3bc	Disable	ECP/EPP	Parallel Port
COM 1	3f8	4	16550A compatible	Serial Port

Video tab

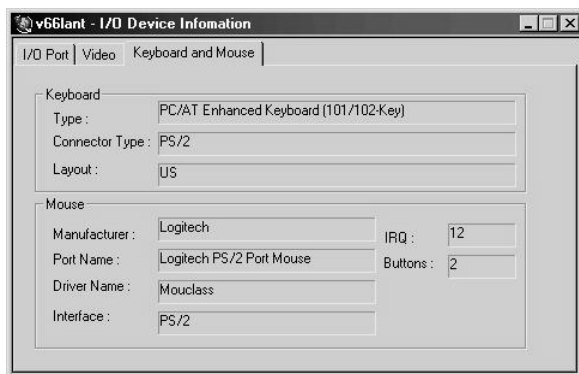
The Video tab displays information about the system's video device and driver.



Manufacturer :	Phoenix
Model :	S3 732/764/765 Compatible Graphics Adapter
Driver Name :	s3
Driver Version :	4.00
Current Resolution :	1024 x 768
Current Colors :	65536

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

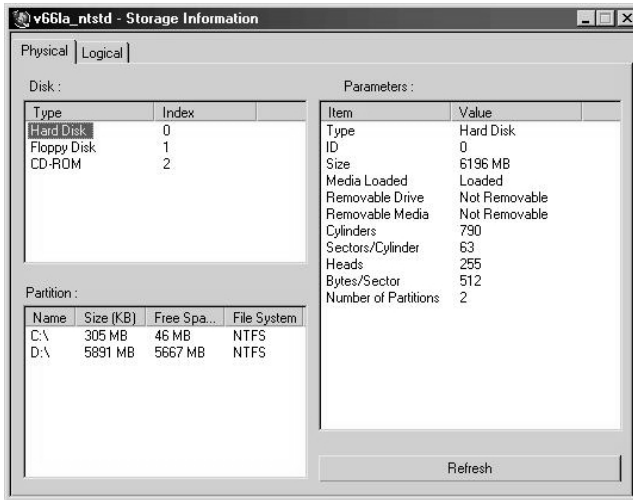
Physical disk indicates the number of actual hard disk drives installed in a system. Each hard disk drive is connected to an adapter that controls them.



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.

The screenshot shows a window titled "BULL - Storage Information" with two tabs: "Physical" and "Logical". Below the tabs is a "Number of Volume:" field containing the number "6" and a "Refresh" button. The main area contains a table with the following data:

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

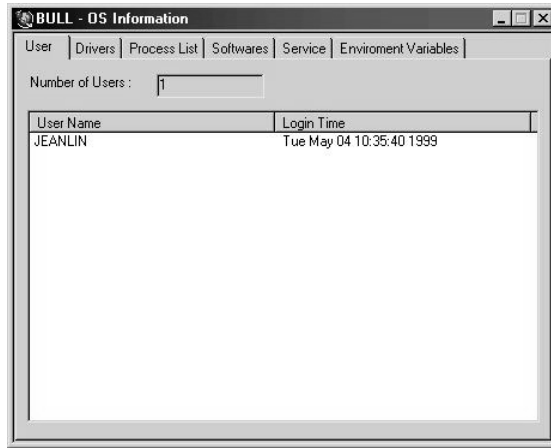
Select Information > Server (or Desktop) Information > O.S. Information to display the Operating System Information screen that displays information about the operating system. There are six screen tabs for server systems and three for desktop systems.

Server system

There are six screen tabs for server systems.

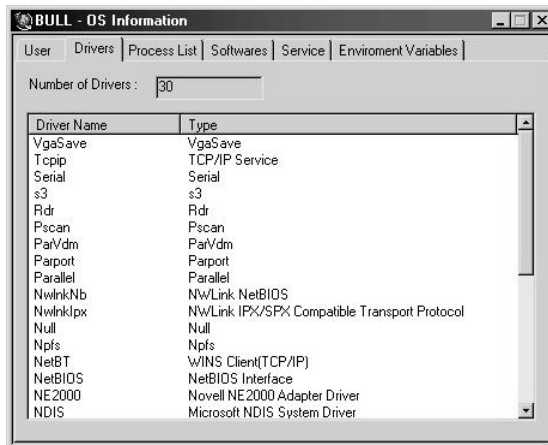
User tab

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)

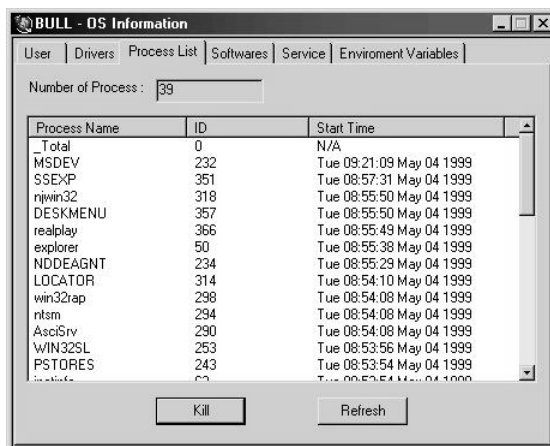
The Drivers tab displays all the device drivers installed in the ASM Agent. It also displays the total number of drivers installed in the system.



Process list tab

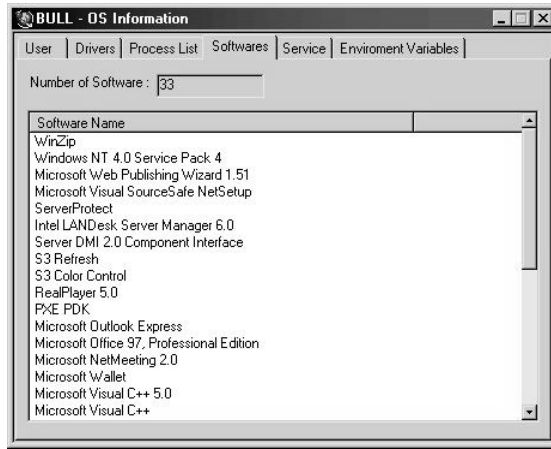
The Process List tab displays the programs and DLL libraries that are currently running on the system. For a server agent, it also displays the time that a process was executed.

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



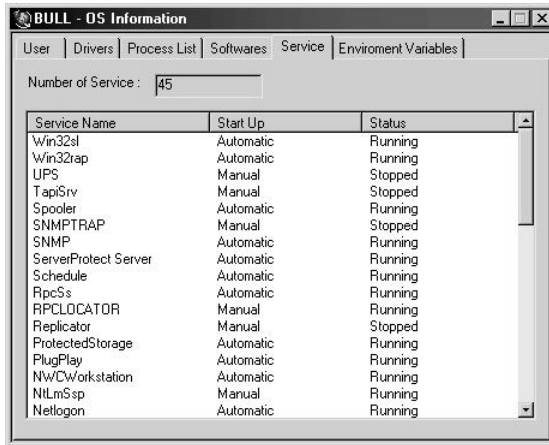
Software tab

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.



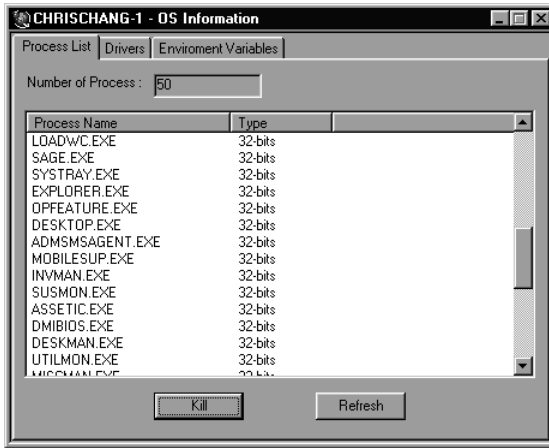
Desktop system

There are three screen tabs for desktop systems.

Process list tab

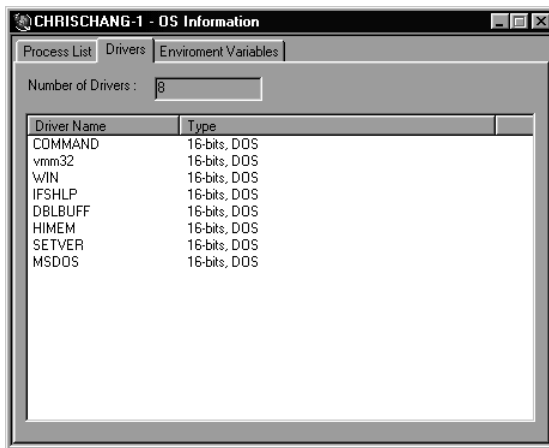
The Process List tab displays the number of processes the desktop has executed since it was turned on. It also shows the type (16-bit or 32-bit) of the program that was executed.

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



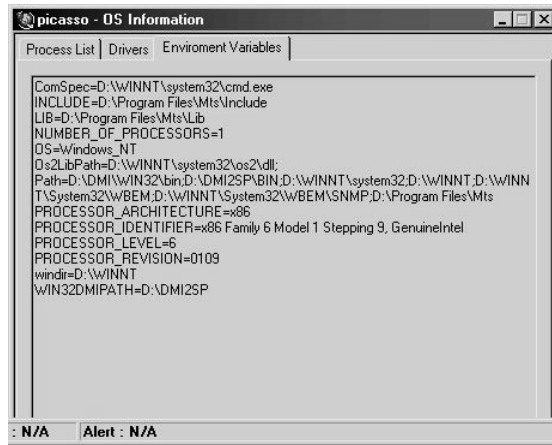
Drivers tab

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

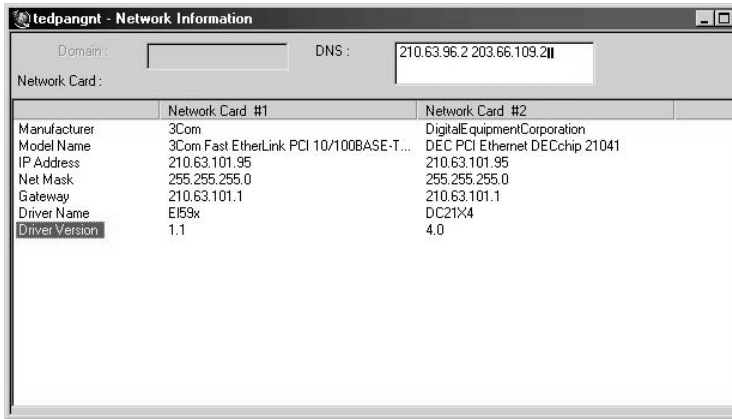
The Environmental Variables tab displays the contents of the initialization file of the operating system.



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.

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.

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" with a tab labeled "Memory Addr.". The window contains a table with two columns: "Range" and "Description".

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

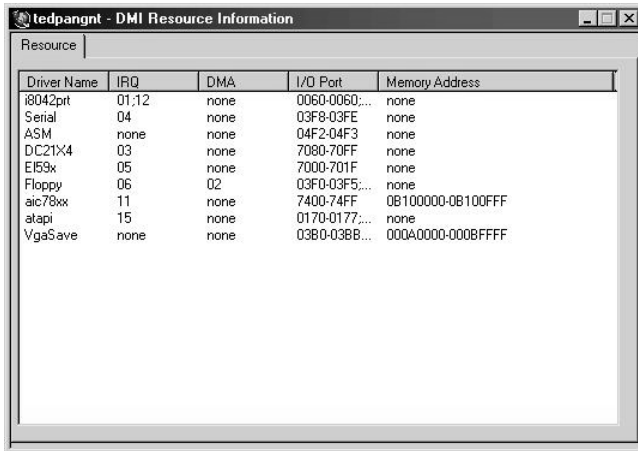
Memory address

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 tab selected, "Memory Addr.". The window contains a table with three columns: "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. The window 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
E153x	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

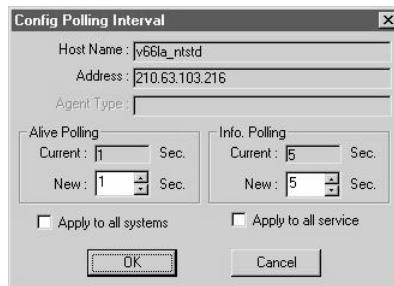
This displays the system's base memory usage, including the address, the length, and its description.

Performance monitoring

ASM monitors the performance of each agent periodically and sends this information back to the ASM 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.

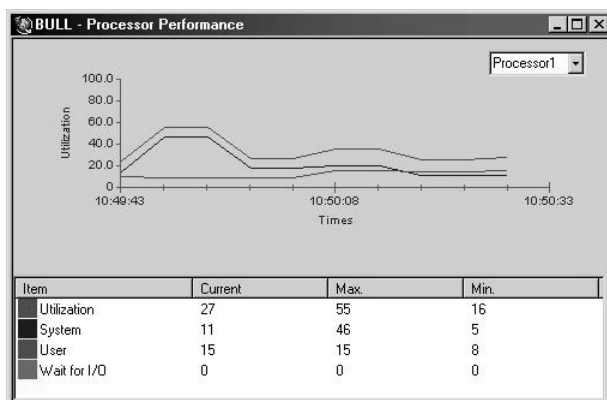
To change the polling interval, click the up and down button to increase or decrease the number of seconds, or type in the number of seconds, and click **OK**. The polling intervals must be from 1 to 60 seconds.

Processor performance (for server system)

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

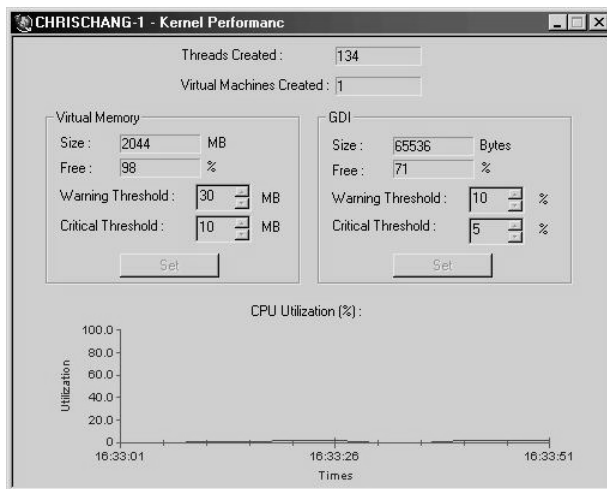
This window displays the current load and load limit of each CPU (Central Processing Unit) installed in the system. The higher the percentage, the more the CPU is being used. This indicates how much load the system has and how well the system's processing power is handling the load.

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 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

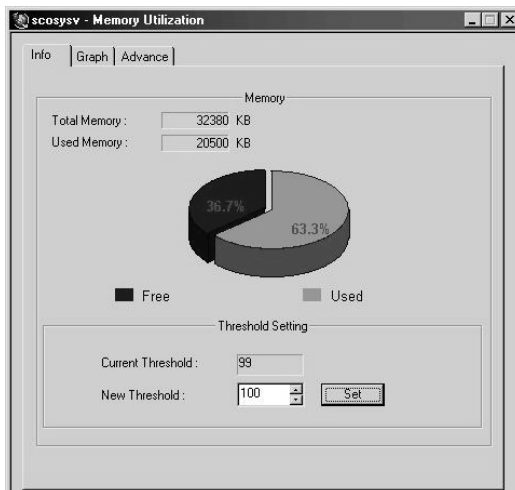
Select Desktop (or Server) Information > Performance > Memory to access the Memory Utilization information screen

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 3 - System Alert Manager for more information.

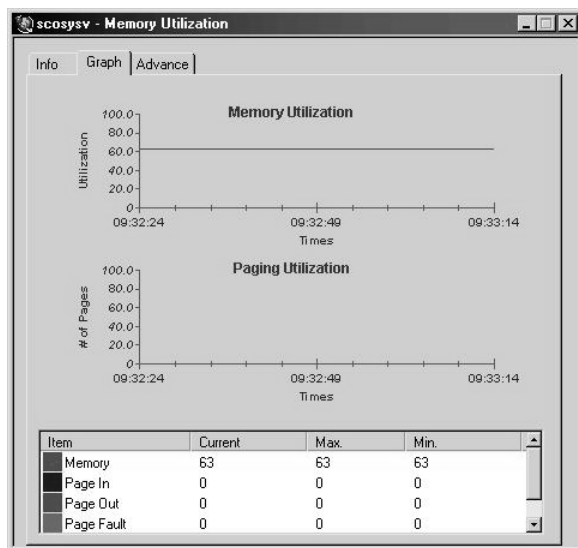




Note: If the password is enabled in the ASM Server Agent, enter the password for the Agent when changing the threshold setting.

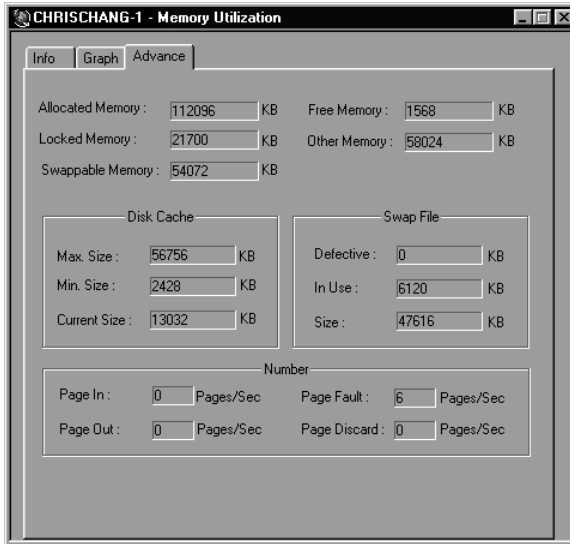
Graph

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.



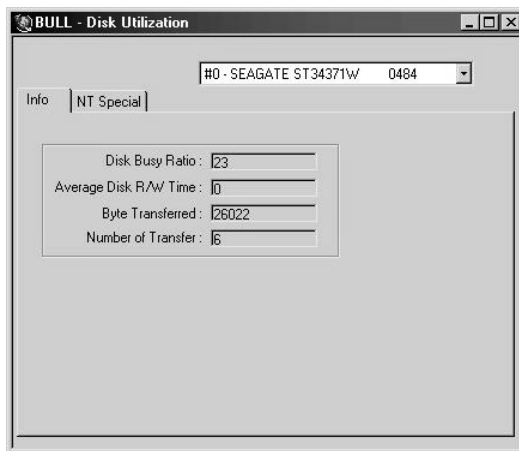
Note: This screen display may be different for different operating systems.

Disk utilization (for server systems only)

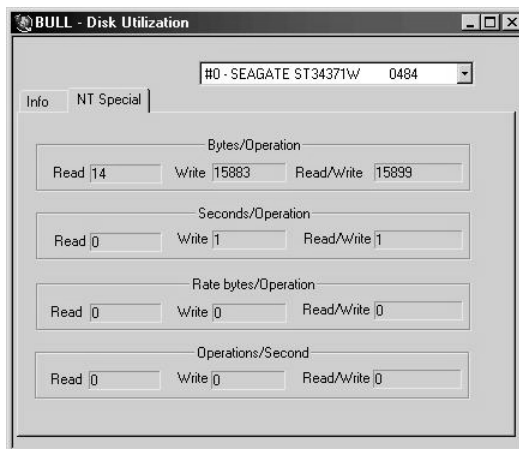
Select Server Information > Performance > Disk to access the Processor Performance information screen.

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.



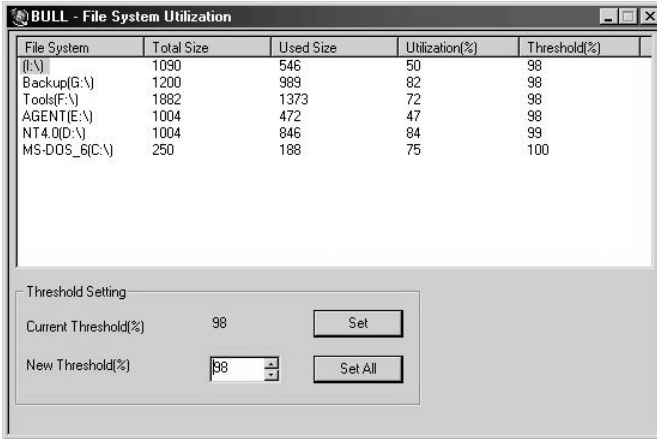
For Windows NT, you can click on the NT Special tab to display information about Read, Write, and Read/Write operation that is only supported in Windows NT. See the following example screen.



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 3 - 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.

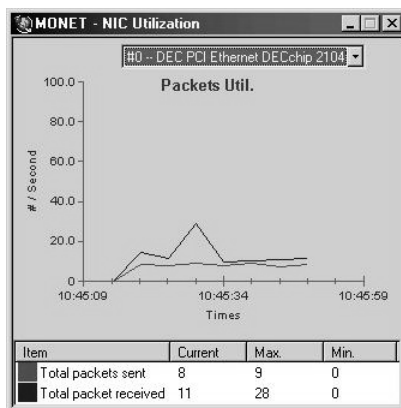


Note: If the password is enabled in the ASM System Agent, enter the password for the Agent when changing the threshold setting.

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.

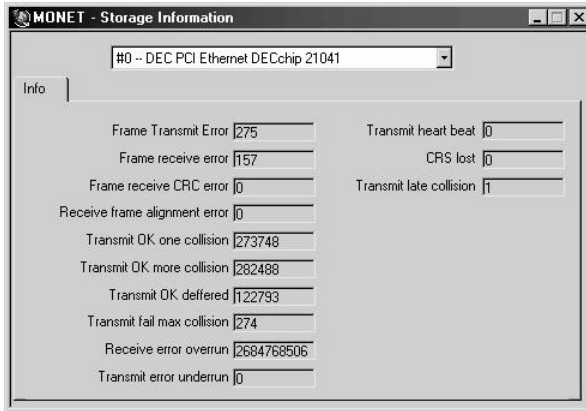


This information is useful for determining the network traffic in the periods that the agent is at its peak.

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.



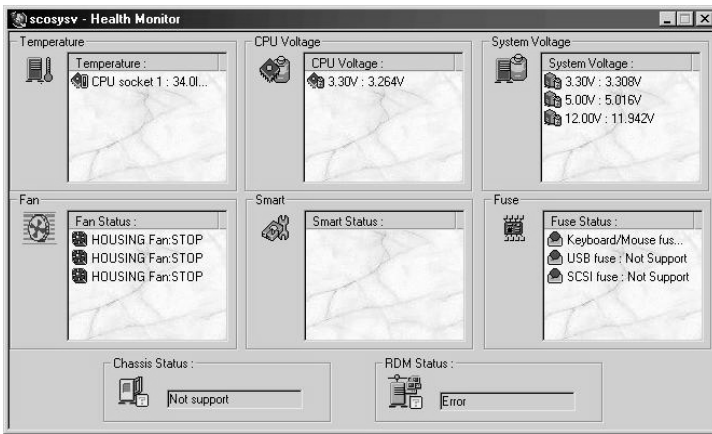
To view a particular network card, click the arrow button of the NIC# combo box and select a network card from the list.

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 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 3 - 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)

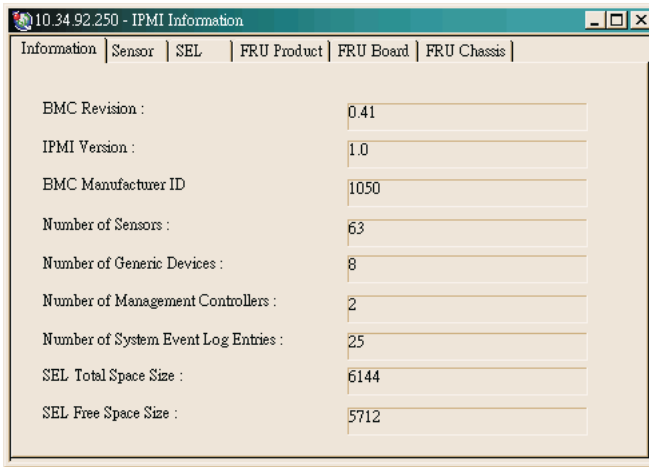
The RDM status is monitored through the hardware module of the server. If the server does not have RDM status detecting capability, the status is "Unknown." The status is "Active" if you have RDM installed in your systems. The status is "Not Exist" if your server does not have the RDM module installed.

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).

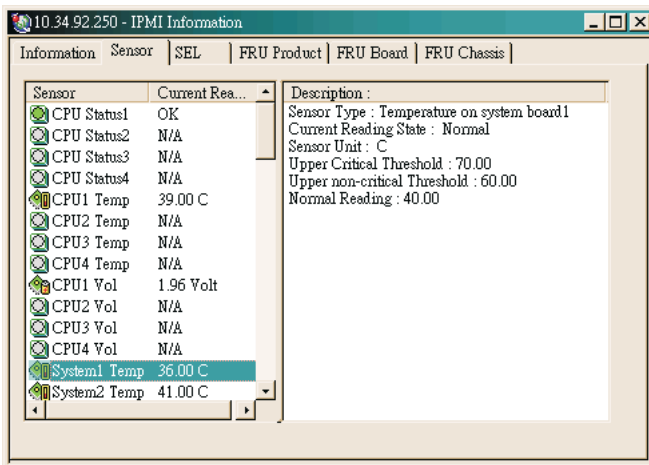
Information

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.



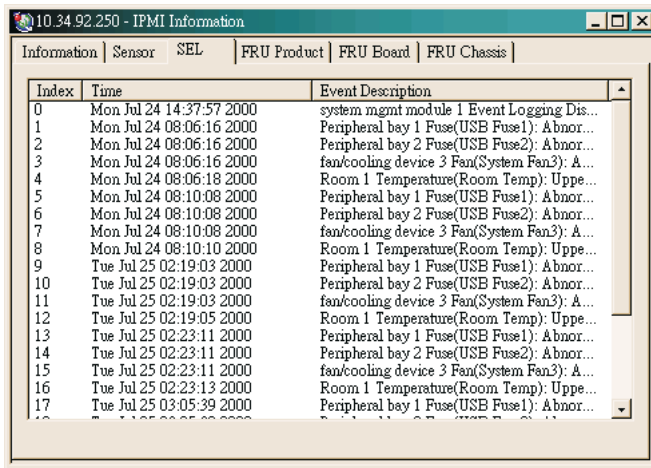
SensorFRU

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.



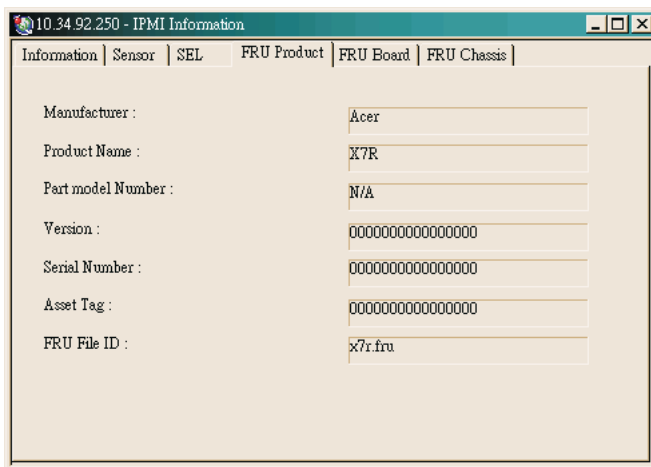
10.34.92.250 - IPMI Information

Information | Sensor | SEL | FRU Product | FRU Board | FRU Chassis

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.



10.34.92.250 - IPMI Information

Information | Sensor | SEL | FRU Product | FRU Board | FRU Chassis

Manufacturer :

Product Name :

Part model Number :

Version :

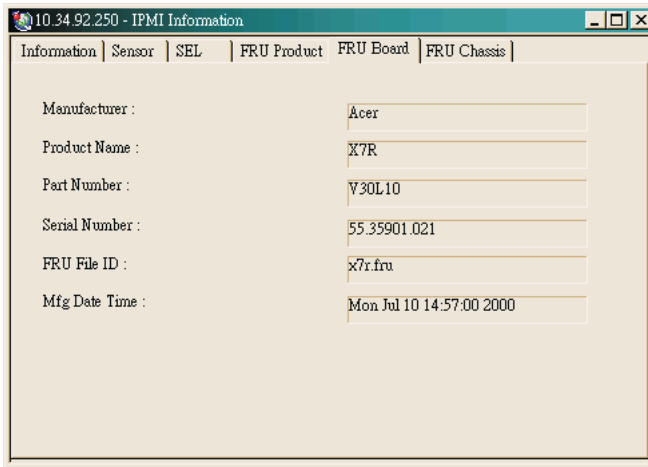
Serial Number :

Asset Tag :

FRU File ID :

FRU board

Field replaceable unit board displays motherboard information.

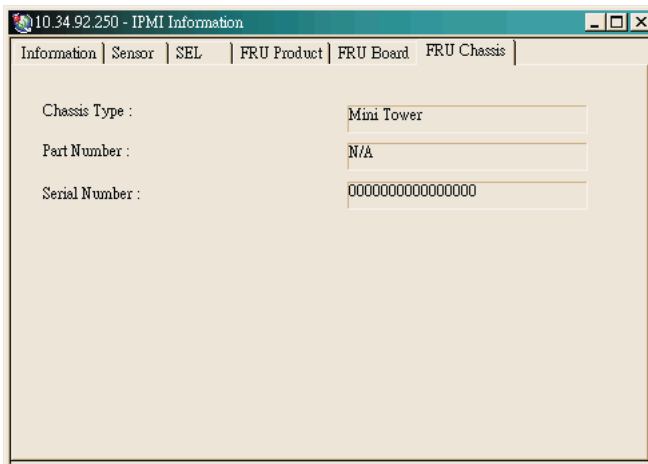


The screenshot shows a window titled "10.34.92.250 - IPMI Information" with a menu bar containing "Information", "Sensor", "SEL", "FRU Product", "FRU Board", and "FRU Chassis". The "FRU Product" tab is selected. The main area displays the following information:

Manufacturer :	Acer
Product Name :	X7R
Part Number :	V30L10
Serial Number :	55.35901.021
FRU File ID :	x7r.fru
Mfg Date Time :	Mon Jul 10 14:57:00 2000

FRU chassis

Field replaceable unit chassis displays chassis information.

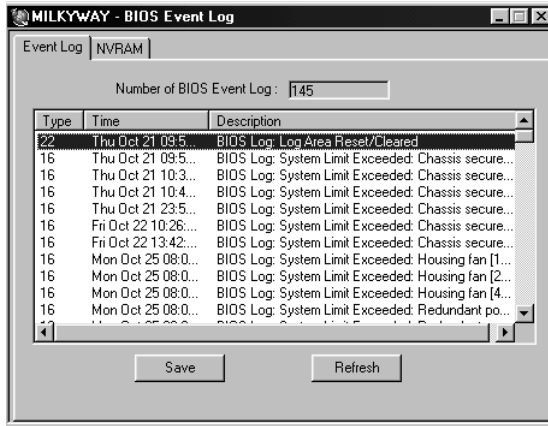


The screenshot shows the same window as above, but with the "FRU Chassis" tab selected. The main area displays the following information:

Chassis Type :	Mini Tower
Part Number :	N/A
Serial Number :	0000000000000000

BIOS event log

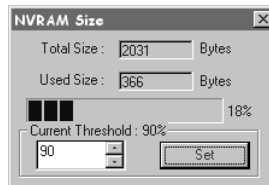
This dialog box appears when you select Information > Hardware Status > BIOS Event Log in the menu bar. It shows you the event log of the servers being monitored.



Note: Please refer to the user's manual for your main board for more information about BIOS Event Log.

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.

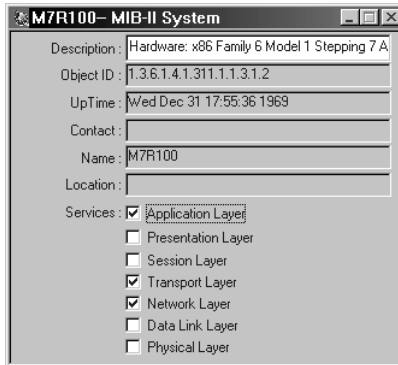
MIB-II information

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 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.



The screenshot shows a window titled "M7R100- MIB-II System". It contains the following fields and options:

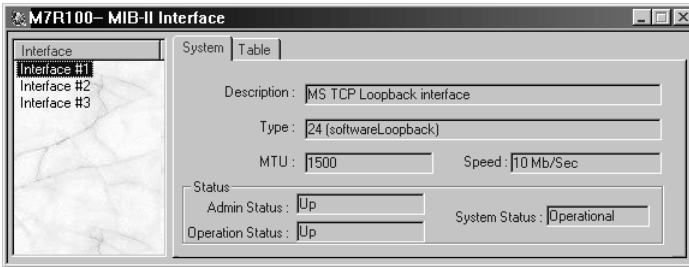
Description:	Hardware: x86 Family 6 Model 1 Stepping 7 A
Object ID:	1.3.6.1.4.1.311.1.1.3.1.2
UpTime:	Wed Dec 31 17:55:36 1969
Contact:	
Name:	M7R100
Location:	
Services:	<input checked="" type="checkbox"/> Application Layer <input type="checkbox"/> Presentation Layer <input type="checkbox"/> Session Layer <input checked="" type="checkbox"/> Transport Layer <input checked="" type="checkbox"/> Network Layer <input type="checkbox"/> Data Link Layer <input type="checkbox"/> Physical Layer

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

The screenshot shows a window titled "M7R100-MIB-II Interface" with a "Table" tab selected. On the left, a list of interfaces includes "Interface #1", "Interface #2", and "Interface #3". The main area displays a table of statistics for the selected interface:

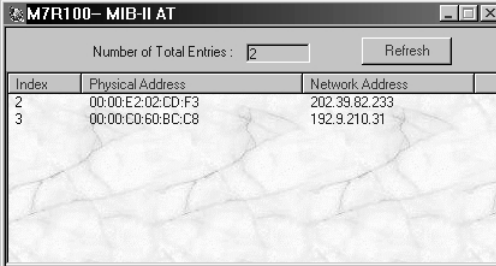
	Input	Output
Total Bytes :	11941	11941
Unicase Packets :	183	183
Non-unicast Packets :	0	0
Error Packets :	0 (0.00%)	0 (0.00%)
Discard Packets :	0 (0.00%)	0 (0.00%)

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". Below the title bar, there is a label "Number of Total Entries : 2" and a "Refresh" button. The main content is a table with three columns: "Index", "Physical Address", and "Network Address".

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

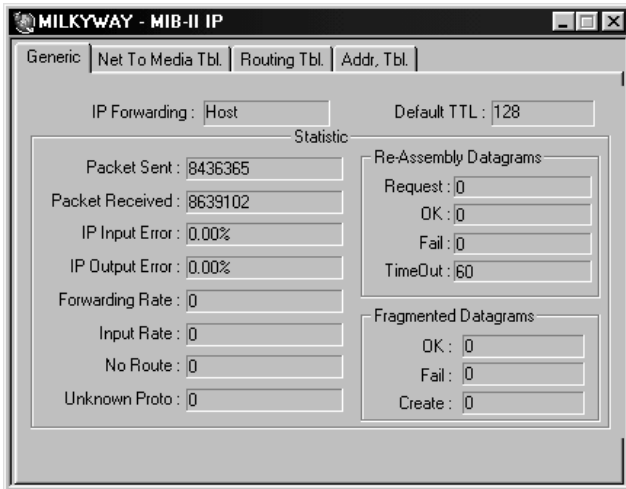
The Address Translation group contains one table which is the union across all interfaces of the translation tables for converting a NetworkAddress (e.g., an IP address) into a subnetwork-specific address. This document refers to such a subnetwork-specific address as a 'physical' address.

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



MILKYWAY - MIB-II IP

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

IP Forwarding : Host Default TTL : 128

Statistic

Packet Sent :	8436365	Re-Assembly Datagrams
Packet Received :	8639102	Request : 0
IP Input Error :	0.00%	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.

Number of Total Entries : 1 Refresh

Index	Physical Address	Network Address	Type
2	00:00:E2:04:83:58	100.100.100.101	dynamic

Routing table tab

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

Number of Total Entries : 6 Refresh

Destination	I...	Next Hop	Type	Proto...	Age	Net Mask
100.0.0.0	2	100.100.10...	direct	local	961...	255.0.0.0
100.100.100...	1	127.0.0.1	direct	local	961...	255.255.25...
100.255.255...	2	100.100.10...	direct	local	961...	255.255.25...
127.0.0.0	1	127.0.0.1	direct	local	961...	255.0.0.0
224.0.0.0	2	100.100.10...	direct	local	961...	224.0.0.0
255.255.255...	2	100.100.10...	direct	local	961...	255.255.25...

IP address table tab

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

The screenshot shows a window titled "MILKYWAY - MIB-II IP" with tabs for "Generic", "Net To Media Tbl", "Routing Tbl", and "Addr. Tbl". The "Addr. Tbl" tab is active. Below the tabs, there is a "Number of Total Entries" field set to "1" and a "Refresh" button. A table displays the IP address information:

Address	IF Index	Net Mask	Broadcast A...	Max. ...
100.100.100.100	2	255.0.0.0	1	65535

ICMP (Internet Control Message Protocol)

Implementation of the ICMP group is mandatory for all systems.

The screenshot shows a window titled "M7R100- MIB-II ICMP" with a table of ICMP statistics. The table has columns for "Input", "Output", and "Total".

	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 window titled "MILKYWAY - MIB-II TCP" with two tabs: "Generic" and "Table". The "Generic" tab is active and displays the following parameters in a form:

- Retrans. Alg.: vanj
- Retrans. timeout: 300 ms. < timeout < 240000 ms.
- Max. Conn.: Dynamic
- Current Conn.: 10
- Active Open: 34
- Passive Open: 59
- Received Seg.: 4245873
- Sent Seg.: 4042555

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.

MILKYWAY - MIB-II TCP

Generic Table

Number of Total Entries : 1 Refresh

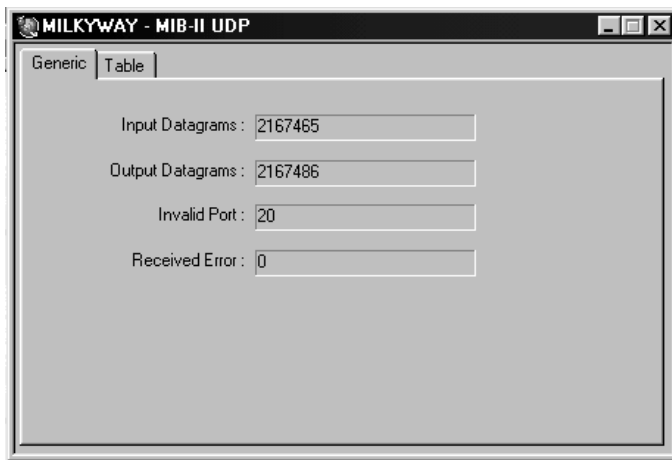
Status	Remote Addr.	Remote...	Local Addr.	Local Port
listen	0.0.0.0	135	0.0.0.0	18636

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 endpoints on which a local application is currently accepting datagrams.

Generic tab



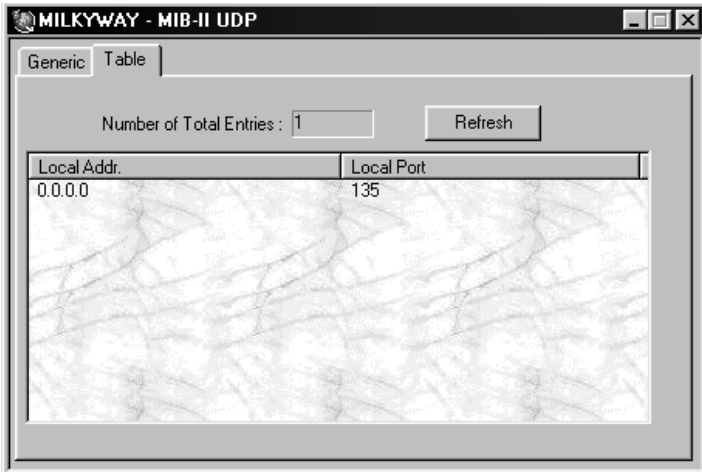
The screenshot shows a window titled "MILKYWAY - MIB-II UDP" with two tabs: "Generic" and "Table". The "Generic" tab is active and displays four statistics in a list format:

- Input Datagrams : 2167465
- Output Datagrams : 2167486
- Invalid Port : 20
- 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 endpoints 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.

Uninterruptible Power Supply (UPS)



Caution: The following must be present on the server for this feature to be operational:

- Built-in hardware support
- Agent software component; applies to all network operating systems that ASM supports

Agent supports a UPS feature, if one is built-in to the server hardware. This feature ensures a graceful system shutdown in the event of an AC power failure. A battery backup maintains power for a short time. This allows users to save their data and log off the system.

UPS is a very important server feature, because most servers have critical data files stored online that are constantly being modified. If these changes are not saved or the file system becomes damaged, users may lose a substantial amount of work.

If an AC power failure occurs, Agent detects it automatically and broadcasts a message to all users logged on to the server, notifying them that they must save their data and log off the system. Agent broadcasts the first message two minutes before it shuts down the server; it broadcasts a second message one minute before it shuts down the server. One minute after it broadcasts the second message, Agent synchronizes all file systems and performs an orderly system shutdown.

The UPS feature distinguishes a power failure from a spike in the power source. When AC power is interrupted, the UPS immediately activates the battery backup. Agent broadcasts the two-minute warning only after a power failure that has lasted for 30 seconds. So, two minutes and 30 seconds elapse between AC power failure and automatic system shutdown.

UPS information

ASM automatically detects UPS hardware that is built-in to the server, and monitors the following four UPS-related components:

- AC power
- UPS fan
- UPS power supply (a maximum of three power supplies are supported, as indicated by the three icons in the following figure)
- UPS battery

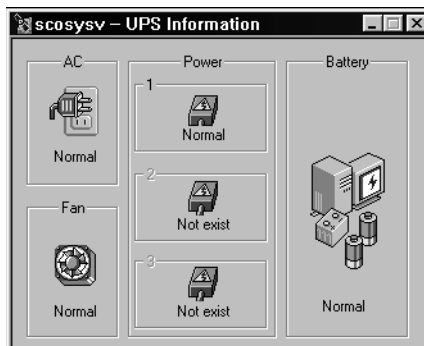
If the server has built-in UPS hardware, selecting Information > Device displays the UPS Information window shown below.



.....
Note: If the Device submenu is grayed out, ASM does not detect the presence of UPS hardware in the server.

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

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



► Fault management

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

The ASM 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.

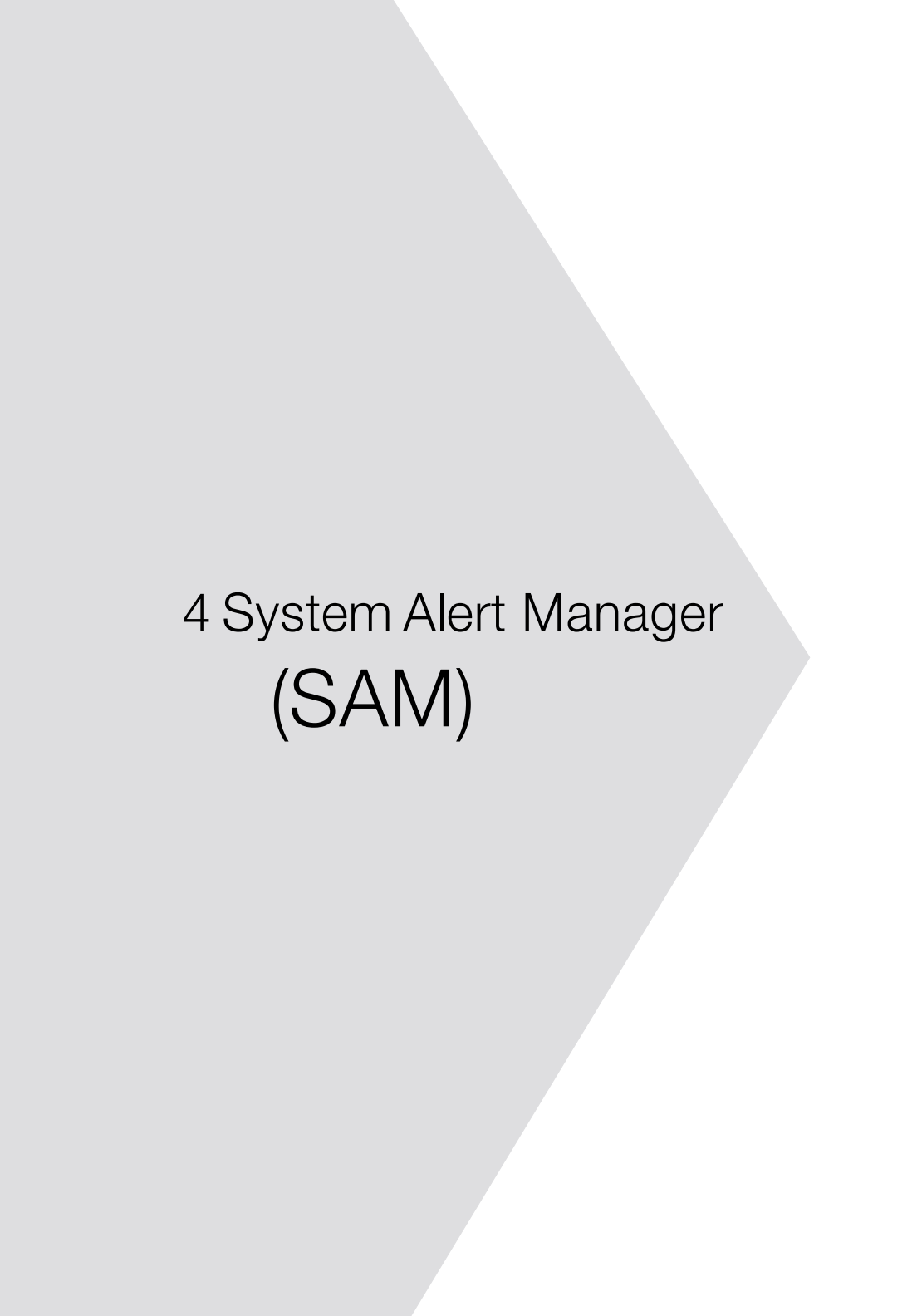
An example of non-configurable threshold values is the internally-preset temperature warning and temperature critical. For example, the manufacturer-suggested threshold value for some types of Pentium processors is between 131°F - 167°F (55°C - 75°C). (131°F (55°C) is the temperature warning threshold; 167°F (75°C) is the temperature critical threshold. ASM 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 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.

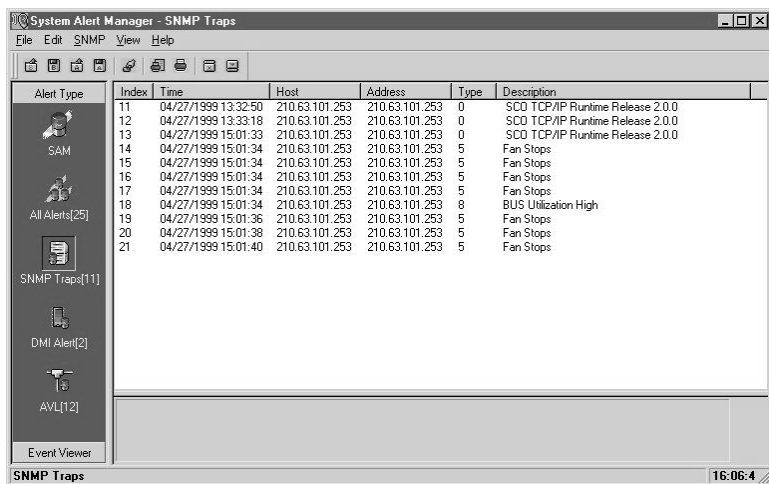
There are three types of alerts associated with the Console:

- 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.



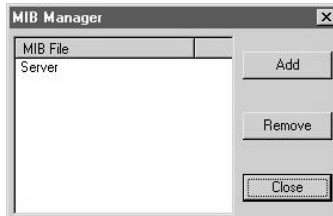
The screenshot shows the 'System Alert Manager - SNMP Traps' application window. The window title bar includes 'File', 'Edit', 'SNMP', 'View', and 'Help' menus. Below the title bar is a toolbar with various icons. On the left side, there is a navigation panel with icons for 'Alert Type', 'SAM', 'All Alerts[25]', 'SNMP Traps[11]', 'DMI Alert[2]', and 'AVL[12]'. The main area displays a table with the following data:

Index	Time	Host	Address	Type	Description
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

The status bar at the bottom of the window shows 'SNMP Traps' on the left and '16:06:4' on the right.

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

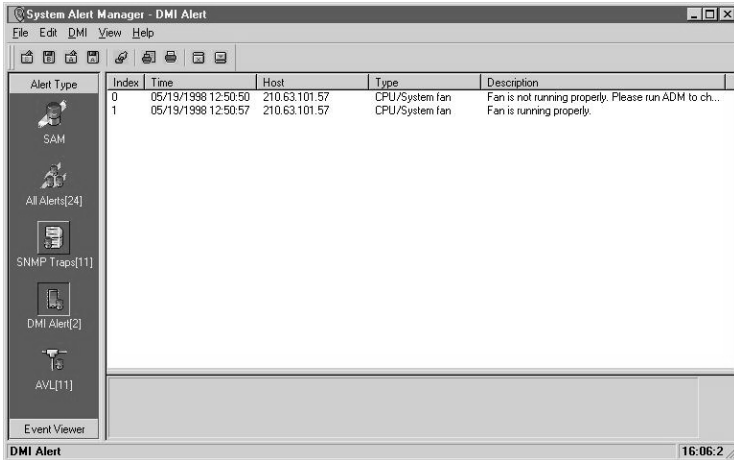
The following event types are listed in the Event Handler window.

Type.	Description
0	Trap Other than ASM
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	
12	UPS Power Supply Fail
13	UPS AC Power Fail
14	UPS Power Supply Fan Fail
15	UPS Battery Fail
16	Chassis Intrusion
17	Fuse Fail
18	Redundant Power Supply Fail
19	Redundant Power Supply Fan Fail
20	BIOS Event Log

Type.	Description
21	BIOS Event Log Utilization High
22	CPU Abnormal
23	Asset Change

DMI indications

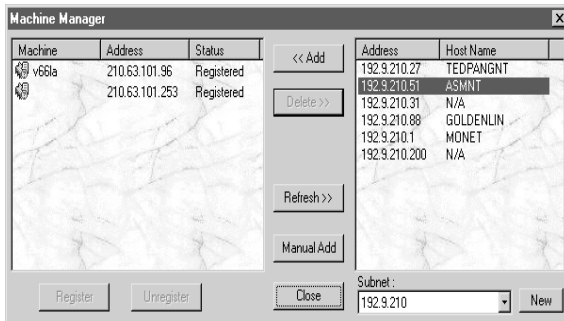
DMI indications are generated by systems that use DMI (Desktop Management Interface) to report devices that are not working properly. To view DMI alerts, select View > DMI or click the DMI icon in the navigation panel. The DMI indication log displays.



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

Item	Description
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.

The screenshot shows the 'System Alert Manager - AVL' window. On the left is a sidebar with 'Alert Type' categories: SAM, All Alerts[19], SNMP Traps[11], DMI Alert[2], and AVL[6]. The main area is a table with columns: Index, Time, Host, and Description.

Index	Time	Host	Description
0	04/27/1999 16:04:00	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	Register
1	04/27/1999 16:04:01	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
1	04/27/1999 16:04:01	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
2	04/27/1999 16:04:16	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
2	04/27/1999 16:04:16	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
3	04/27/1999 16:04:16	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
3	04/27/1999 16:04:31	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
3	04/27/1999 16:04:31	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
4	04/27/1999 16:04:47	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
4	04/27/1999 16:04:47	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
4	04/27/1999 16:04:47	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event
5	04/27/1999 16:05:03	ALERTONLAN:bb687620-ae5d-11ce-be25-0000e2205967	LAN Leash Tamper Event

The status bar at the bottom shows 'AVL' and the time '16:05:00'.

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

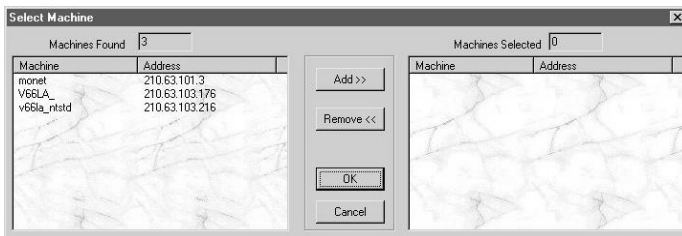
Event Viewer gathers information about events in the system being monitored by the ASM Console. This information is saved in the event log file for future reference.

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 screenshot shows the System Alert Manager (SAM) interface for the system 'scosysv.192.9.210.18'. The main window displays a list of events with columns for Server Name, Type, Event Group, Occurring Time, and Description. Below the list is a summary table with columns for Server Name, Address, Count, and Percent. To the right of the summary table is a 'Brms Statistics' pie chart showing 100.0% for the system 'scosysv.192.9.210.18'. The interface includes a menu bar (File, Edit, Operation, View, Help) and a toolbar with various icons. The status bar at the bottom shows the system name and the time 16:27:0.

Server Name	Type	Event Group	Occurring Time	Description
scosysv.192...	1006		Mon Apr 26 17:07:55 1999	Fan is not running properly. Please run ADM ...
scosysv.192...	1006		Mon Apr 26 17:07:57 1999	Fan is running properly.
scosysv.192...	1006		Mon Apr 26 17:08:46 1999	Fan is not running properly. Please run ADM ...
scosysv.192...	1006		Mon Apr 26 17:08:49 1999	Fan is running properly.
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:52 1999	HOUSING Fan stopped.
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:52 1999	HOUSING Fan stopped.
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:52 1999	HOUSING Fan stopped.
scosysv.192...	8	PCI BUS Util...	Wed Apr 28 04:06:52 1999	Bus #1 utilization 0.53% exceeds threshold 0...
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:54 1999	HOUSING Fan stopped.
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:55 1999	HOUSING Fan stopped.
scosysv.192...	5	Fan Stops	Wed Apr 28 04:06:58 1999	HOUSING Fan stopped.

Server Name	Address	Count	Percent
scosysv.192...	210.63.101...	12	100.00

Brms Statistics

100.0%

scosysv.192.9.210.18

Pie Bar 2D 3D

By Server By Type By Event Group

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.

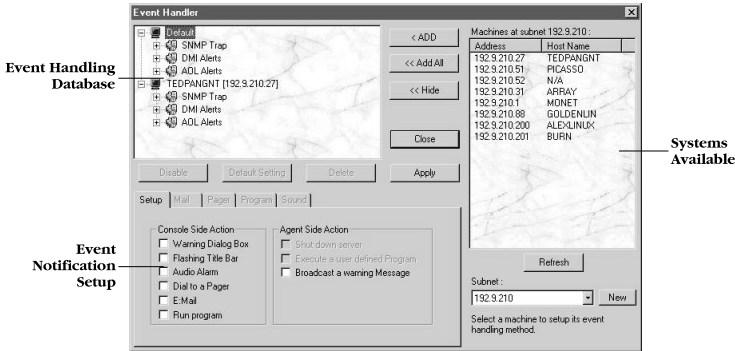
Event Type	Description
Trap Other Than ASM	When trap that is not listed in the ASM event-type listing occurs, ASM Agent sends a trap to Console
System Up/Down	<p>The server has been booted or shut down. Agent sends a trap to Console every time this occurs. Console notifies the system administrator by 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). Agent broadcasts a “Temperature Warning” message to all users on the server. 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. 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. 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 4 - ASM 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	PCI bus utilization has exceeded the threshold setting. Agent sends a trap. Rearrange your PCI add-in components to even out bandwidth distribution, if possible
AC Power Fails	AC power to the server has failed. Agent sends a broadcast and a trap, then shuts down the server
Chassis Intrusion	The server cover is open. Agent sends a broadcast and a trap
Fuse Fail	The keyboard/mouse, USB, or SCSI fuse has failed. Agent sends a broadcast and a trap
Redundant Power Supply Fail	The server's redundant power supply has failed. Agent sends a broadcast and a trap
Redundant Power Supply Fan Fail	The server's redundant power supply fan has failed. Agent sends a trap. How Console handles the trap is determined by the event notification method selected by the system administrator in the Event Notification Setup screen
BIOS Event Log	The BIOS has detected hardware and has saved the information to its event log in NVRAM. Agent sends a trap
BIOS Event Log High	BIOS Event Log utilization has exceeded the threshold setting. Agent sends a trap
CPU Abnormal	The BIOS has detected an internal CPU error. Agent sends a trap
Asset Change	An asset has changed, for example, a disk has been added, removed, or replaced. Agent sends a trap

▶ 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.

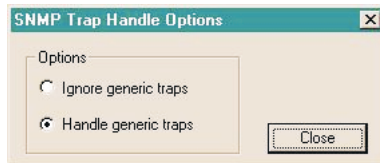
3. Click Close to save the changes.

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.

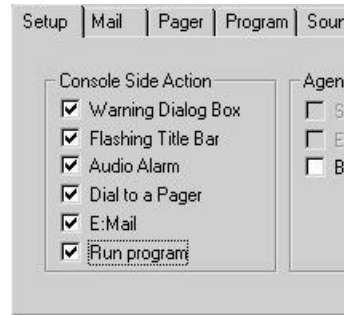


Note: When the checkbox in the Agent Side Action frame is grayed out it indicates that you can only enable this action at the agent side.

Event handling method

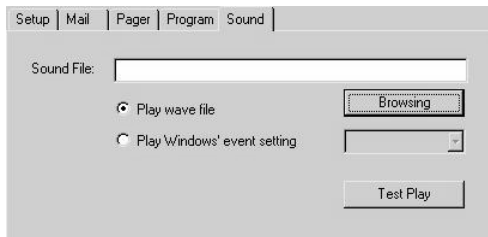
The following list describes the event handling methods and the function of each method. You can check and uncheck as many of these boxes as desired. A check in the box enables the function; removing a check disables the function. Use your mouse pointer to check and uncheck these boxes.

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 Console to take the action indicated in the checkbox.



Console side action

- The Warning Dialog Box appears on the ASM Console screen when the ASM System Agent sends a trap to the Console.
- The Flash Title Bar flashes on and off when the ASM System Console receives a trap.
- The Audio Alarm makes a sound whenever a trap is received from the ASM 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 System Agent sends a trap to the Console. Select the Pager tab from the Event Handler screen. The following display appears:



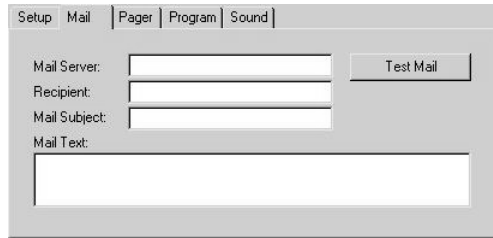
Note: Select the pager tab to set up a pager before marking the "Dial to a pager" trap action.

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 Console sends an email when the ASM 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.

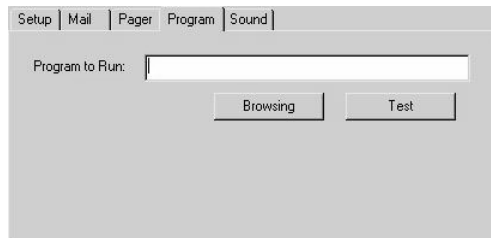


The screenshot shows the 'Mail' tab of the SAM configuration window. The window has a title bar with tabs for 'Setup', 'Mail', 'Pager', 'Program', and 'Sound'. The 'Mail' tab is selected. Below the title bar, there are four input fields: 'Mail Server:', 'Recipient:', 'Mail Subject:', and 'Mail Text:'. To the right of the 'Mail Server:' field is a 'Test Mail' button. The 'Mail Text:' field is a larger text area.



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.



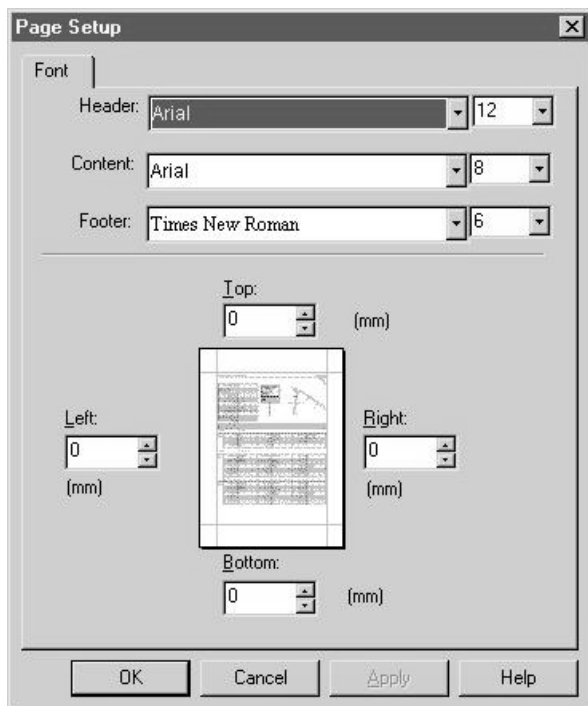
The screenshot shows the 'Program' tab of the SAM configuration window. The window has a title bar with tabs for 'Setup', 'Mail', 'Pager', 'Program', and 'Sound'. The 'Program' tab is selected. Below the title bar, there is a 'Program to Run:' label followed by a text input field. Below the input field are two buttons: 'Browsing' and 'Test'.



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 Server Agent utilities



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

The configuration utility for each operating system allows you to:

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



.....

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

ASM requires a password for the ASM Console and for each server agent. To launch the ASM console program, you need an ASM 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 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 Console to monitor the ASM Server Agent, the Console's IP address must be included in /etc/snmpd.trap on the server site.

In the following screen example, ASM 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 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 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 Console.

This function allows you to specify the type of action that ASM Agent takes when an event occurs. The ASM events that Agent traps are predefined in the ASM software. You can use the Event_Action function to define agent actions performed on the agent system. After ASM Console receives the trap it takes the action defined by the System Alert Manager or ASM 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 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 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 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

```

```

Current PCI Bus Utilization Threshold is 100

```

Event log

This item allows you to view or clear the Trap Log. When any event occurs, the ASM 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 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 configuration file */usr/asm/asmsmuxd.conf*.
5. In the menu select File > Exit to quit from the ASM Configuration Utility.



.....

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

In this form page the user can:

- Enable or disable the ASM password protection by selecting or unselecting the check mark in the square bracket. If the ASM password protection is enabled, the ASM Console will request the user to enter the ASM password each time when issuing an SNMP set command. (The default setting is Disabled.)
- Change the ASM 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 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 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)-----

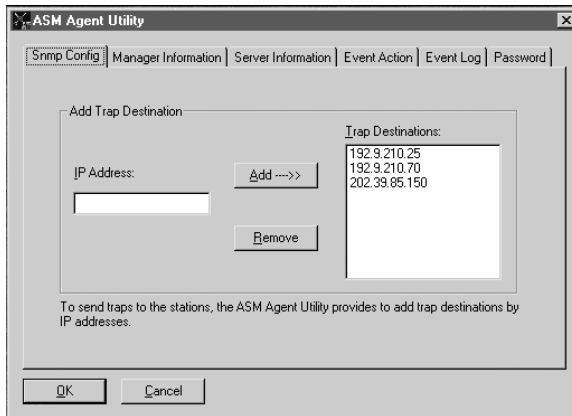
```


▶ asmcfg for Windows NT

The ASM configuration utility for Windows NT (asmcfg) is found in the ASM 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 Server Agent and ASM 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.

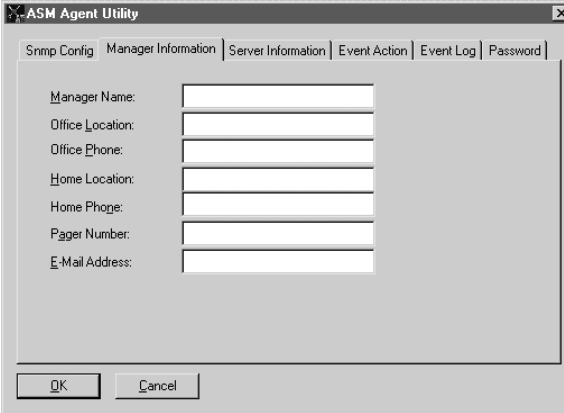
SNMP Config

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

To add an IP address to the trap list, type in the IP address or ASM Console name and click on the Add button. To remove IP address(es) from the trap list, select the IP address or ASM 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 dialog box titled "ASM Agent Utility" with a tabbed interface. The "Manager Information" tab is selected. The dialog contains the following fields:

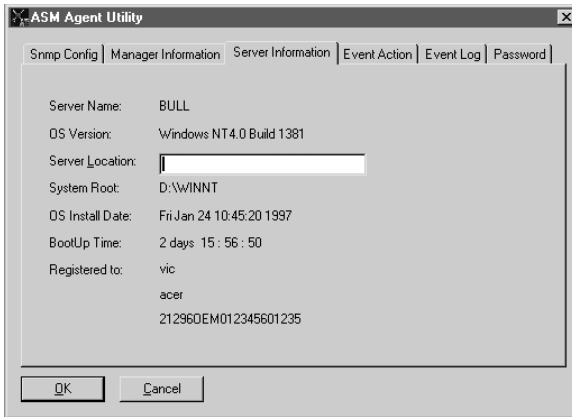
Manager Name:	<input type="text"/>
Office Location:	<input type="text"/>
Office Phone:	<input type="text"/>
Home Location:	<input type="text"/>
Home Phone:	<input type="text"/>
Pager Number:	<input type="text"/>
E-Mail Address:	<input type="text"/>

At the bottom of the dialog are "OK" and "Cancel" buttons.

The maximum number of characters allowed is 48 per field.

Server information

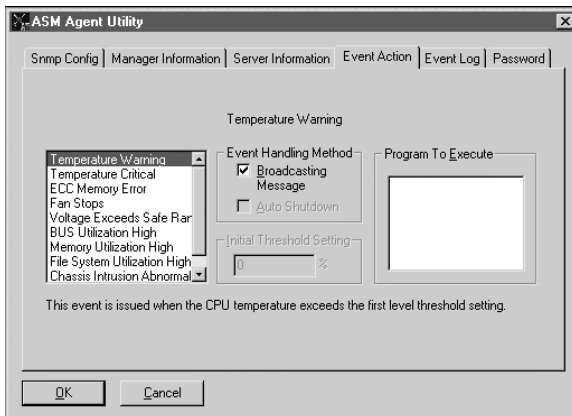
Click on the Server Information tab to change the server location. This tab describes basic server data. You can also view this tab through ASM Console > Server Information > Basic Information. This screen also allows you to specify the ASM server agent location so that you can track it when you need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



The maximum number of characters allowed is 48.

Event action

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



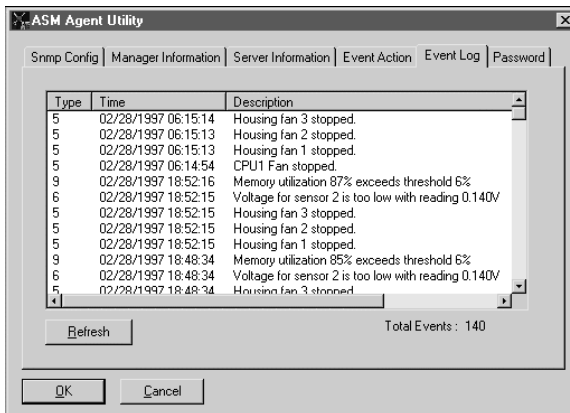
A number of events are defined in ASM. You can define the agent action (broadcast message or shutdown), the threshold setting, and the user-defined program to be executed by the server agent when the trap occurs.

ASM 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 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:

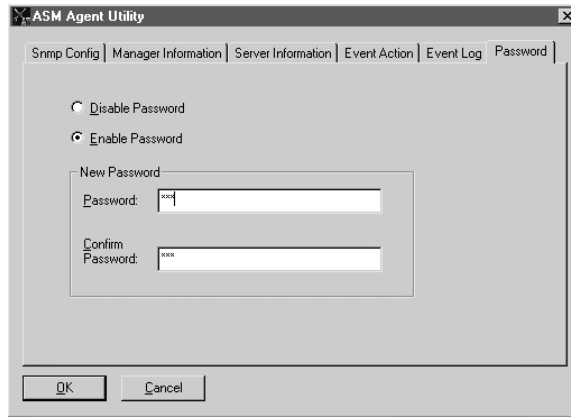


This screen shows the Event Log list. It contains all of the traps generated in the server system. You can view all of the ASM events from the day you installed the ASM server agent.

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 Server Agent does not execute password checking when the threshold is set by the ASM Console.



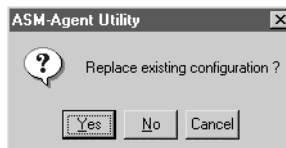
.....

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

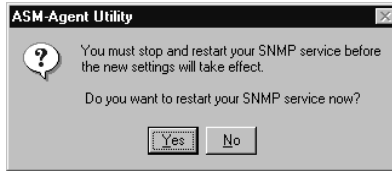
ASM server agent has password protection for setting values. If you want to change threshold values, manager contact information or server location, the ASM Console asks you to enter the ASM Server Agent's password.

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 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 has password protection for setting threshold values. When changing a threshold value from the ASM Console, it asks you to enter the password for the ASM Server Agent. If you disable the password, the ASM 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.



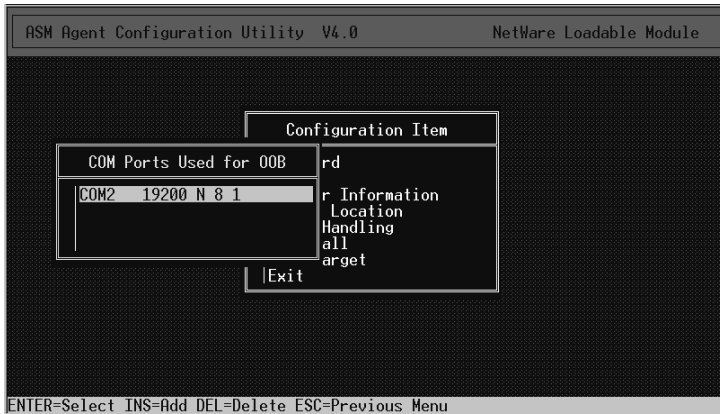
To change the password:

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 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 Server Agent and the ASM 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 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:

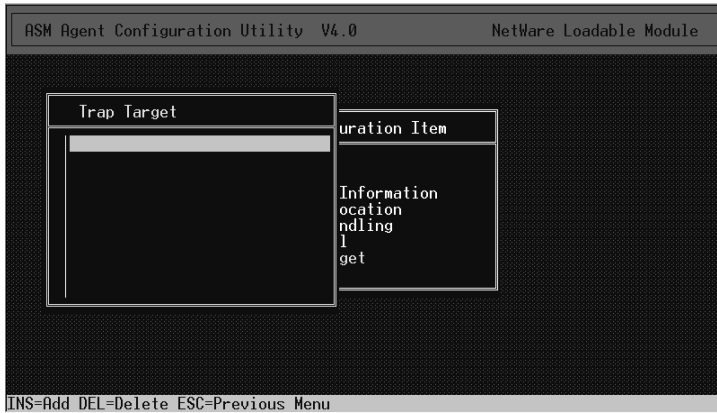
Broadcast - sends a messages to all users logged in to the network.

Shutdown - Shuts down the network operating system.

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

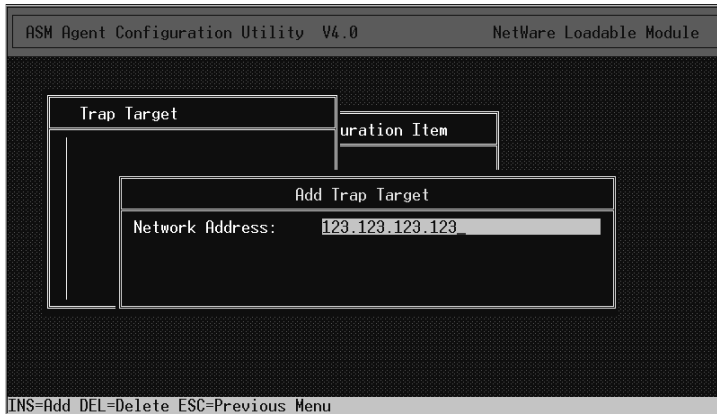
Trap target

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



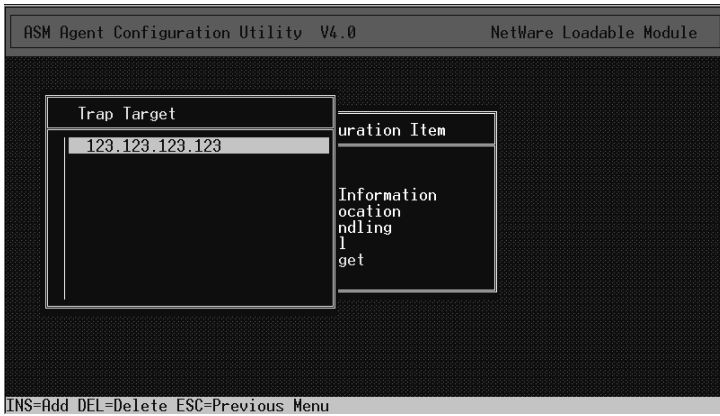
To add an IP address to the trap list:

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.

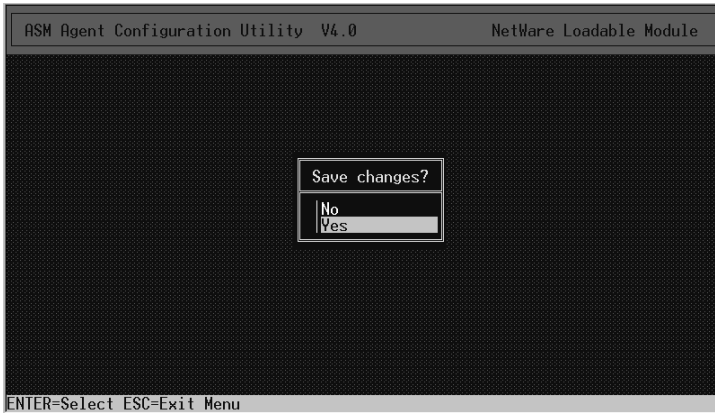


Saving changes in asmcfg

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



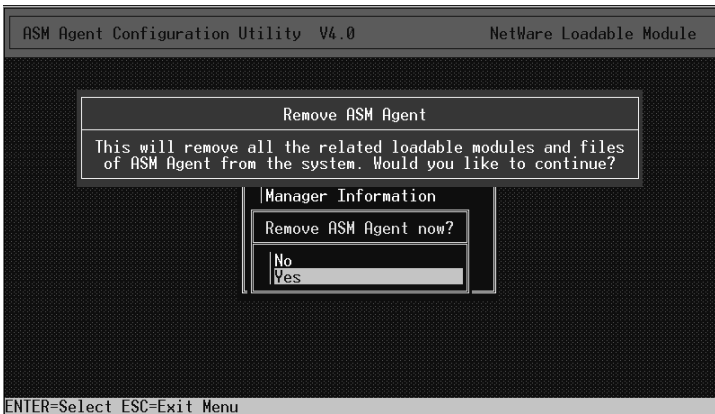
To exit asmcfg, select Yes. If you choose to exit asmcfg, the following dialog box displays:



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

Uninstalling ASM server agent

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



In the following screen example, ASM agent sent event traps for three monitoring systems: 10.34.155.205 and 10.34.155.250.

```
SNMP Config Manager_Info Event_Action Password Threshold Event_Log Quit
|-----|
| trapsink 10.34.155.205 |
| trapsink 10.34.155.250 |
|-----|
| [ 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 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 Address   :
| Home Phone       :
| Home Address     :
| Pager Number     :
| Email Address    :
| Server Location  :
+-----+
| Use arrow key and edit.....
+-----+

```

Event action

One of the most important functions performed by ASM 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 Console.

This function allows you to specify the type of action that ASM Agent takes when an event occurs. The ASM events that Agent traps are predefined in the ASM software. You can use the Event_Action function to define agent actions performed on the agent system. After ASM Console receives the trap it takes the action defined by the System Alert Manager or ASM 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.

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 Server Agent does not execute password checking when the threshold is set from the Console.

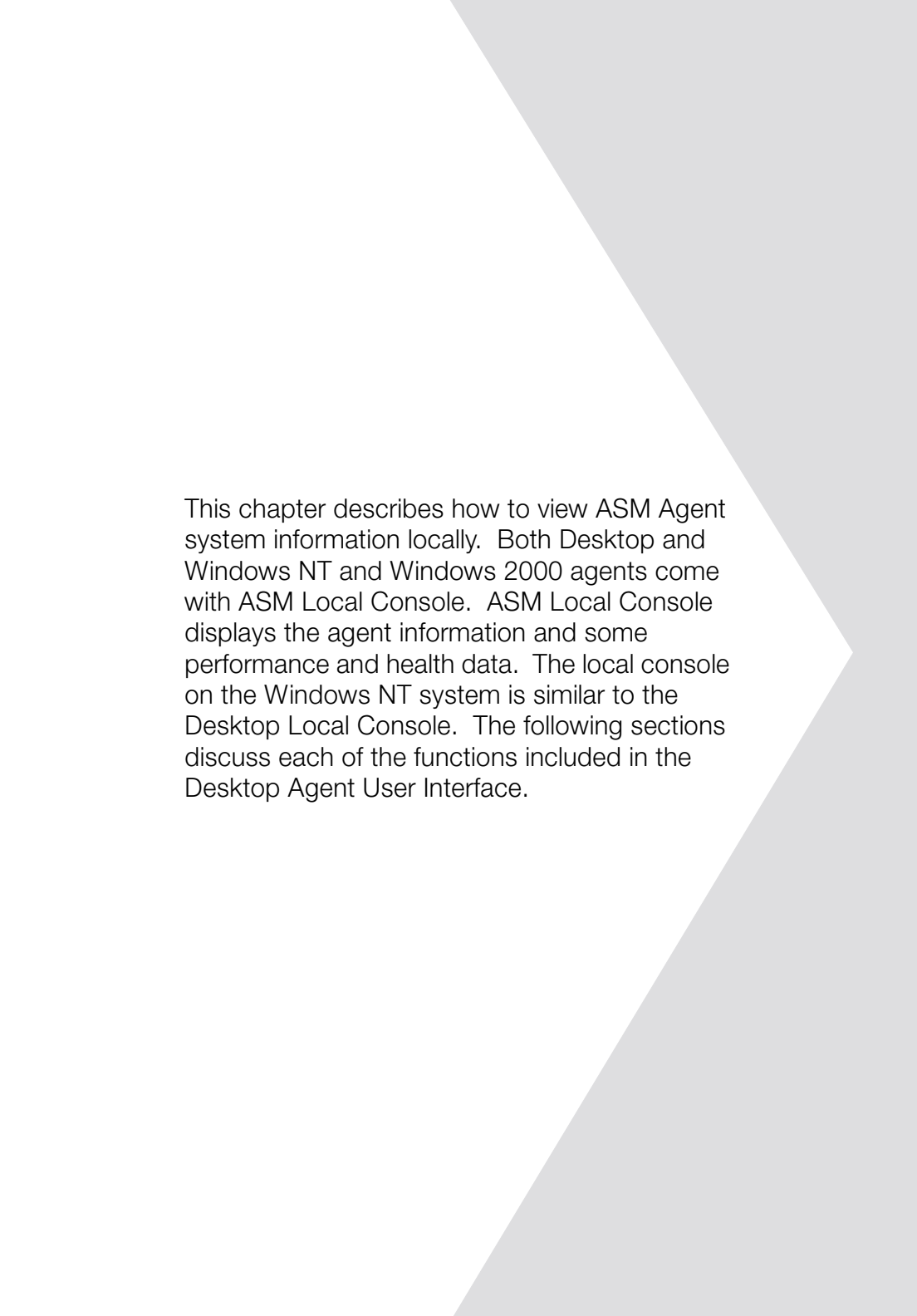


Caution: If the password feature is disabled, the server has NO SECURITY protection.

ASM 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 Server Agent's password.



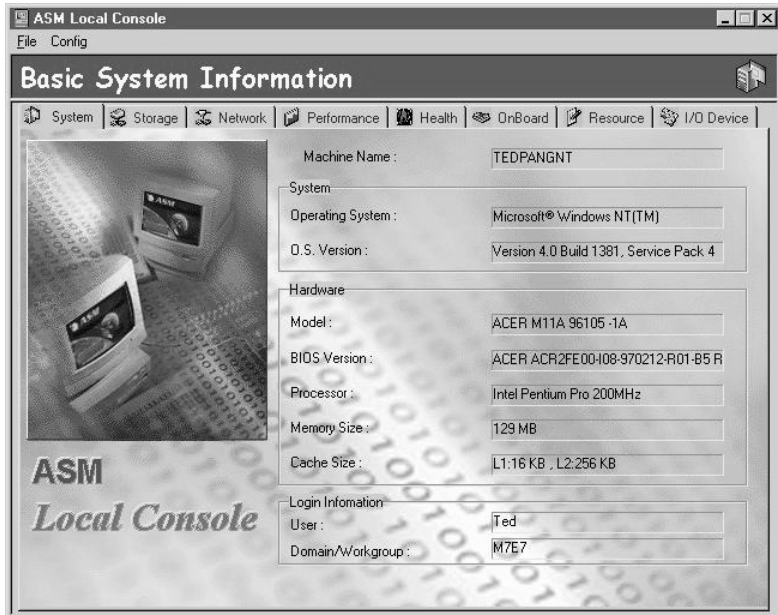
6 ASM Local
Console



This chapter describes how to view ASM Agent system information locally. Both Desktop and Windows NT and Windows 2000 agents come with ASM Local Console. ASM Local Console displays the agent information and some performance and health data. The local console on the Windows NT system is similar to the Desktop Local Console. The following sections discuss each of the functions included in the Desktop Agent User Interface.

► 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 three sections: the display window, the pie chart, 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.
4. Click on the logical drive to display more partition information and the usage pie chart.



The information section displays the following:

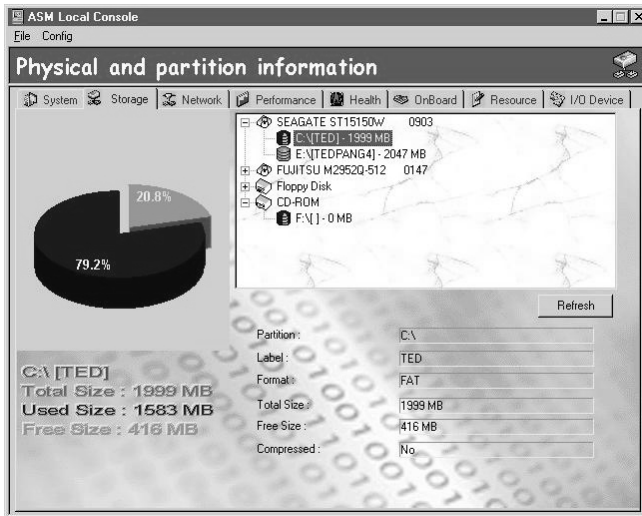
Parameter	Description
Type	Type of storage device (i.e., hard disk, cd-rom, etc.)
Model	Model name of the storage device
Interface	Type of interface the storage device uses (i.e., SCSI, IDE, etc.)
Device ID:LUN	Device ID and LUN (Logical Unit Number) of physical devices. ID number is 0 or 1 for IDE (Integrated Drive Electronics) interface devices, while 0 to 7 is for SCSI (Small Computer System Interface) devices. 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.
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

Accessing partition information

Logical partitions are created when you divide a hard disk into several parts and specify each of them as an independent logical drive.

To access logical partition information:

1. Click the plus (+) sign, or double-click on a physical device to see its logical partitions.
2. Click the partition you want to view.
3. Click the Refresh button to display the most current device setup.

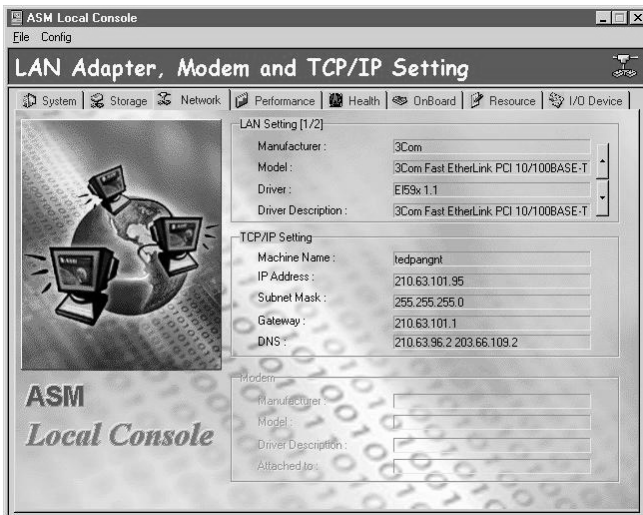


The pie chart shows the total space and the free and used space of the partition. The information section displays the following:

Parameter	Description
Partition	Displays the logical drive name for the partition.
Label	Partition label
Format	Format type of the partition (FAT or NTFS) File system format
Total Size	Total capacity of the partition in MB
Free Size	Amount of unused space in MB
Compressed	Shows if the partition is compressed or not

▶ 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

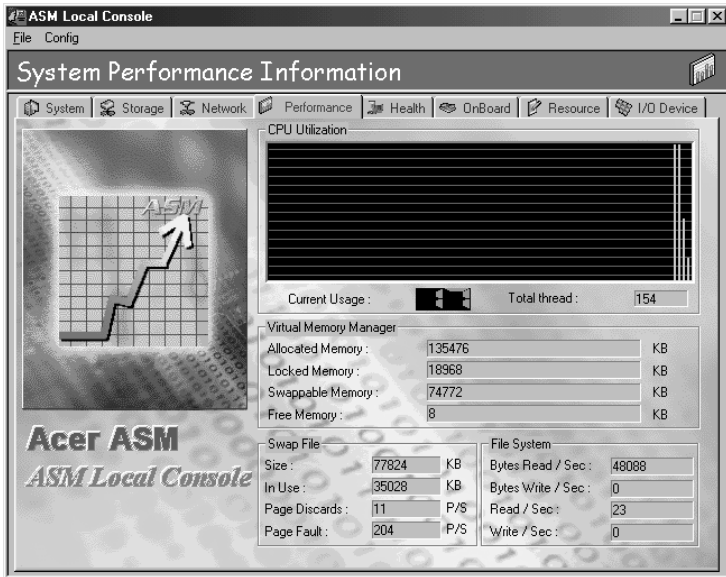
Modem

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.

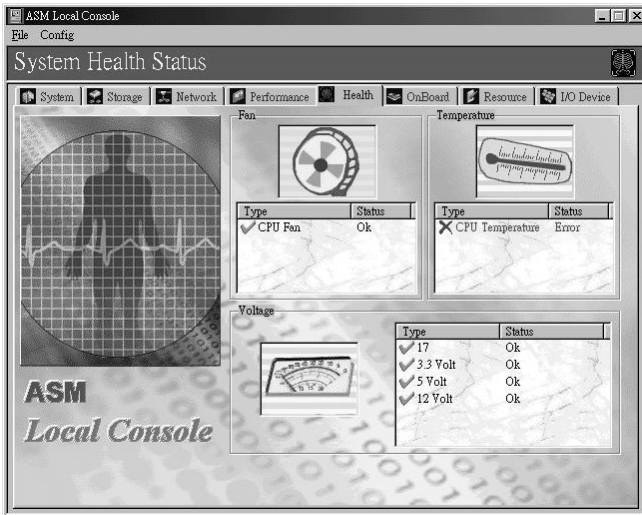
Parameter	Description
Bytes Read/Sec	Speed at which the system can read files
Bytes Write/Sec	Speed at which the system can write files

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

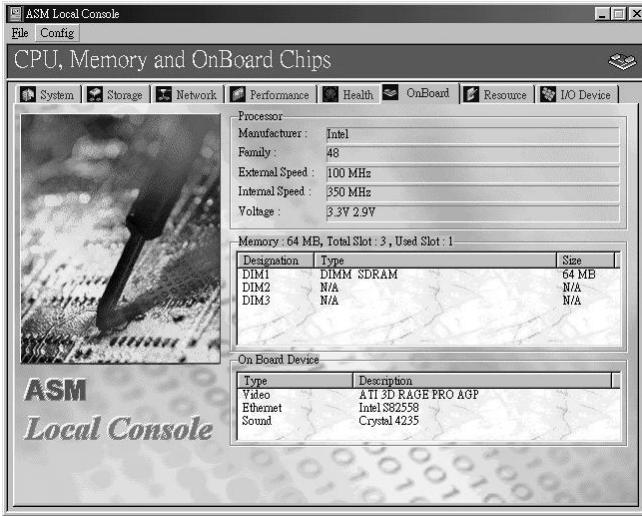
This section displays the CPU's temperature. Temperature status is monitored through the hardware module of the desktop. The green check icon indicates that the CPU temperature is normal while the red X mark icon indicates that the temperature exceeds the normal threshold.

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.

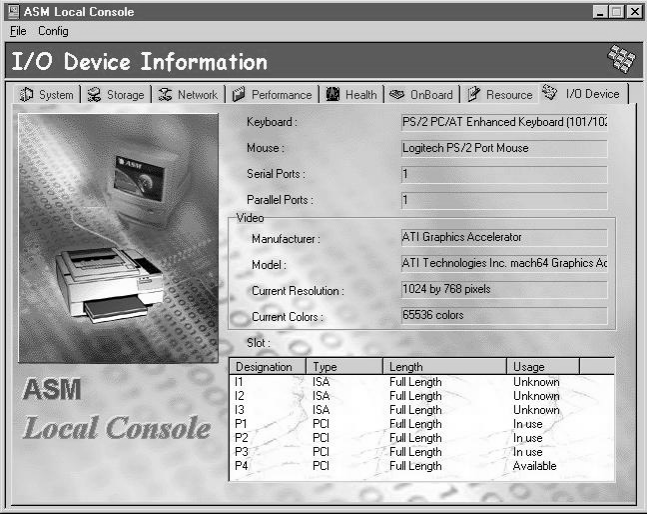


The screenshot shows the 'ASM Local Console' window with the 'System Resource' tab selected. The window title bar includes 'File' and 'Config' menus. Below the title bar is a navigation bar with icons for System, Storage, Network, Performance, Health, OnBoard, Resource, and I/O Device. The main content area displays a table of system resources. To the left of the table is a graphic showing computer monitors on a grid of binary code, with the text 'ASM Local Console' below it.

Device Name	IRQ	DMA	I/O Port	Memory Addr.
8042prt	01,12	none	0060-0060,00...	none
Serial	04	none	03F8-03FE	none
ASM	none	none	04F2-04F3	none
DC21X4	03	none	7080-70FF	none
E153x	05	none	7000-701F	none
Floppy	06	02	03F0-03F5,03...	none
ac78x	11	none	7400-74FF	0B100000-0B100FFF
elapi	15	none	0170-0177,03...	none
VgaSave	none	none	03B0-03B8,03...	000A0000-000BFFFF

► 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.



ASM Local Console
File Config

I/O Device Information

System Storage Network Performance Health OnBoard Resource I/O Device

Keyboard : PS/2 PC/AT Enhanced Keyboard (101/102)

Mouse : Logitech PS/2 Port Mouse

Serial Ports : 1

Parallel Ports : 1

Video

Manufacturer : ATI Graphics Accelerator

Model : ATI Technologies Inc. mach64 Graphics Ac

Current Resolution : 1024 by 768 pixels

Current Colors : 65536 colors

Slot :

Designation	Type	Length	Usage
I1	ISA	Full Length	Unknown
I2	ISA	Full Length	Unknown
I3	ISA	Full Length	Unknown
P1	PCI	Full Length	In use
P2	PCI	Full Length	In use
P3	PCI	Full Length	In use
P4	PCI	Full Length	Available

ASM
Local Console

7 ASM MIB

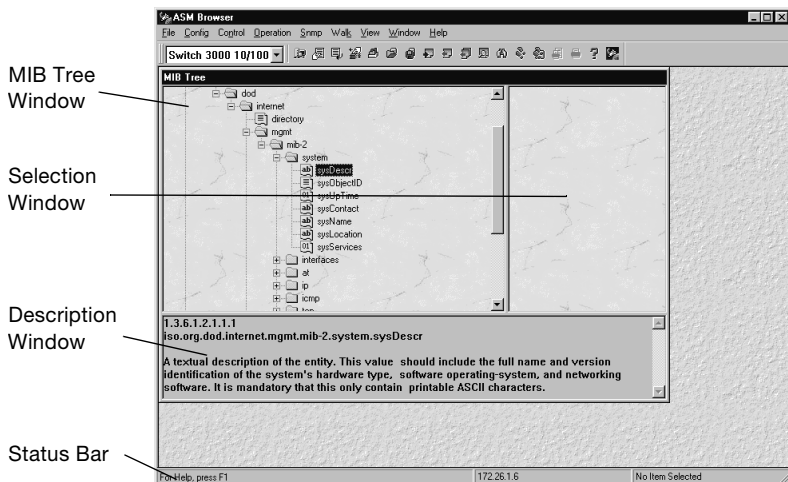
Browser

ASM MIB Browser is a MIB (Management Information Base) file browsing tool. It is an add-on utility available with the ASM package. ASM 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 MIB Browser

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

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



► User interface

The ASM 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 MIB Browser, the main screen displays the information from your last ASM 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 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 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 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 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 MIB Browser Help, displaying the Index screen
About		Displays ASM MIB Browser product information

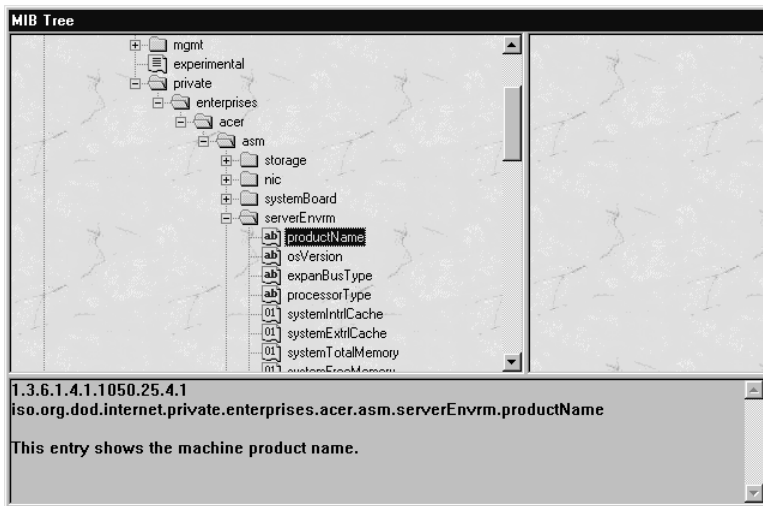
MIB tree window

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 MIB Browser gets its value and shows it in the Description Window.

MIB tree



ASM MIB information is located under:

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

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

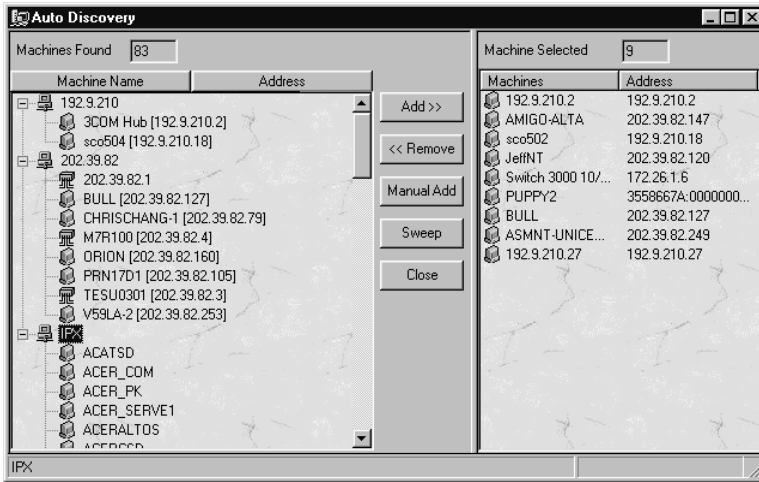
This section tells you how to perform the following tasks:

- 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 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 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 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.

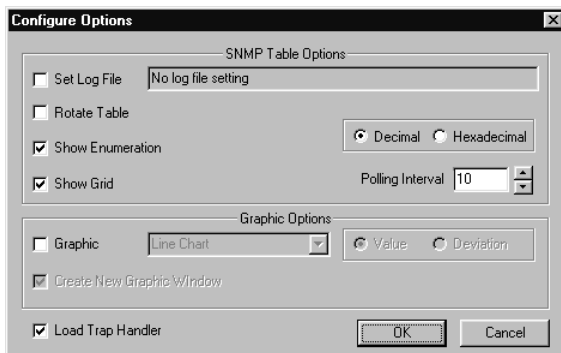
Item	Description
Sweep	Searches an address by matching the first three parts of the IP Address that you specify
Refresh	Searches the subnet that is currently in the Auto Discovery database.
Close	Closes the dialog box and causes the modifications you made to take effect; the System List Combo Box now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

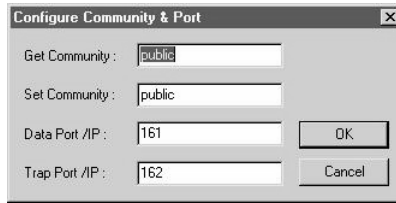


Configure timer dialog box items

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.

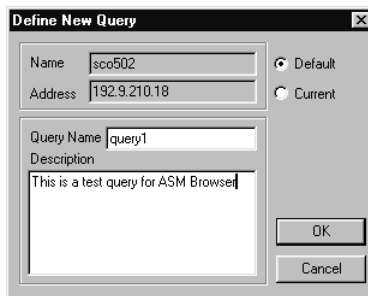


Defining a new query

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 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):

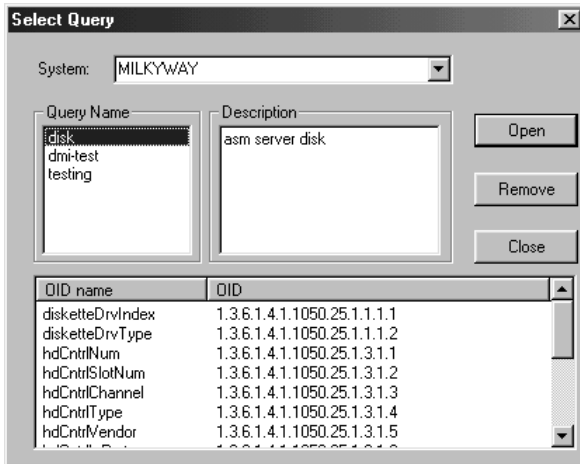
1. From the MIB tree window, select the OIDs you want to include in the query and add them to the Selection Window.
2. Select Control > Define New Query. The Define New Query dialog box displays.
3. Type a name and description for the query.
4. Click OK to accept it.



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

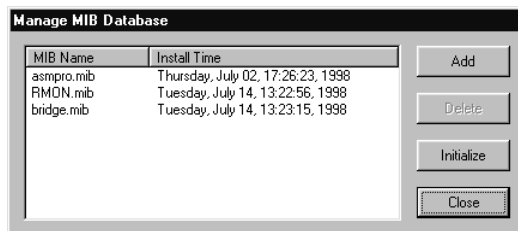
Item	Description
Button	Description
Open	Opens the selected query. A SNMP table appears.
Remove	Removes all queries in the database. This action takes effect only after clicking OK
Close	Closes the dialog box, discarding all changes made

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. ASMserver Agent uses a `asmnt.mib` file to describe its own object IDs. It is installed on the `asm` agent system. ASM 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.

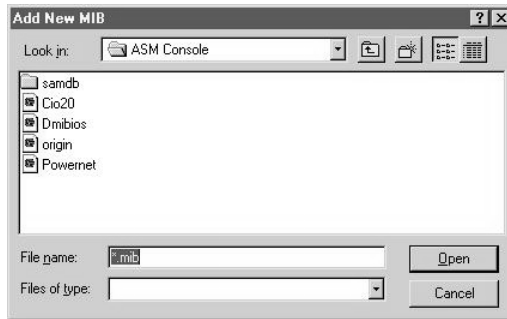
This dialog box prompts you to confirm whether or not to continue initializing the MIB database. To continue, click **OK**; otherwise, click **Cancel** to close this box without initializing.



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.

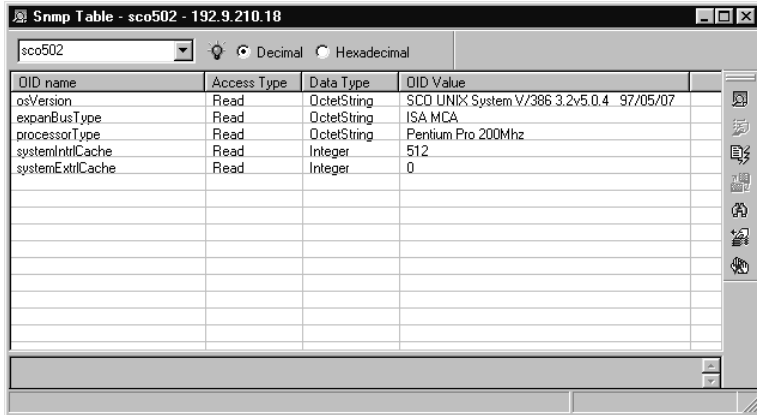
Browsing OIDs (SNMP table)

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.

- Select Operation > Browse or click the Browse button on the toolbar. The SNMP Table window appears displaying the OID values you selected.

To search for a particular OID, select Operation > Find or click the Find button on the toolbar and specify the OID to find.



OID name	Access Type	Data Type	OID Value
osVersion	Read	OctetString	SCO UNIX System V/386 3.2v5.0.4 97/05/07
expanBusType	Read	OctetString	ISA MCA
processorType	Read	OctetString	Pentium Pro 200Mhz
systemIntrCache	Read	Integer	512
systemExtrCache	Read	Integer	0



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

SNMP table (Simple Network Management Protocol)

SNMP table allows you to manage and view information about OIDs.

The toolbar at the right allows you to Get Value, Set Value, Poll, Rotate, Find, Configure Options for, and Stop OIDs in the table. The Browse button updates the contents of the OID Value table with the current OID values. Clicking the Stop button immediately stops the get value feature.

The Set button is enabled only when the SNMP Table is the active window and when the selected OID has the “write” attribute and can be modified. You can also record events in the log file by activating the log file entry.

There are 4 columns for each OID: OID name, Access Type, Data Type and OID Value.

- OID name - the OID label defined in the MIB file.

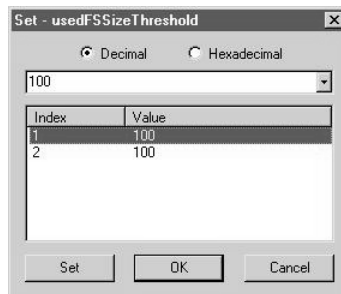
- Access Type - Read, Write, R/W or No Access for each OID, depending on the definition in the MIB file. Only an OID whose access type is R/W or Write can be set.
- Data Type - Integer, Unsigned Integer, Gauge, Counter, Counter64, TimerTick, OctetString, BitString, Network Address, IP Address, Opaque, 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.



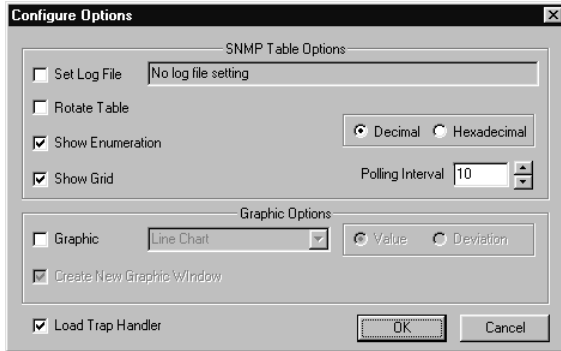
Decimal or hexadecimal

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	scounix
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

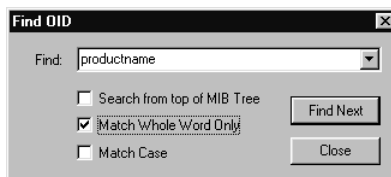
You can set the time interval for polling. The polling interval must be in the range from 1 to 60 seconds.

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.

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...	expandBusType.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...	systemExtrCache.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...	serverMgtName.0	Read	OctetString	

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.

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 MIF

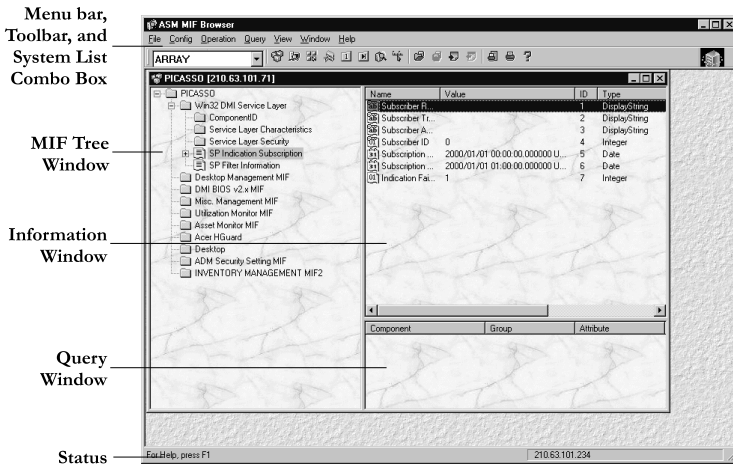
Browser

ASM MIF Browser is a MIF (Management Information Format) file browsing tool. It is an add-on available with the ASM 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 MIF Browser

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

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



► User interface

The ASM MIF Browser user interface allows you to move around easily and access information using menu commands or by clicking buttons. When you start ASM MIF Browser, the main screen displays the information from your last ASM 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 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 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 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 MIF Browser comes with a context-sensitive Help menu with the following items:

Command	Icon	Description
Help Topics		Starts ASM MIF Browser Help, displaying the Contents screen
About		Displays ASM MIF Browser product information

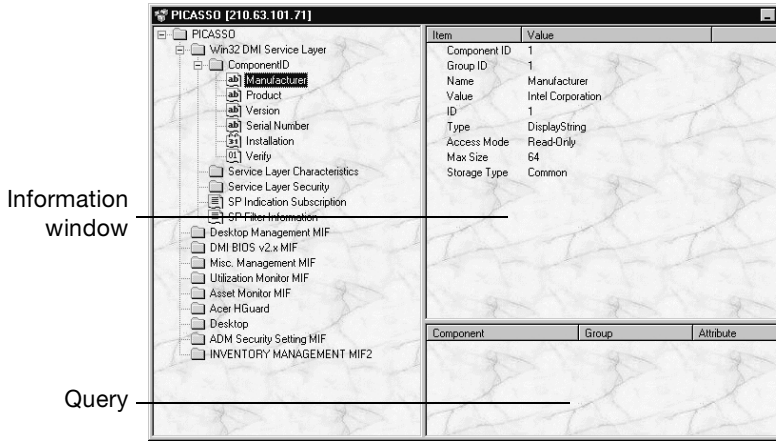
MIF tree window

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 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 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.

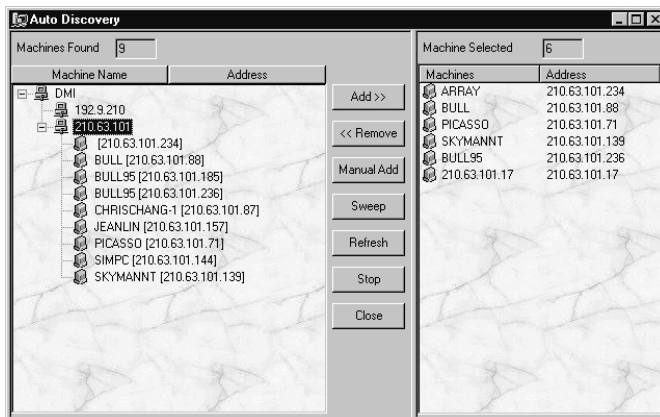
► Functions

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 MIF Browser.

The following items are available in this dialog box:

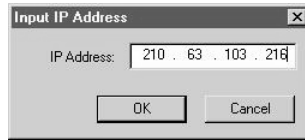
Item	Description
System Found	Displays all the DMI systems available on your network
System Selected	Shows all the systems to be monitored by ASM MIF Browser
Button	Description
Add	Appends the highlighted DMI systems in the System Found list to the System Selected list
Remove	Deletes the highlighted 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.

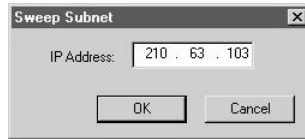
Manually adding a system

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

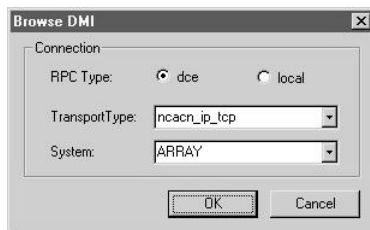
To sweep subnets, type the first three address blocks of the subnet and click OK. If the sweep finds a system in the subnet, it is displayed in the System List Combo box and MIF Tree window. If the sweep does not find anything, it displays a not found message.



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.

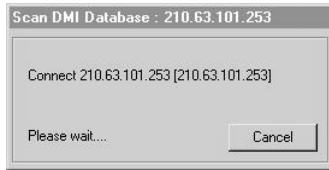
Select File > New to start a new connection. The Browse DMI window displays.



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.

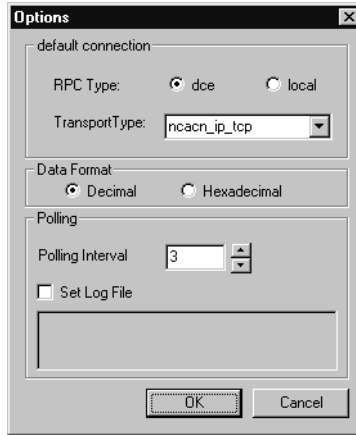


5. Click Cancel to stop the process.

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

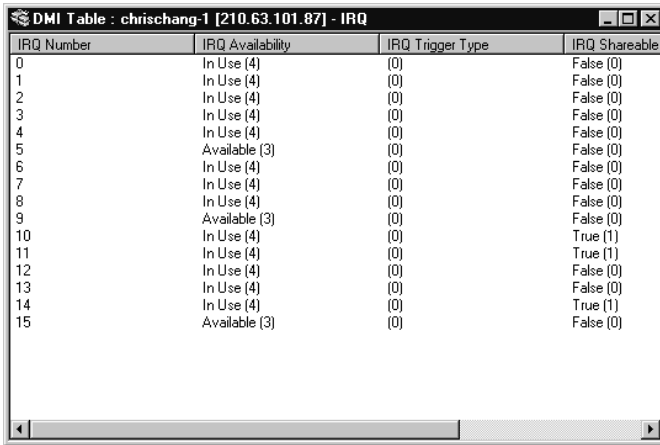
Browsing the DMI table

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.



The screenshot shows a window titled "DMI Table : chrischang-1 [210.63.101.87] - IRQ". The window contains a table with the following data:

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" (which is selected) and "Hexadecimal". Below the radio buttons is a dropdown menu with the text "ASM 4.0 Test" and a downward-pointing arrow. At the bottom of the dialog 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.

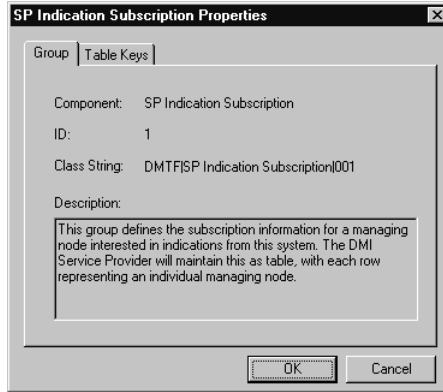
For date attributes

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 close button (X) in the top right corner. It is divided into two main sections: "Date" and "Time".
 The "Date" section has three input fields: "Year" (containing 1998), "Month" (containing 4), and "Day" (containing 22).
 The "Time" section has four input fields: "Hour" (containing 19), "Min" (containing 5), "Sec" (containing 11), and "Micro Sec" (containing 840000).
 Below the "Time" section is a "Timezone (Minutes)" input field containing -480.
 At the bottom of the dialog 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.

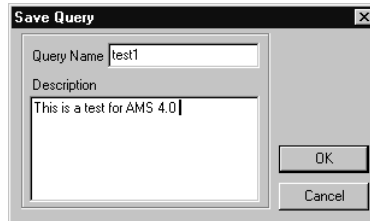


Defining a new query

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 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.



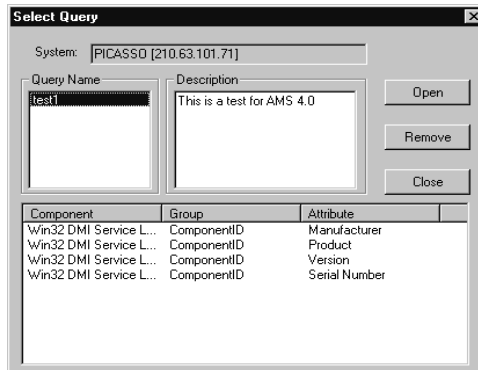
3. Type a name and description for the query.

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 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:

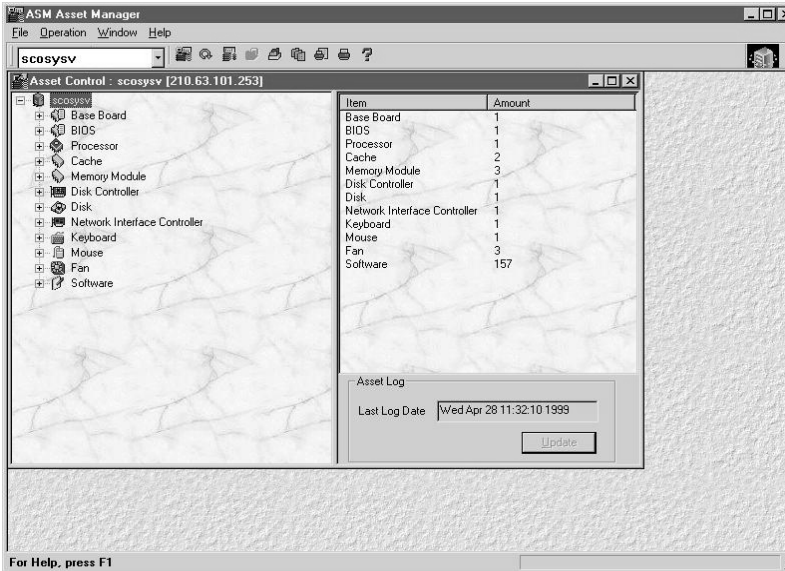
- Select Asset Manager from the Utility menu.
- Click the Asset Manager icon in the toolbar.

The Asset Manager works with ASM Agent. If the monitored system is not an ASM 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

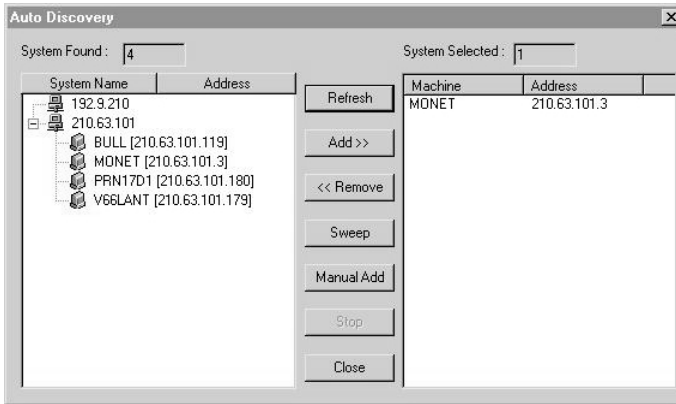
System list combo box

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.

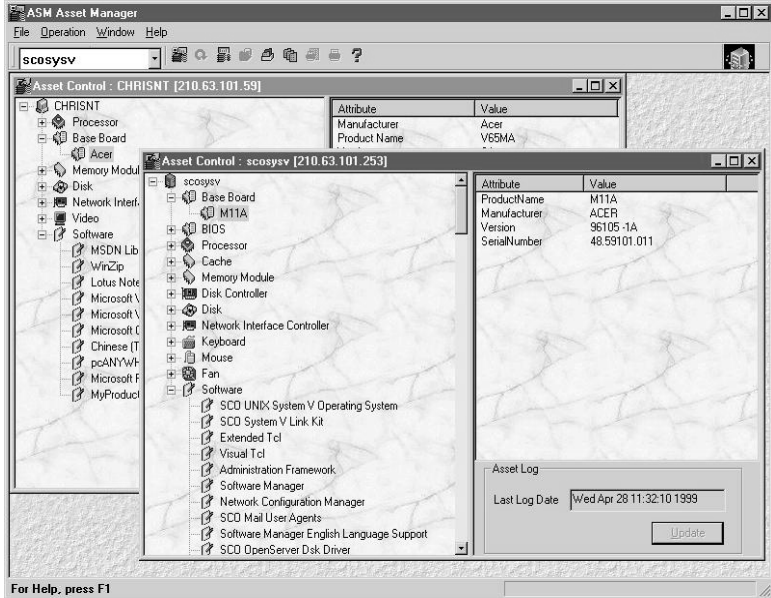
Auto Discovery dialog box items

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.



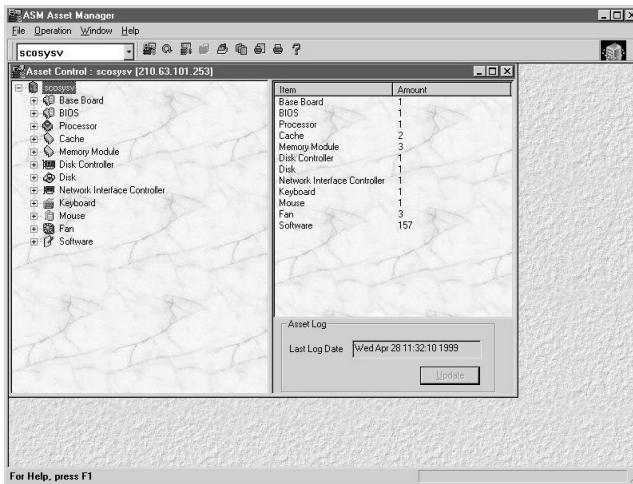
Asset Control also monitors the hardware and software changes within a system. It compares the devices currently installed in the system with the ones recorded earlier in the asset list log file.

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.

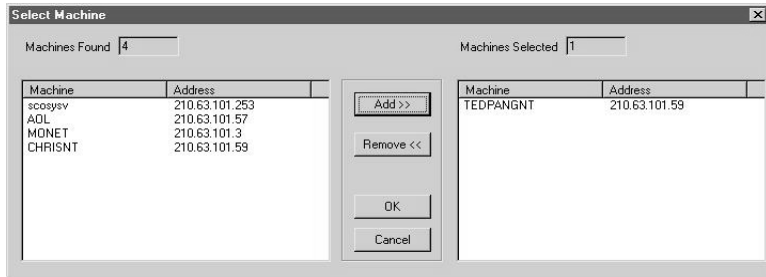


The Asset Log dialog box automatically updates the log file and displays the date and time of the latest update.

▶ Asset statistics information

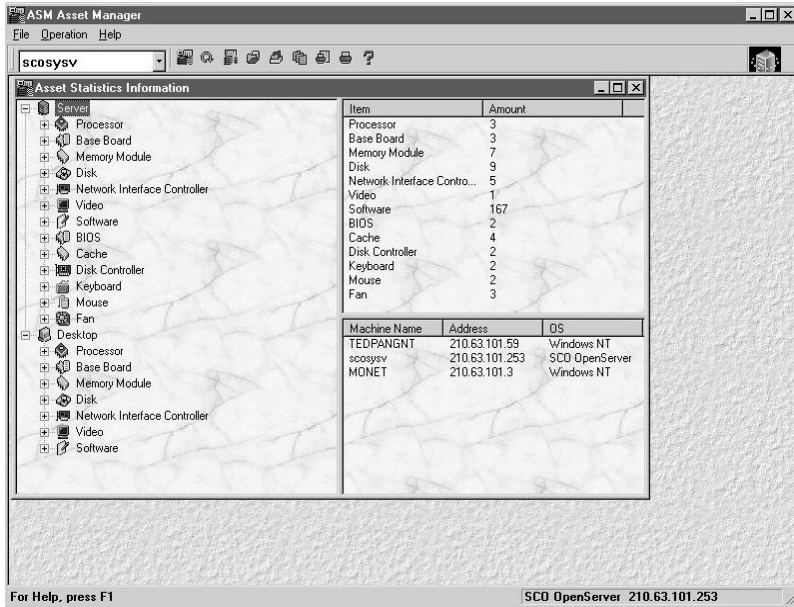
The Asset Statistics Information window collects the total number of hardware devices and software components installed in a system and displays them for your reference. You can choose one or more systems at the same time as shown below.

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.

The screenshot shows the 'Asset Information Query' window. On the left, under 'Value Selection', the following fields are set: Family: Pentium Pro, Type: Central, Manufacturer: Intel, ID: Don't care, CurrentSpeed: = 200MHz. Below this is a 'Processor' dropdown menu and a 'Query' button. On the right, there are two tables. The top table has columns 'Item' and 'Amount', with two rows: 'Pentium Pro' with amount 1. The bottom table has columns 'Machine Name', 'Address', and 'Amount', with two rows: 'scosysv' with address '210.63.101.253' and amount 1, and 'MONET' with address '210.63.101.3' and amount 1. A 'Close' button is at the bottom right.

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 pull-down 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.

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
AOL	Processor	Central Proce...	0 > 1	Sun May 17 13:20:48 1998
AOL	Processor	Central Proce...	1 > 0	Sun May 17 13:20:48 1998
AOL	Processor	Central Proce...	0 > 1	Sun May 17 13:20:48 1998
AOL	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

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

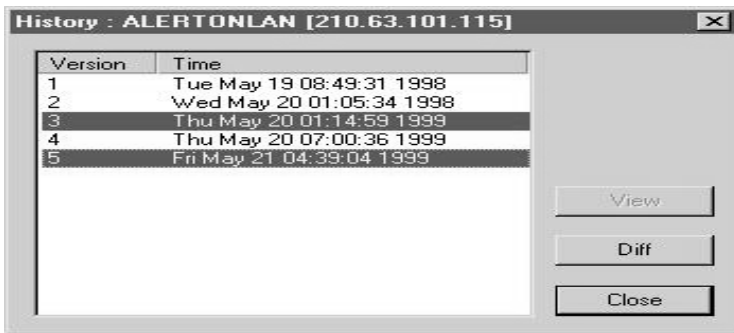
To save the log file, click the Save button and choose a filename for the log.

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

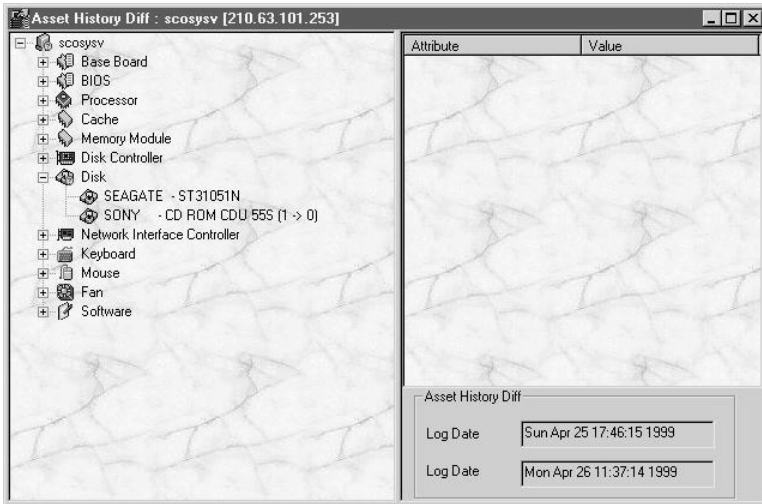
The Asset History window displays a list of log versions with their date. You can view each version independently or compare two log versions to view the hardware and software configurations of the system. Choose an item in the Asset Control window and select Operation > Asset History or click the Asset 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

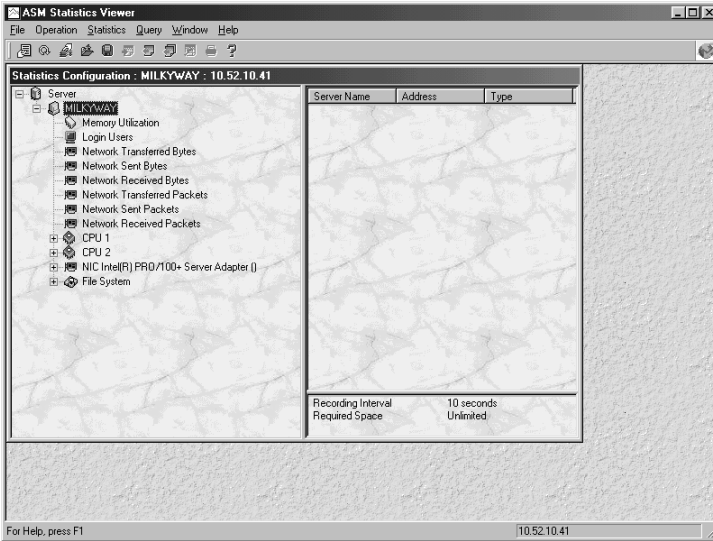
To add Statistics Viewer to your system, select Custom as the setup type during ASM Console installation, then select Utility, and click Change.

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.

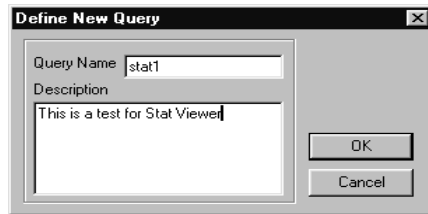
To specify the recording interval and file size for each item you are recording, use the items in the Recording Parameters section.

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.

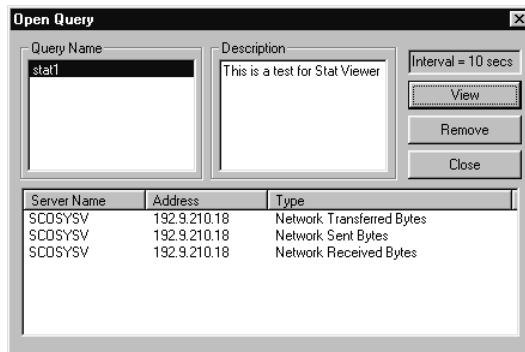
The Record Size limits the number of records that are recorded for each item. Choose Limited and specify the number of allowable records for each item. The Required Space field is calculated automatically based on the number of records that you specify. Choose Unlimited for unlimited file size.

► 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.



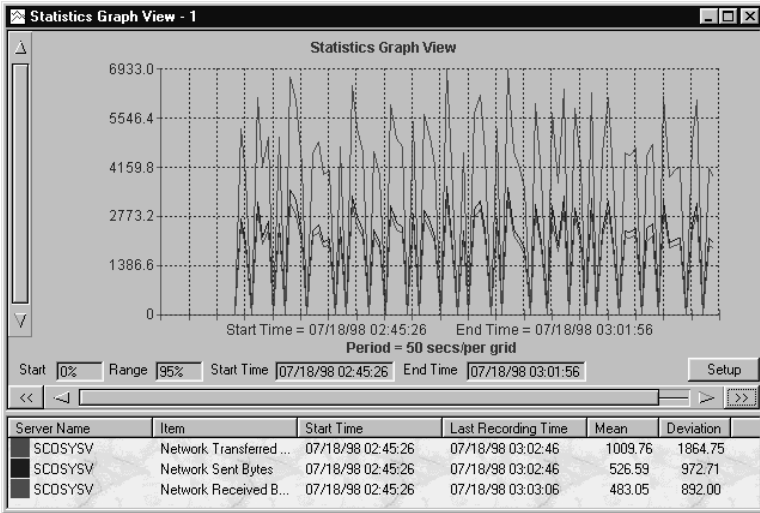
To open an existing query, click the Open Query toolbar button. The following Open Query dialog box appears.



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

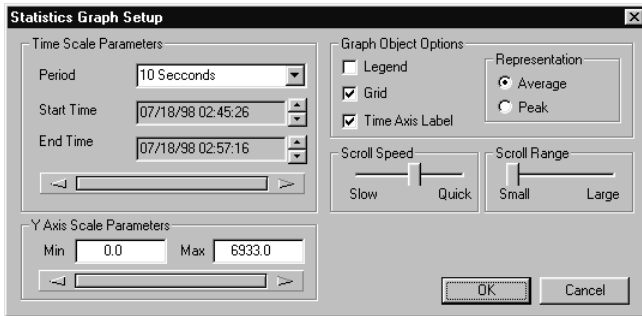
The Statistics Graph View window displays item utilization graphically. It is a “snapshot” of selected utilization statistics information. The y-axis (vertical) indicates utilization frequency; the x-axis (horizontal) indicates utilization start and end times.



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 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 Main menu
- Click on the Alert via LAN button from the ASM toolbar

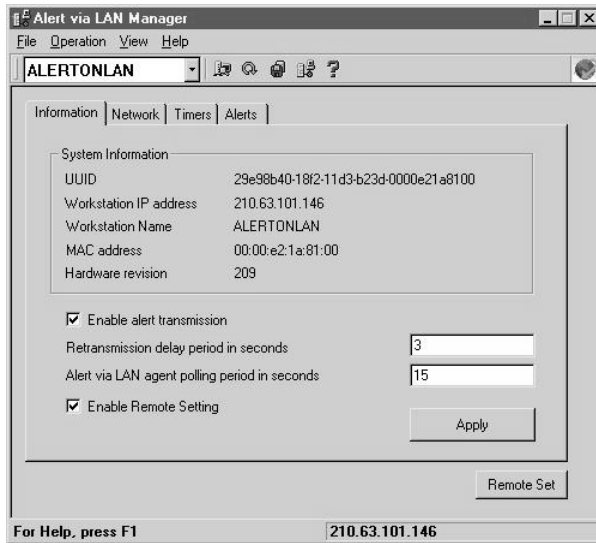
Menu bar and toolbar

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

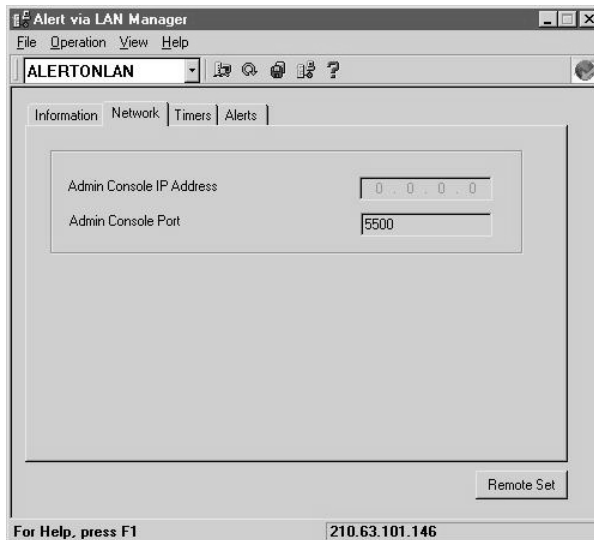


Item	Description
System Information	Displays the system configuration of the local system currently being monitored

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>

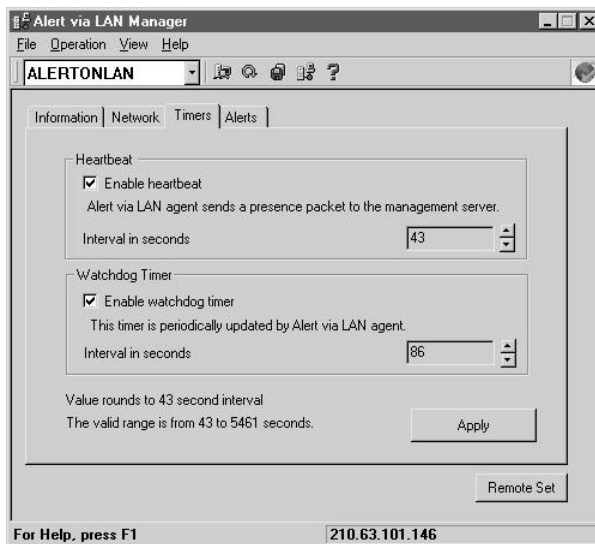
After you have entered your settings, click on the Apply button.

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

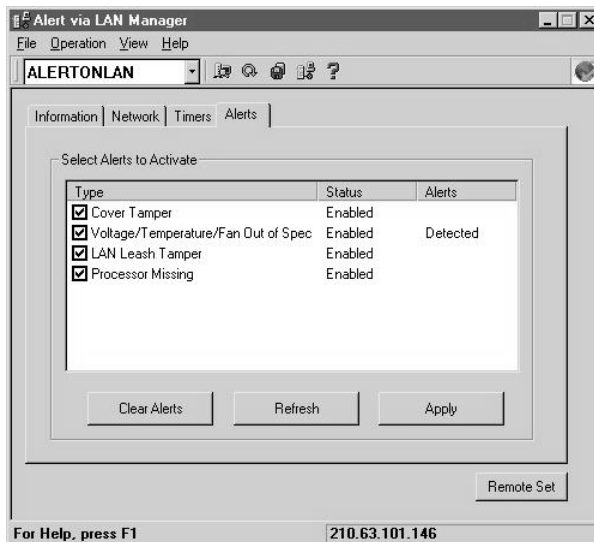


Item	Description
Heartbeat: Enable heartbeat	When enabled, the server checks for the heartbeat signal sent by the local system to determine its connection status Interval in seconds - specifies the period (in seconds) after which, if the server does not detect any heartbeat signal, the local system is 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.

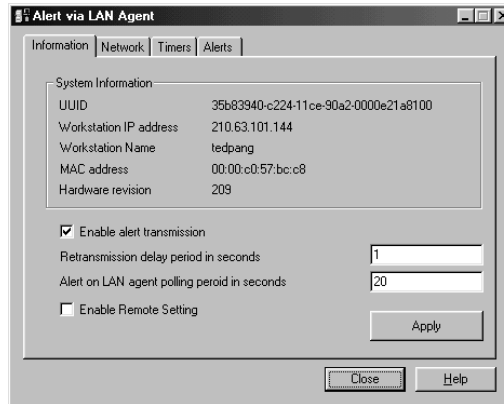
Saving the Alert via LAN Manager settings

After you have configured the Alert via LAN function, click the Set button for the changes to take effect.

▶ Alert via LAN local function

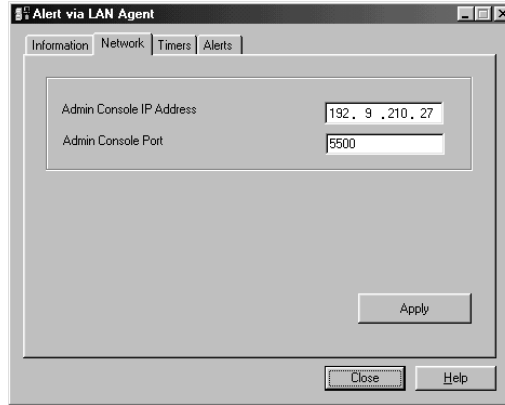
To launch the Alert via LAN function on a local system, click on the Alert via LAN icon located on the Taskbar.

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.

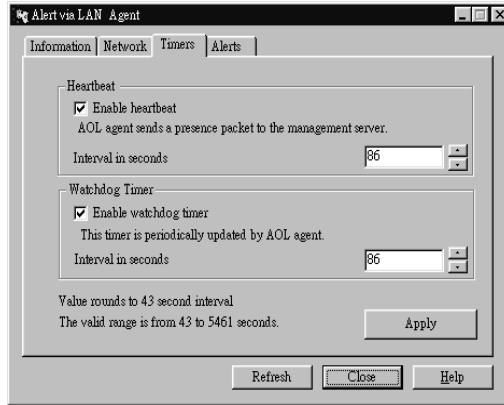
Network tab



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

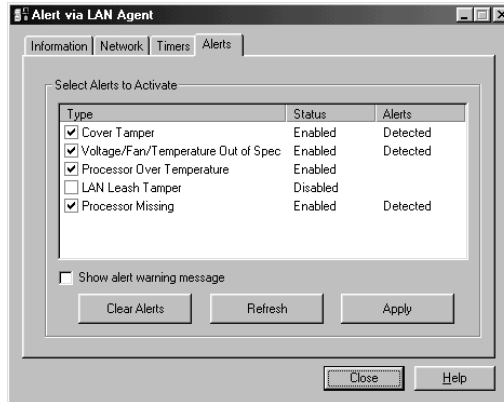
Click on the Apply button for your settings to take effect.

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

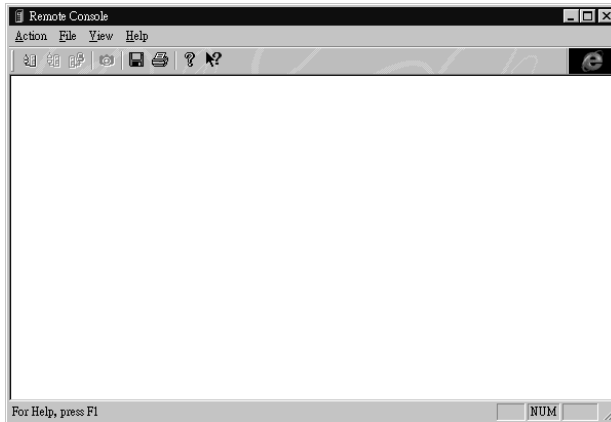
The Remote Console function allows you to control the ASM agent systems through the Local Area Network (LAN).

► 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 main menu
- Click on the Remote Console button from the ASM toolbar
- Run the Remote Console program from the ASM 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.

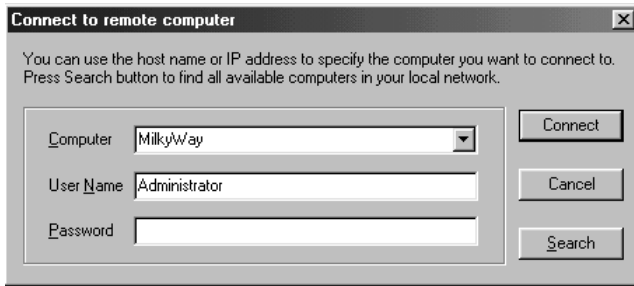
Item	Icon	Description
Action menu		
Connect		Choosing this command enables the administrator to establish connection to an ASM agent system.
Disconnect		Choosing this command automatically disconnects the existing server-client connection
File Transfer		Opens the File Transfer window, allowing the server to send and receive files from an ASM 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 server system

To establish connection to an ASM 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 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 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 agent system from your site.

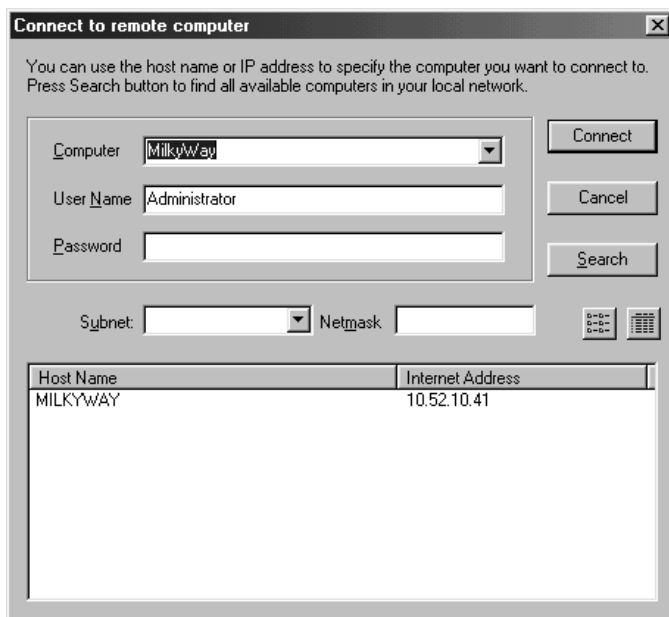
File transfer function

The File Transfer function of the Remote Console application enables the server to send and receive files from any ASM 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

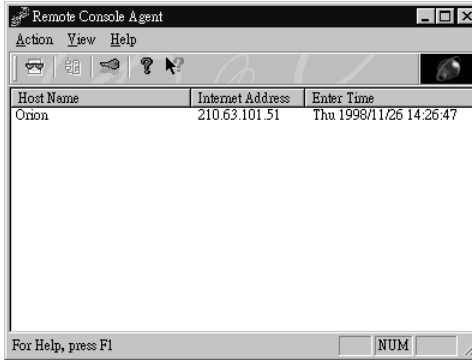
To disconnect, do one of the following:

- 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:

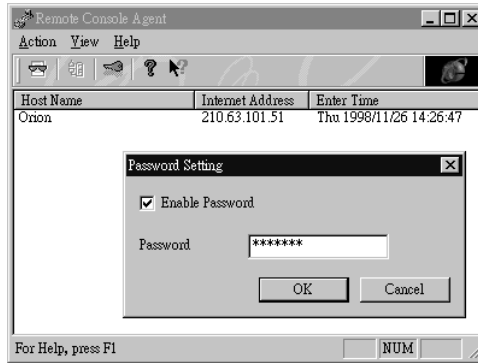
Item	Icon	Description
Action menu		
Hide		Minimizes the screen and reduces it into an icon on the taskbar. To restore the window, simply click on the icon
Enable Command		Enables the Remote Console function. When enabled, it allows you access to control the server system

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:

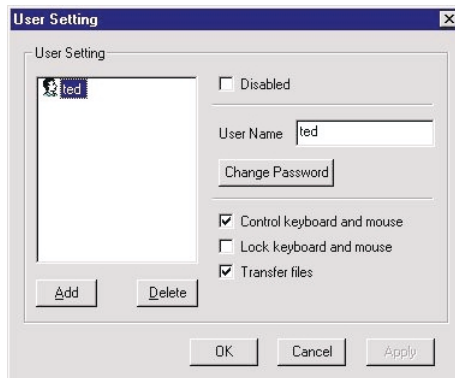
1. Select Action > Set Password from the menu bar, or click the Set Password button on the toolbar. The Password Setting dialog box appears:



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.



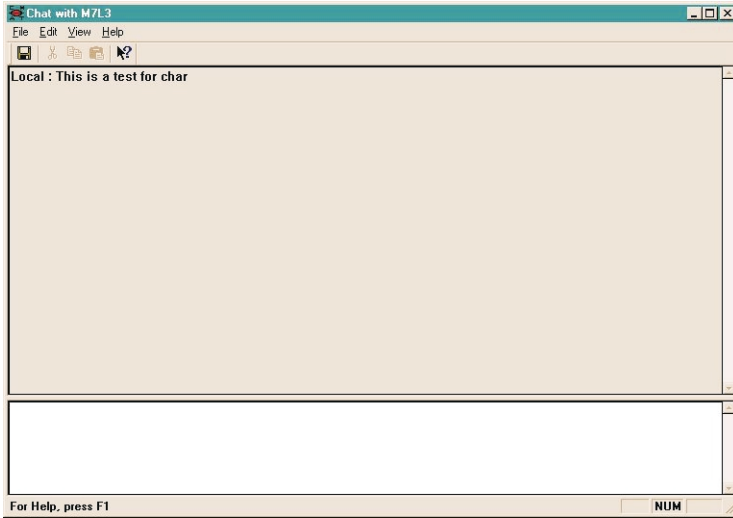
You can add or remove users by selecting the user's name and then clicking Add or Delete. The Disable checkbox prevent the user from any access to remote console. This is a nice way of suspending the user without erasing the user from the list.

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 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 Console component that is automatically installed when you install the ASM Console. Refer to “Installing ASM Console” on page 13 for the installation instructions for ASM 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 Console folder. Click on the Uninstall Acer ASM option to uninstall the whole ASM package.
2. Restart the system.

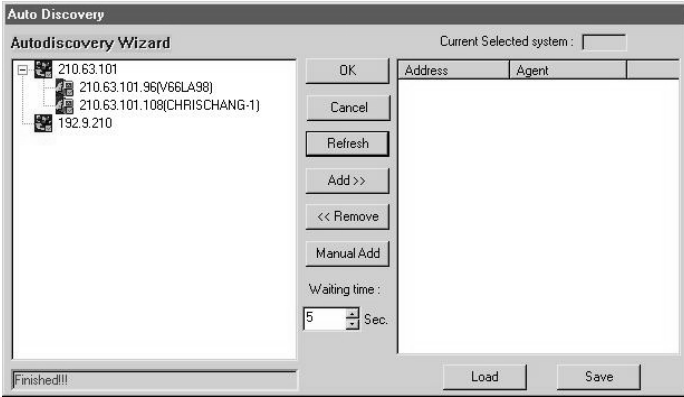


Note: Only the ASM Console includes the CMOS Setup Manager. This function is not available in the Agents.

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 agent.



This window displays all IP/IPX systems in your network detected by ASM. 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
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

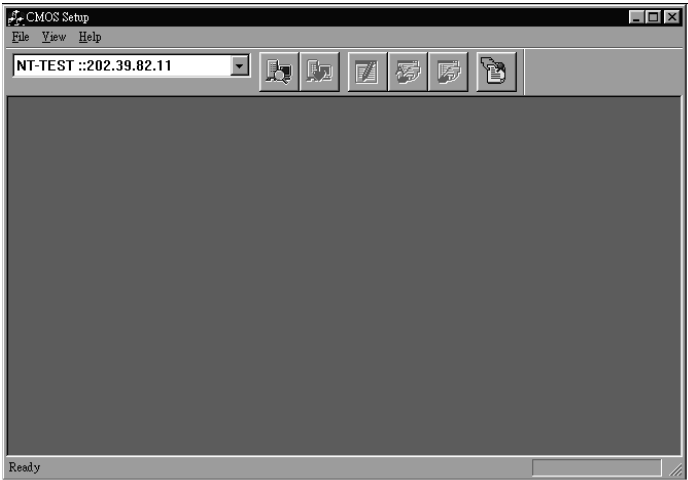


Note: In order to make the Auto Discovery function work properly, the agent must be able to respond to standard MIB-II requests. Please refer to RFC1213 for more information about MIB-II.

Basic operations

To launch the CMOS Setup Manager:

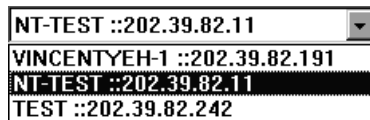
1. Make sure the desired system is available in the system list. To do this, find the ASM agent systems automatically via the Auto Discovery function, then select the desired system from the system list.
2. Click on the CMOS Setup Manager button on the ASM Console Toolbar or select Tools > CMOS Setup Manager.
3. The CMOS Setup Manager main window appears on the screen.



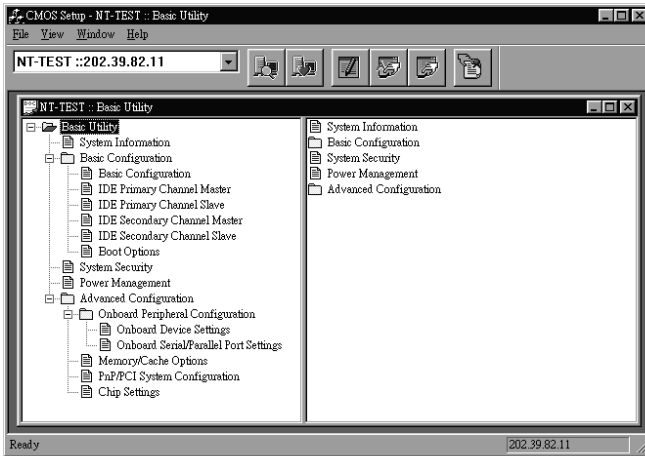
Note: You can use the auto discovery function to find the system whose CMOS data can be setup remotely.

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.



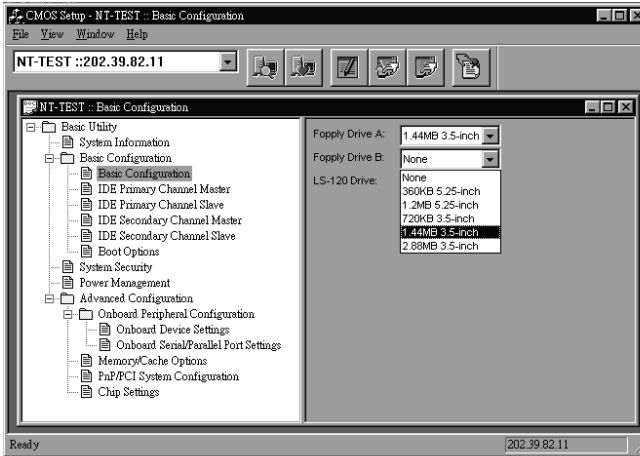
2. Select File > Get CMOS to launch the CMOS Setup window.



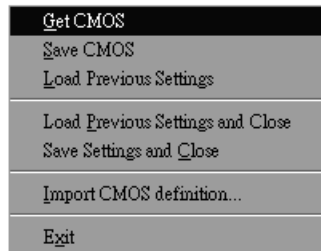
▶ Advanced operations

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 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 Console component. It is automatically installed once you install the Console of ASM. Refer to “Installing ASM Console” on page 13 for the installation instructions of ASM Console under Windows NT 4.0 and Windows 95/98.
2. Restart the system.

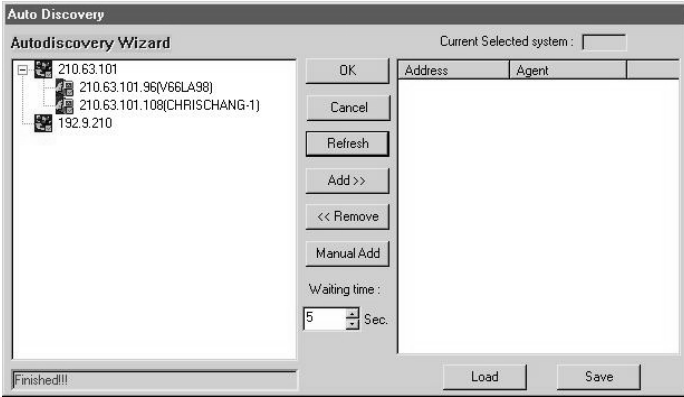
To uninstall the BIOS Update Manager:

1. Click on the Start menu, select the Programs folder, then the Acer ASM Console folder. Click on Uninstall Acer ASM to uninstall the whole ASM 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 agent.



This window displays all IP/IPX systems in your network detected by ASM. 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
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

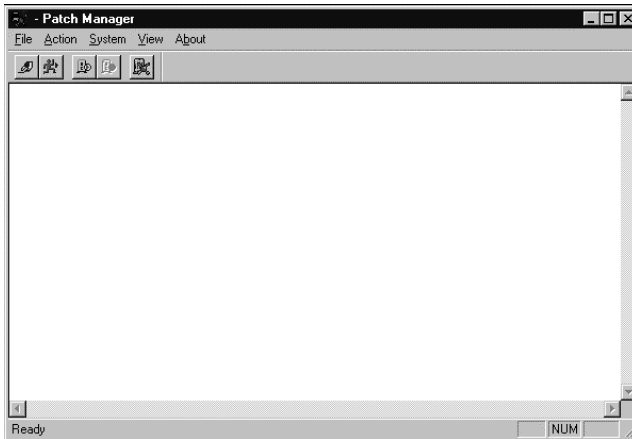


Note: In order to make the Auto Discovery function work properly, the agent must be able to respond to standard MIB-II requests. Please refer to RFC1213 for more information about MIB-II.

► Basic operations

To launch the BIOS Update Manager:

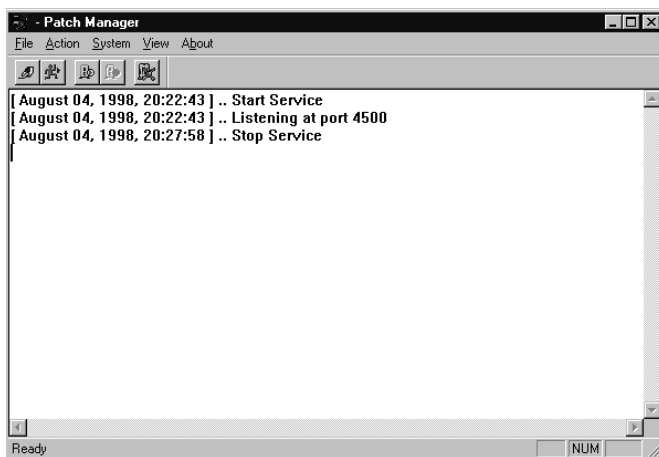
1. Make sure the desired system is available in the system list. To do this, find the ASM agent systems automatically via the Auto Discovery function and then select the desired system from the system list.
2. Click on the BIOS Update Manager button on the toolbar or select Tools > BIOS Update Manager 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.

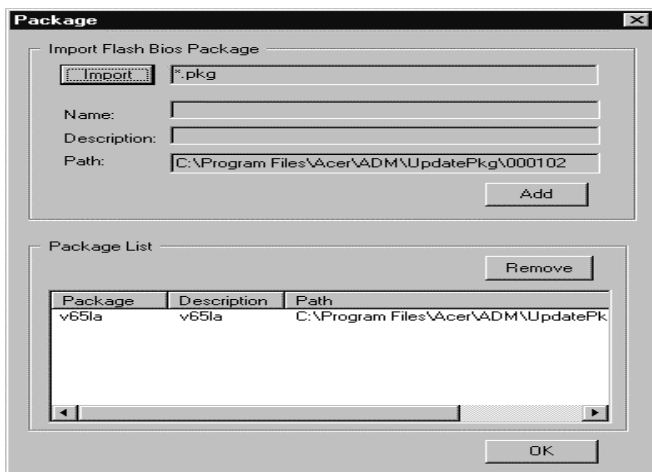


To stop the BIOS update service:

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.



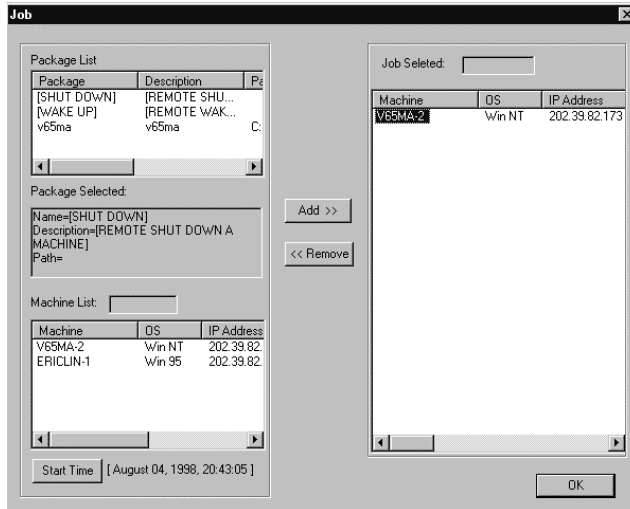
2. Click on the Import button to launch the Open dialog box.



3. Select the PKG file and click on the Open button to close the dialog box.
4. Click on the Add button to add the selected package to the package list.
5. Click on the OK button to close the Package dialog box.

To prepare the job:

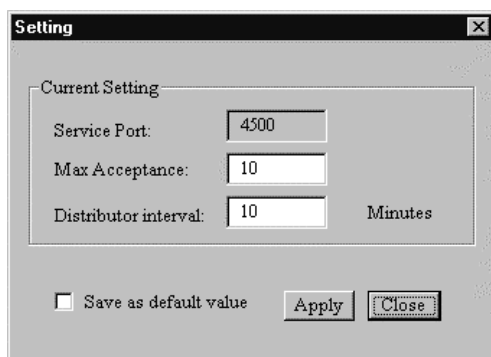
1. Select Action > Job or click on the Job button on the toolbar to open the Job dialog box.
2. Select the package item from the Package List and select the system where you want to apply the package.
3. Click on the Add >> button to add the job to the Job list.
4. Click on the OK button to close the 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 Windows-style dialog box titled "Setting". The dialog box has a title bar with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Current Setting" which contains three input fields: "Service Port" with the value "4500", "Max Acceptance" with the value "10", and "Distributor interval" with the value "10" and the unit "Minutes" to its right. Below these fields, 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	Value
Service Port:	4500
Max Acceptance:	10
Distributor interval:	10 Minutes

Save as default value



14 Remote Diagnostic
Manager (RDM)

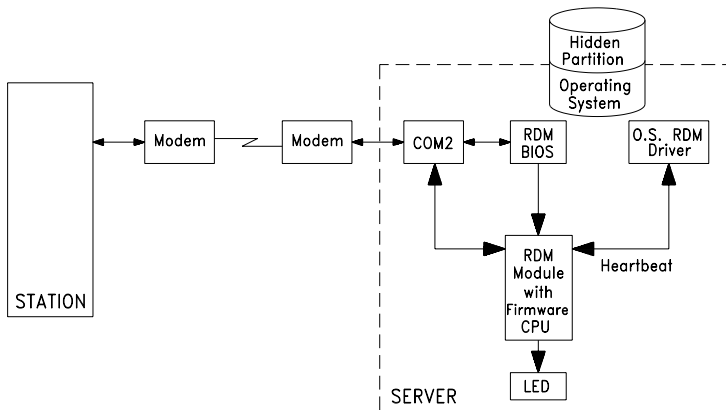
Remote Diagnostic Manager (RDM) is a server service program that offers remote server management functionality. It utilizes modems and telephone lines to remotely monitor and analyze the server condition via a remote RDM station, allowing you to update system BIOS settings for quick restoration of the 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:

- RDM agent
- RDM station
- RDM connectivity



During normal operation, the RDM driver periodically sends a heartbeat signal to the RDM module. Once the server fails, the RDM driver stops sending heartbeat signals to the RDM module. If the module processor 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 RDM module takes emergency management, it takes control of the COM 2 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 348).

RDM agent

The RDM agent refers to the system with an RDM module. An RDM module contains a microprocessor that acts as an RDM controller.

To enable the RDM module, the RDM agent driver (in ASM Pro) must be installed into the RDM agent and the system BIOS must include the RDM BIOS.

For information on how to configure the system BIOS, see the user's guide that came with the system.

RDM station

The RDM station can be any standard PC system with RDM station software installed and the necessary peripherals connected. For details on how to install the RDM station software and the necessary peripherals, refer to page 342.

RDM connectivity

This refers to the RDM connection. For the RDM agent to establish connection, it must have the RDM module, and the RDM agent driver installed into the server. For the RDM station to connect, it must have the RDM station software installed.

Peripherals such as a modem and pager are necessary for RDM to function properly. The RDM agent and the RDM station communicate via modem protocol.



Note: Make sure that the modem and other peripherals are turned ON. Otherwise, the RDM agent will not be able to establish connection with the RDM station.

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, and SCO UnixWare
- 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 station

RDM station 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 partition
- Allows remote access to the server's diagnostic utilities
- Supports file transfers
- BIOS supports ANSI terminal, allowing the RDM station to display the RDM server screen after connection is established
- Features the Talk utility that allows users at both server and RDM station 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
- RDM module
- RDM LED indicator
- 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
- ASM (Advanced System Manager Pro) agent

RDM Station 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 4.3 Console

RDM server setup

This section describes how to set up the RDM server.

Installing RDM module



Note: The RDM module is installed at the Acer factory. The following RDM module instructions is provided in the event you need to reinstall the RDM module.

ESD precautions

Electrostatic discharge (ESD) can damage your processor, disk drives, expansion boards, and other components. Always observe the following precautions before you install a system component.

- Do not remove a component from its protective packaging until you are ready to install it.
- Wear a wrist grounding strap and attach it to a metal part of the system unit before handling components. If a wrist strap is not available, maintain contact with the system requiring ESD protection at all times.

Preinstallation instructions

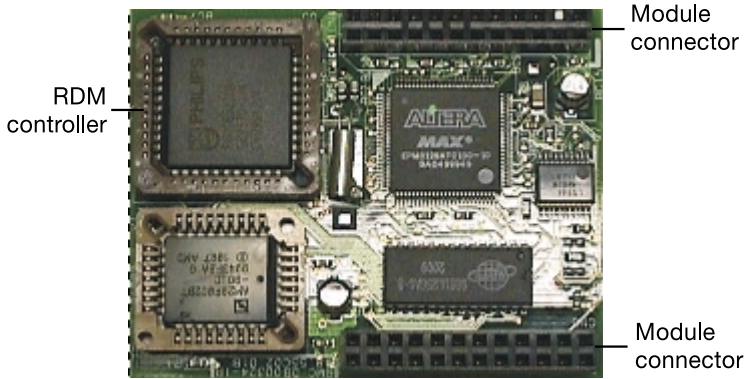
Always observe the following before you install a system component:

- Turn off and unplug the system and all the peripherals connected to the unit before opening it.
- Open the system housing.
- Follow the ESD precautions listed above before handling a system component.
- Remove any expansion boards or peripherals that block access to the desired system board slot or connectors.
- See the following sections for specific instructions on the component you wish to install.

Installing the RDM module

1. Open the system housing.

2. Align the module connectors with their corresponding connectors on the system board.



3. Gently insert the module. Make sure not to bend the pins and that the module is properly seated.



4. Replace the housing cover.
5. Enter BIOS Setup to set the desired RDM Work Mode.

Connecting communication peripherals

Modem

The RDM server and the RDM station 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: The modem at the RDM server side must be connected to the COM2 port, while the modem at the RDM station side can be connected to either the COM1 or COM2 port. 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

Observe the following after installing a system component:

- Make sure that the components are installed according to the step-by-step instructions in their respective sections.
- Replace any expansion boards or peripherals that you removed earlier.
- Replace the system cover.
- Connect the necessary cables.
- Turn on the system and the peripherals connected to it.

Installing RDM agent software

You must do the following to ensure successful installation of the RDM agent software:

1. Create a hidden RDM partition.

The hidden RDM 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 station.

To create a hidden RDM 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 hidden RDM 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.
2. 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.

3. Install the RDM Agent Driver.



.....

Note: Before you proceed, make sure that you have installed the necessary components and peripherals, for both the RDM server and RDM station.

The RDM agent driver or the server driver is contained in the Advanced System Manager Pro (ASM Pro) software package. Therefore, to install the RDM agent driver, you need to install the ASM agent software. For information on how to install the ASM Pro software, refer to the documentation that comes with the ASM Pro package.

RDM station setup

This section describes how to install and uninstall the RDM station software.

Installing the RDM station software



.....

Important! Before you proceed, make sure that you have installed the necessary components and peripherals, both for the RDM server and RDM station.



.....

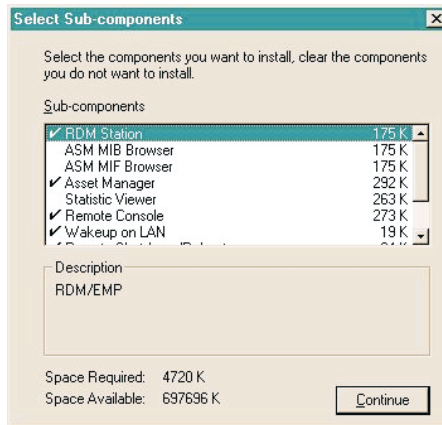
Note: The RDM station software can be installed only under Windows NT 4.0/Workstation or Windows 95/98/2000.

The RDM function is one component of ASM Pro 4.3 Console software.

Follow these steps to install the RDM station software:

1. Turn on the system.
2. Turn on the peripherals connected to the system such as the monitor, modem, etc.
3. Install ASM Console. Run the installation program, i.e., SETUP.EXE. The Setup Program Welcome screen appears.

4. For typical installation in ASM Console, the RDM station will be installed. In Custom mode, user can choose to install RDM station or not.



5. Continue to finish the installation of ASM Console.

Uninstalling the RDM station software

RDM station software can only be uninstalled within ASM Console package.

► Configuring the RDM 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 hidden RDM 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 hidden RDM partition is activated; the system boots up to the activated RDM partition; and a remote connection is automatically established to the pre-specified RDM station. This makes all RDM features available to both the local server and the RDM station. You can run any RDM utilities remotely from the RDM station. 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 station 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 4.3 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 station. If enabled and conditions are met, the RDM enabled server automatically dials the RDM station using the phone number specified in the Remote Console Phone No. parameter (see page 347) when the server reboots. Once the connection is established, both the RDM server and RDM station display the same screen which enables the RDM station to function the same as the server console. Setting this to Disabled deactivates the RDM station.

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 station 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 station 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 350) and waits for the RDM station to call in. When the RDM station calls in with the specified phone number and password, the Agent Information automatically appears on the RDM station 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 350) 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 station 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 station.

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 350) 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 station to run in different RDM operation modes.

RDM local mode

In RDM Local mode, the RDM server boots to the hidden RDM 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 hidden RDM partition and automatically establishes a remote connection, which makes all the RDM features available to both the RDM server and RDM station 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 station to make a connection.
- In the Remote Console Phone No. parameter, enter the RDM station phone number.
- Save your changes and exit the BIOS Setup. The server automatically reboots and dials the specified RDM station 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 station.

If the remote RDM connection is successfully established, you can access all RDM utilities from the RDM station.

From the RDM station, 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 station 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 station 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 station.

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 station.

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.



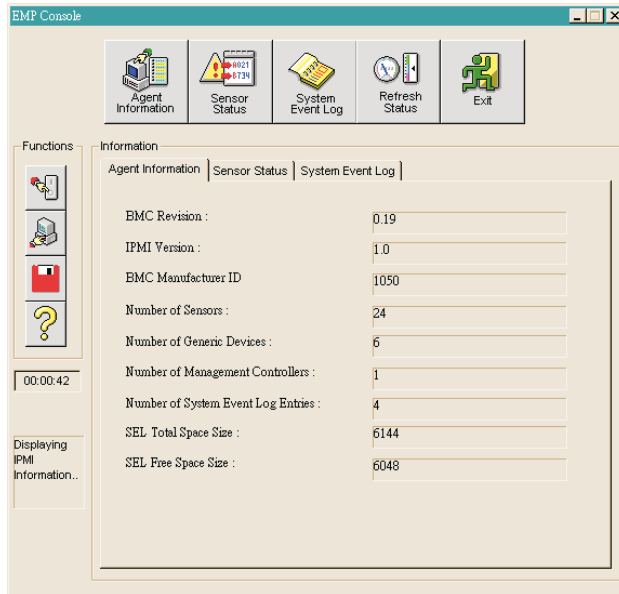
.....

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 station to the RDM Server. Once the connection is established, the Emergency Management Console appears on the screen.



Through the RDM station, 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 357, using the RDM Station.

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 station.
- 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 station

This chapter describes how to use the RDM station.

Running the RDM station



Note: To optimize the screen resolution, select 800x600.

Starting the RDM station

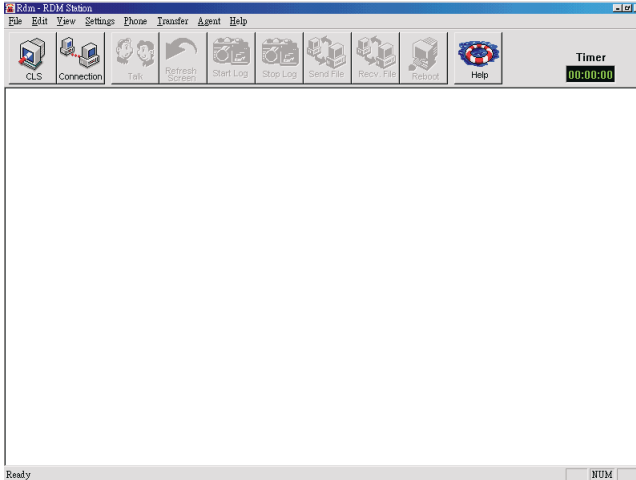
In order to run the RDM station, connect to the RDM server by doing the following:

- RDM station automatically starts when you run the ASM Pro console system. To start RDM station manually, click on the RDM station icon located on the toolbar of ASM console or select Utility > RDM Station 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 station window.

Connecting to the RDM server

To access the remote server from the RDM station, do the following:

1. From a remote location, launch the RDM station program. The RDM Station Utility window appears on the screen.



For more details on the RDM Station Utility, see section page 364.

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 RDM agent icon already exists, double-click it. The station automatically dials to the RDM agent. Otherwise, create a new RDM agent. See section page 372 for details on creating a new RDM agent.
4. When the call is successful, the RDM module verifies the entered password. If the password matches the RDM 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 station screen. You may get RDM agent information by clicking various EMP Console buttons, or perform RDM functions by clicking on the function buttons.

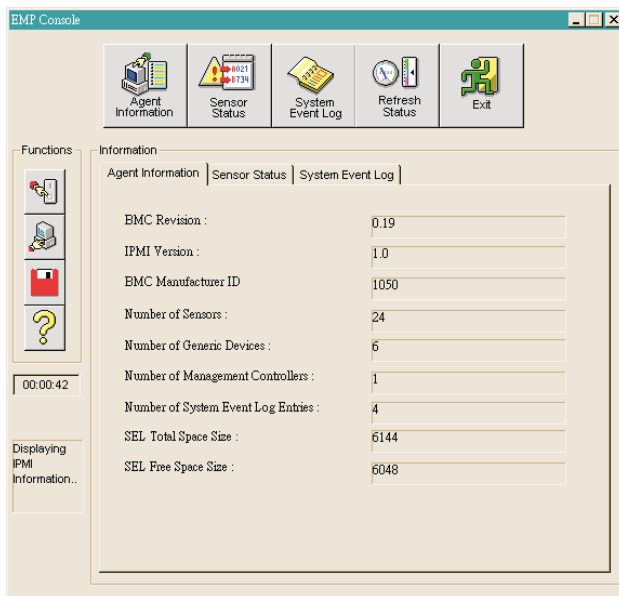
EMP console buttons

From the EMP Console window, you can do the following by clicking the respective RDM Agent Information button:

Agent information



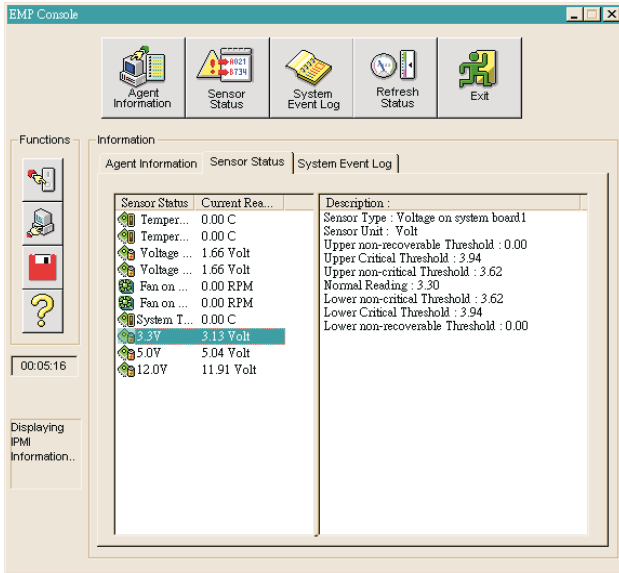
Displays important agent information.



Sensor status



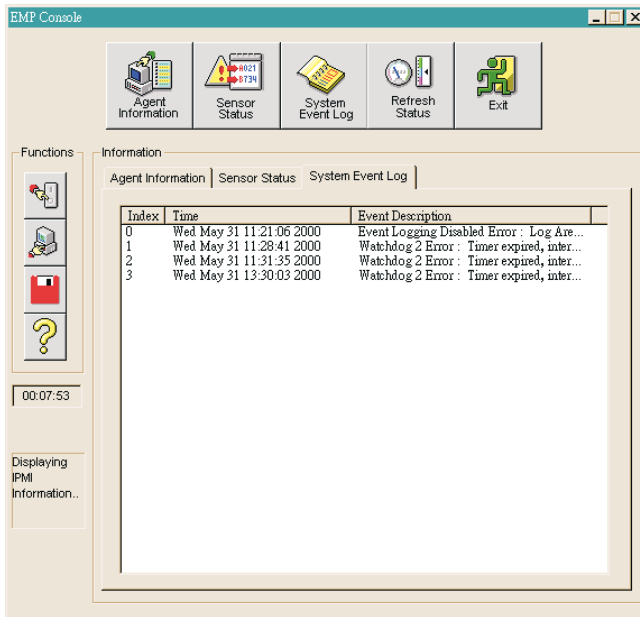
Displays readings of sensors.



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 station 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 RDM Agent Information functions:

Power On/Off

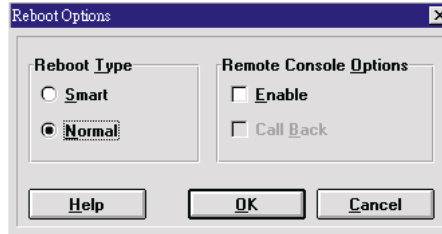


Turns off the server. If you click this button, the message System turned off appears. Simply click on OK.

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



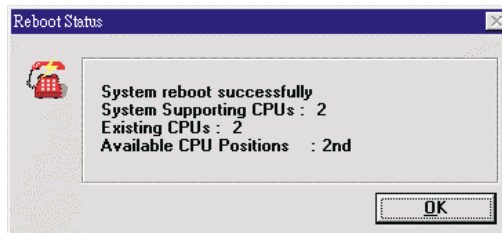
Displays the Help information.

RDM reboot options

From the RDM reboot options dialog box, the following reboot options are available:

Smart reboot

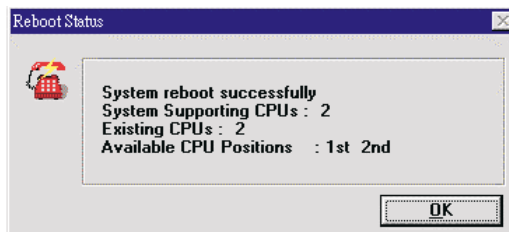
When the Smart Reboot option is selected, RDM checks the status of all processors installed in the server. If there is at least one processor that is in good condition, the system automatically reboots to that processor. After reboot, the following message box appears:



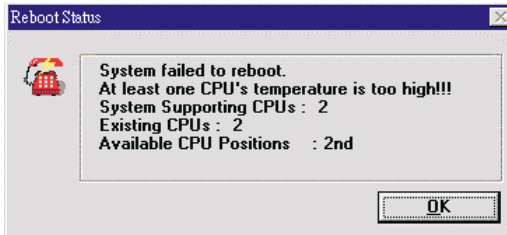
If all processors are in bad condition, a message informing you of the condition of the processor(s) appears, asking if you still want to force to reboot the system. Click Yes to "force" the reboot of the server. The system will use all the processors installed in it to reboot.

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 station options

From the RDM reboot options dialog box, the following RDM station options are available:

Enable

Maintains remote connection after server reboots and allows the RDM station 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 station 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 station utility

This section describes the functions available through the RDM station utility.

RDM station 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 station window.
- Shutdown RDM Station - Exits the RDM station 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 station 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 station and the RDM server to send and receive files.

Send File - Enables the RDM station to send files to the server.

Receive File - Enables the RDM station 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 Station Talk - Runs the Talk utility. This utility allows the users located at RDM station and RDM agent to communicate online.

Reboot Agent - Allows you to reboot the server from the RDM station.



.....

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 Station - Displays the copyright, version number and release date of the RDM station utility.

RDM station 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 station and RDM 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 station to send files to the server.
Receive File		Enables the RDM station to receive files from the server.

Reboot		Allows you to reboot the server from the RDM station.
Help		Opens the RDM online help.

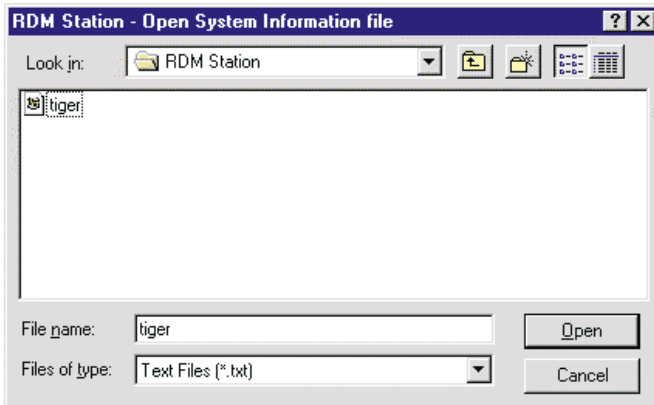
RDM station functions

This subsection describes the various RDM station functions you can perform through the RDM station utility.

Viewing a snapshot file

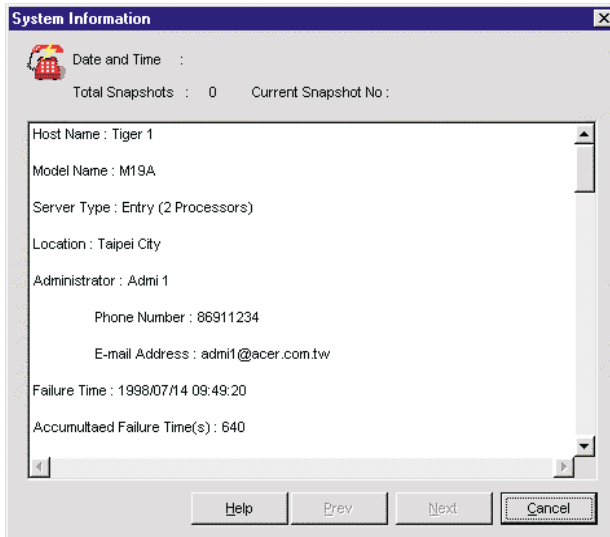
This feature is only for RDM 4.0x Agent. To view a previously saved Snapshot file, do the following steps:

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:

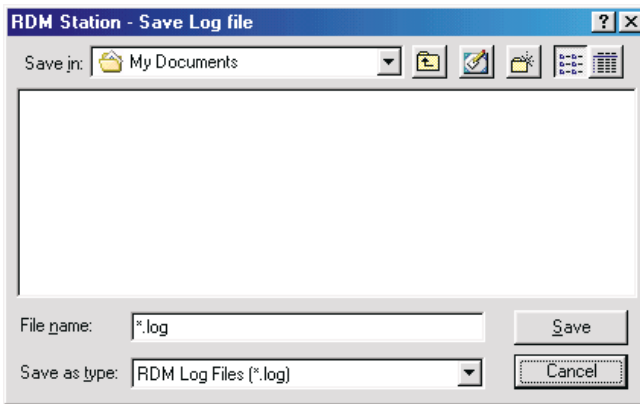
- Click on the Clear button from the Toolbar.
- From the menu bar, click on the Edit menu and select the Clear Window command.

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:

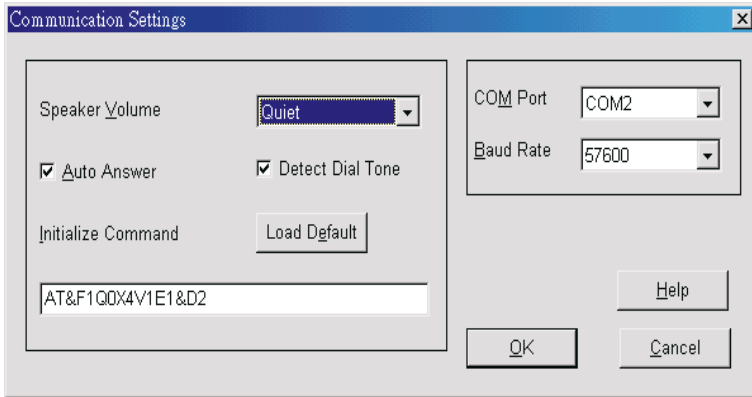
- Click on the Stop Log button from the Toolbar.
- From the menu bar, click on the Edit menu and select the Stop Saving log command.

Configuring RDM station 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.

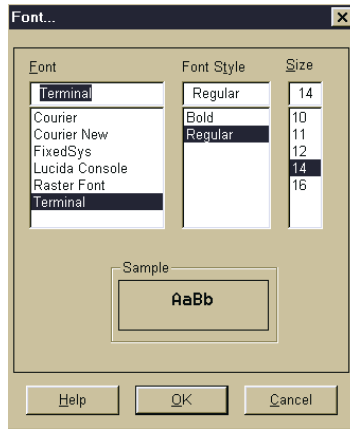
Setting the font properties

You can select the font that you want to appear on the RDM station 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.

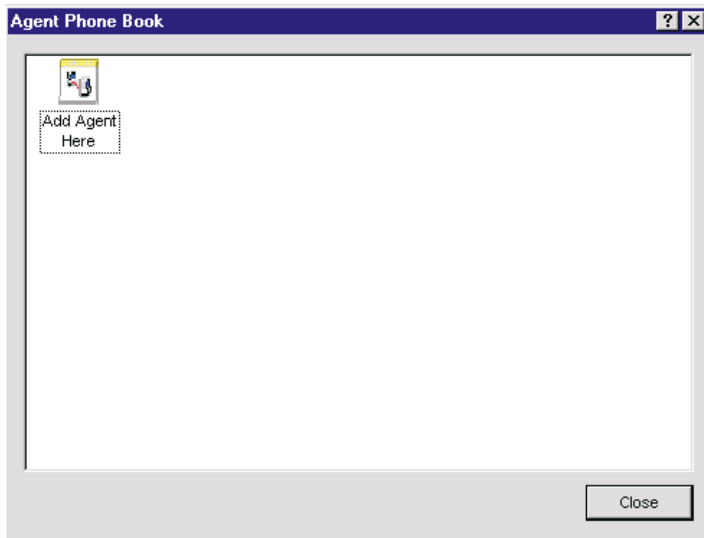


3. From the Font box, select the desired font type.
4. From the Font Style box, select the desired font style.
5. From the Size box, select the desired font size.
6. After making your selections, the desired character type appears in the Sample box. Verify your settings and click on OK.

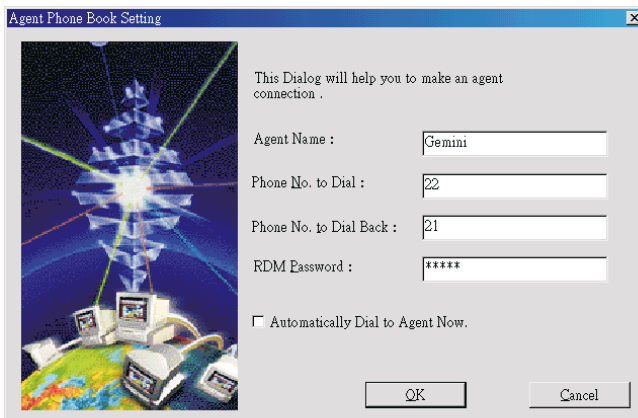
Creating a new RDM agent

To create a new RDM 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.



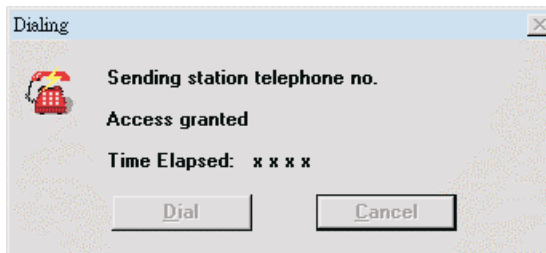
3. Enter the RDM agent in the Agent Name textbox, RDM agent phone number in the Phone No. to Dial textbox, RDM station's phone

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.

- 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 station automatically dials the server number. When the call is successful, the RDM module verifies the entered password and the following message box appears:



- If the password matches the server's password for remote connection, the Agent Information window appears. This window displays general information about the server.
- After verifying your settings, click on Exit. The server boots according to your specified settings.

Sending files



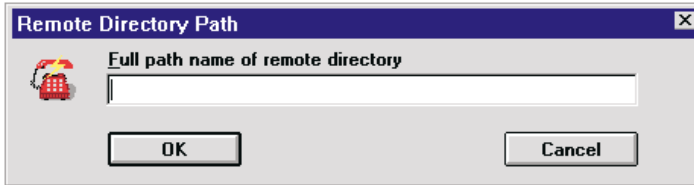
Note: Before you send files, make sure that the agent is in DOS command mode and that the files to be transferred are stored on the local hard disk.

To send files to the server, follow these steps:

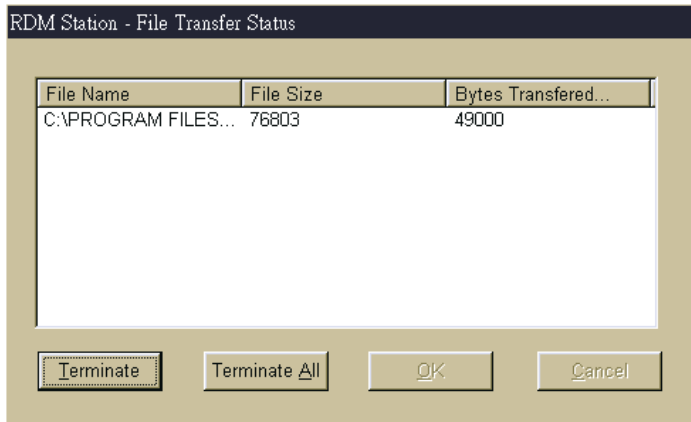
- Do either of the following:
 - From the menu bar, click on the Transfer menu and select the Send File command.
 - Click on the Send button from the Toolbar.

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 station 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

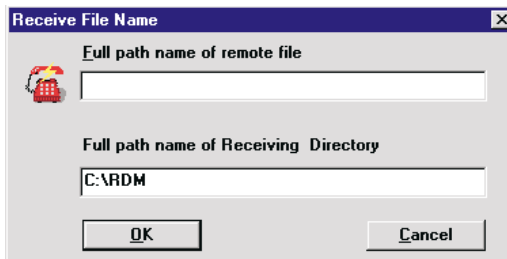


Note: Before you receive files, make sure that the agent is in DOS command mode.

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 station screen.

Running the talk utility

The Talk utility allows the user at the RDM station 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.

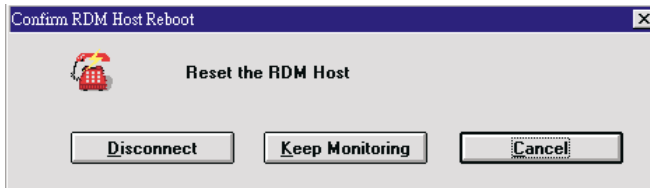
2. Type in the messages that you want to send. The messages from the server site appear in the upper portion of the screen, while the messages from the RDM station appears in the lower portion
3. To exit this utility, the user at the RDM station must press `Ctrl + X` keys.

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).

RDM 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 station manager troubleshooting

1. When running any DOS application that requires ALT + hotkey, RDM station 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 station function has been enabled. BIOS will dial out to connect to the RDM station. 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 station is busy now. Wait for a few minutes, then try reconnecting.
Connect Fail: No Answer	No response from the RDM station. Make sure that the RDM station phone number is correct.
Connect Fail: No Telephone to Dial	RDM station is enabled, but no RDM station phone number is set. Enter the BIOS Setup, select the Remote Diagnostic Configuration option, and enter the RDM station 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 Advanced Web-based
Manager

Advanced 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 Console with some differences in GUI design and item layout.

► Installing AWM and Microsoft IIS

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 (4.0 is recommended)
 - Microsoft Active Server Pages (ASP)
 - SNMP Service
- Ethernet card
- Modem

Installing AWM

To install AWM:

1. Insert the Resource CD into the CD-ROM drive on your system.
2. Click on the Startup icon.
3. Click on Software Installer, and select AWM.
4. Follow the Installation Wizard.
5. 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.

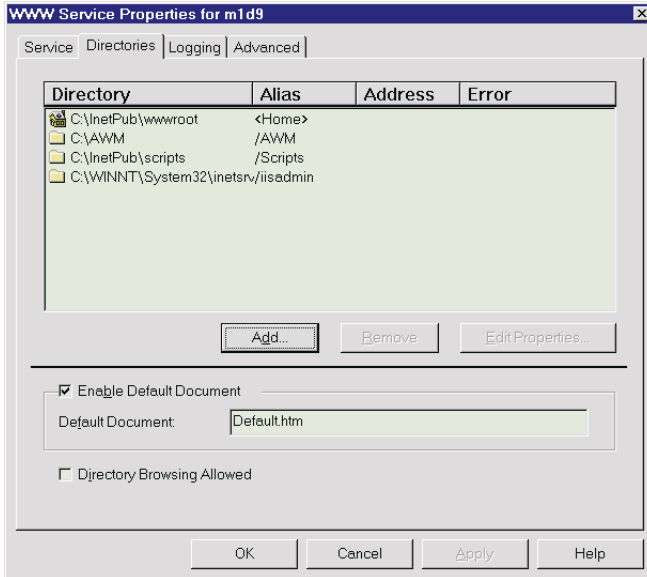
Setting up Microsoft IIS



Note: If you have IIS version 4.0 or later the directory is automatically added.

To set up Microsoft IIS:

1. Open your IIS configuration program and check the virtual directory setting.
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. C:/AWM).



3. After adding the virtual directory, click the Execute checkbox and then click OK to save changes and exit.

Directory Properties

Directory:

Home Directory

Virtual Directory

Alias:

Account Information

User Name:

Password:

Virtual Server

Virtual Server IP Address:

Access

Read Execute

Require secure SSL channel (Not installed)

Enable Client Certificates Require Client Certificates

Running AWM

Type this address in your browser:

`http://{IPADDRESS}:9999/AWM`

The password window appears prompting for authentication as shown below.

Enter Network Password

Please type your user name and password.

Resource: 210.63.98.238

User name:

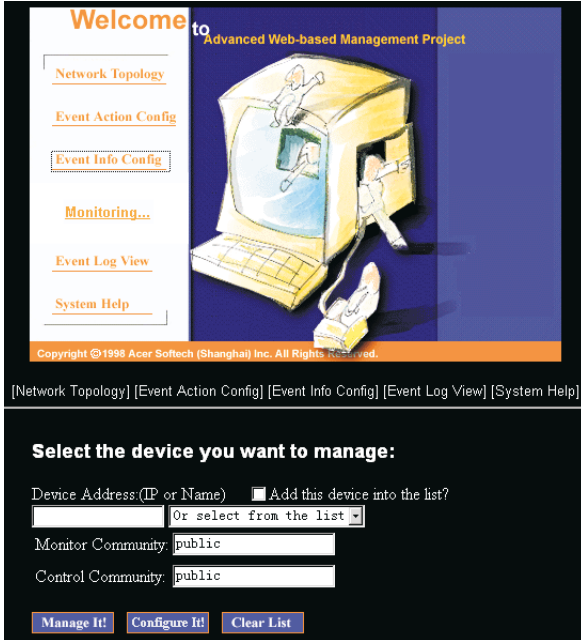
Password:

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 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.

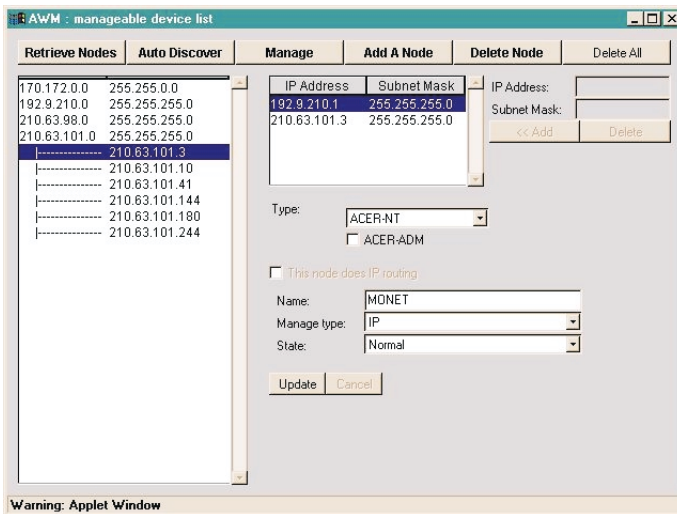


Item	Description
Network topology	<p>Shows the current state of network devices allowing you to view different portions of your network. It also displays the gateways and subnets in your network system. If you are using AWM for the first time, AWM automatically discovers devices on your network. See “Network topology” on page 393..</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 page 397</p>
Event action configuration	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 information configuration	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.
Real time event monitoring	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
Network event log	Records event information and saves them to file for future reference
Help	If you don't know what to do.....
Manage device form	Allows you to directly choose which network device you want to manage
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 this device into the list?	Click this check box if you want to include the device name or address in the Device Address box

Item	Description
Monitor Community and Control Community	
Manage It!	Opens a management window for the specified device
Configure It!	Opens an Event Action Configuration window for the specified device
Clear List	Erases the list of devices in the device list pull down menu

► Network topology

The Dynamic Network View 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. However, if you are using AWM for the first time the subnet and device list panel will be empty.



Using Auto Discovery to add a network device to the Dynamic Network View

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 Auto Discovery button. The Auto Discovery dialog box appears.



To start the discovery process:

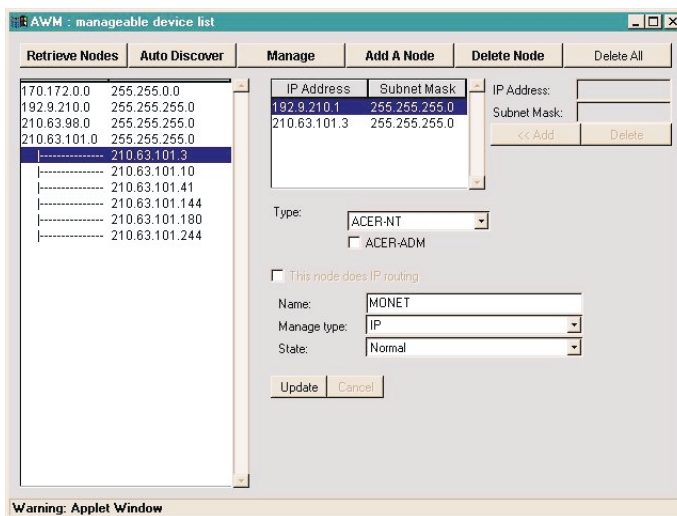
1. Enter the subnet ID and Mask and then click the Discover button. The process might take some time depending on the size of your network.
2. After Auto Discovery finish detecting manageable network devices, the Cancel button will change to Close.
3. Click the Close button to exit. The discovered devices displays in the left panel of the Dynamic Network View window.

Changing device properties

The Dynamic Network View window displays the properties of network devices. To change device properties:

1. Highlight the device you want to change.

2. Make the appropriate changes and click the Update button.



Adding a device

To add a device:

1. Click the Add a Node button.
2. Enter the IP address, name, and type of device.
 - The IP Address/Subnet Mask of the new device must be indicated.
 - If the new device is an IP forwarding node, then add the IP Addresses for each interface and click the This node does IP routing checkbox.
 - If the device happens to be one of the predefined device types, select the correct device type. The URL/Icon File, etc. are picked up from the device defaults configuration. In case of a new device, give the URL of the management page and the icon file to be used to show this device in topology views.

IP Address	Subnet Mask
170.172.0.0	255.255.0.0
192.9.210.0	255.255.255.0
210.63.98.0	255.255.255.0
210.63.99.0	255.255.255.0
210.63.101.0	255.255.255.0
210.63.103.0	255.255.255.0
210.63.106.0	255.255.255.0
10.34.5.0	255.255.255.0
10.34.89.0	255.255.255.0
10.34.91.0	255.255.255.0
10.34.92.0	255.255.255.0
10.34.100.0	255.255.255.0

IP Address:
 Subnet Mask:
 << Add Delete

Type:
 ACER-ADM

This node does IP routing

Name:
 Manage type:
 State:

Add Cancel

Warning: Applet Window

- Fill up the form and click the Add button to add the device to the database. Click the Cancel button to cancel adding device operation.

Removing a device

To remove a device, select the device to be deleted and then click the Delete Node button.

To remove all devices, click Delete All. This empties the whole device information database.

► Managing network devices

There are three types of device management page available to AWM:

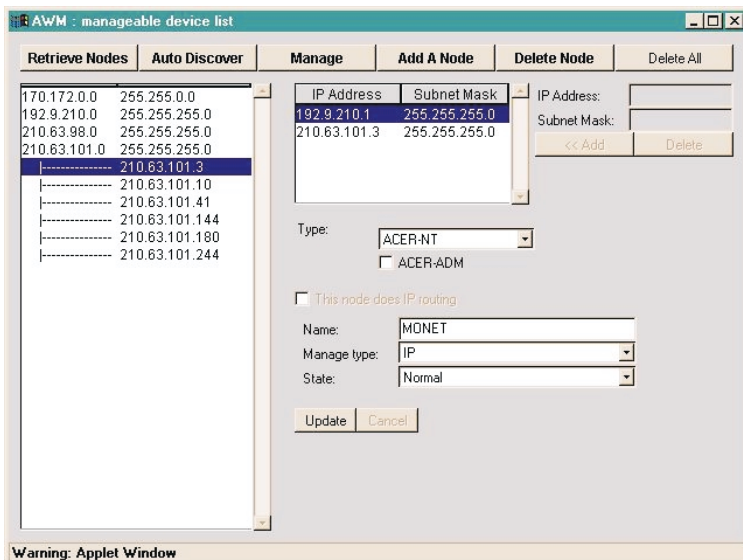
- Server devices that has a ASM (Advanced Server Manager) agent installed
- Desktop devices that has a ADM (Advanced Desktop Manager) local agent installed
- Generic SNMP (Simple Network Management Protocol) devices that support SNMP RF1213 MIB

Depending on the system, AWM can use either types of management for a network device. There are two ways you can manage a device. By using Network Topology or by using the Manage Device Form.

Managing devices using the Network Topology

To manage devices using the Network Topology:

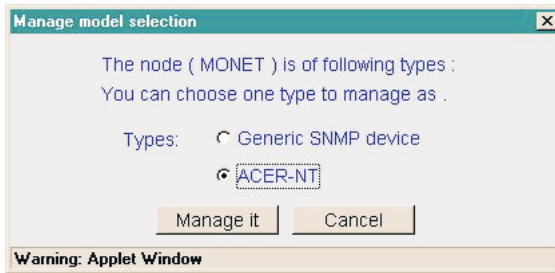
1. Click the Network Topology link on the main page. The Dynamic Network View window displays.





Note: If you are using AWM for the first time the subnet and device list panel will be empty. See “Using Auto Discovery to add a network device to the Dynamic Network View” on page 393..

2. Select the subnet where the device is located and then click the Retrieve Nodes button to show all the devices in this subnet.
3. Double click on the device to manage it or select a device and then click the Manage button. The AWM prompts a dialog box to choose the management type.



4. Click the management type you want to use and then click Manage It! The appropriate management window displays.

Managing devices using the Manage Device Form

To manage devices using the Manage Device Form:

1. Type the device name or address in the Device Address (IP or name) field or click on the pull down menu to select available devices.
2. Set the community information if necessary and click Manage It! The appropriate management window displays.

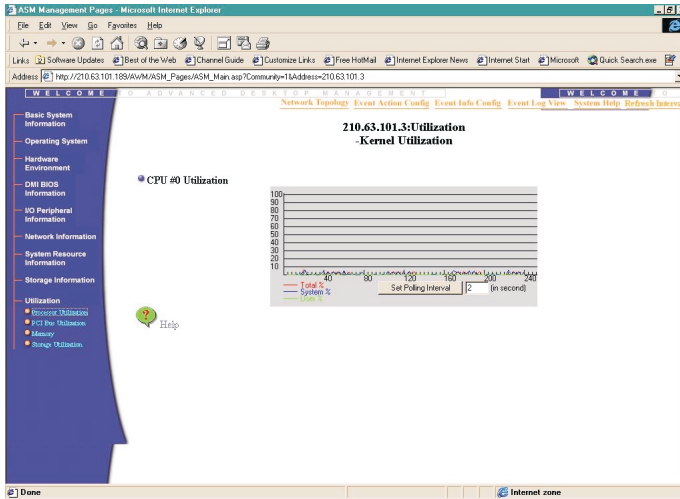
To add a device name or address to the device list, type the device name or address and then click the Add this device to the list? check box. When you click on the Manage It! or Configure It! button, the device you just entered will be saved into the device list.

If you want to erase an existing device name or address from the device list, select the device and click the Clear List button or if you want to erase the whole list simply click the Clear List button to erase.

Dynamic graphing

Pages optionally permit real time monitoring of various device performance. These pages contain a Java Applet to present a dynamic graph which draws real time retrieved data.

The default polling interval is 2 seconds. This can be modified by clicking the Set Polling Interval Button on the Graphing Applet.



Management pages

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 management pages for Server devices that have ASM agent installed
- MIB-2 browser pages for Generic SNMP devices that support SNMP RFC1213 MIB

ASM 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.

The screenshot shows the AWM interface with the following elements:

- Navigation Menu (Left):** Basic System Information (selected), System, Machine, Manager, Operating System, Hardware Environment, CMI BICS Information, I/O Peripheral Information, Network Information, System Resource Information, Storage Information, Utilization.
- Page Title:** 210.63.101.3: Basic System Information - System Information
- System Information Table:**

Contact person	<input type="text"/>
Network Address	210.63.101.3
Operating System	Windows NT 4.0 (build 1381) Service Pack 5
Computer Time	Wed Oct 20 09:57:48 1999
Up time	6 days 00 : 06 : 01
Location	<input type="text"/>
ASM Agent Version	version 2.0
- Buttons:** Submit, Refresh, Set Refresh Interval
- Help:** A green question mark icon labeled "Help" is located at the bottom left.

Machine page

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

WELCOME | 210.63.101.3:ADVANCED DESKTOP MANAGEMENT | WELCOME

Network Topology | Event Action Config | Event Info Config | Event Log View | System Help | Refresh

210.63.101.3:Basic System Information - Machine Information

Basic System Information

- System
- Machine
- Manager

Operating System

Hardware Environment

DMI BIOS Information

IO Peripheral Information

Network Information

System Resource Information

Storage Information

Utilization

Base Board

Manufacture	ACER
Product Name	M11A
Version	96105-1A
Serial No.	48.59101.011

BIOS

Vendor	ACER
Release Date	06/05/06
Version	ACR2F800.108-961106.R01-B5

CPU

Manufacture	Family	Current Speed	External Clock
Intel	Pentium D36 Class CPU	200	66

Physical Memory

Total Memory	Maximum Memory Capacity	Memory Slots No.	Memory Slots Used No.
160 MB	384 MB	3	3

Refresh | Set Refresh Interval

Manager page

Click the Manager page to view information about the person in charge of the system.

WELCOME | 210.63.101.3:ADVANCED DESKTOP MANAGEMENT | WELCOME

Network Topology | Event Action Config | Event Info Config | Event Log View | System Help | Refresh

210.63.101.3:Basic System Information - Manager Information

Basic System Information

- System
- Machine
- Manager

Operating System

Hardware Environment

DMI BIOS Information

IO Peripheral Information

Network Information

System Resource Information

Storage Information

Utilization

Manager Name

Office Address

Office Phone

Home Address

Home Phone

Pager

E-mail

Submit | Refresh | Set Refresh Interval

Help

Operating system

User page

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

W E L C O M E TO ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log View](#)

210.63.101.3:Operating System
- login User

Number of User: 23

User Name	Login Time
NWVIEWS	Thu Oct 14 10:00:48 1999
ARRAY	Mon Oct 18 17:54:49 1999
ARRAY\richie	Mon Oct 18 17:55:06 1999
TPE_ED03574\WGOLDEN	Wed Oct 20 08:40:35 1999
TPE_ED06992	Wed Oct 20 08:58:37 1999
TPE_ED06992\Ted	Wed Oct 20 08:58:37 1999
TPE_ED4899	Wed Oct 20 09:10:13 1999
TPE_ED4899\skyman	Wed Oct 20 09:10:13 1999
TPE_ED0072\FAUL	Wed Oct 20 09:44:43 1999
TPE_D19983	Wed Oct 20 09:48:47 1999
TPE_D19983\curtis	Wed Oct 20 09:50:36 1999
ARRAY	Wed Oct 20 09:51:08 1999

Drivers page (only available for Windows NT operating systems)

The Drivers page displays all the device drivers installed in the server. It also shows the total number of drivers installed in the system.

W E L C O M E TO ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log View](#)

210.63.101.244:Operating System
- Driver

Number of Driver: 41

Driver Name	Type
Afd	AFD Networking Support Environment
aic78xx	aic78xx
AMDFCN	AMD PCNET Family Ethernet Adapter Driver
ASM	ASM
Aspi32	Aspi32
AsyncMac	Remote Access Mac
atapi	atapi
AW_HOST	AW_HOST
Beep	Beep
Cdrom	Cdrom
DC21X4	DEC DC21X4 Adapter Driver
Disk	Disk

Hardware environment

WELCOME TO ADVANCED DESKTOP MANAGEMENT

Network Topology Event Action Config

210.63.101.244:Hardware Environment

- Basic System Information
- Operating System
- Hardware Environment
- DMI BIOS Information
- I/O Peripheral Information
- Network Information
- System Resource Information
- Storage Information
- Utilization

Chassis, RDM, Fuse

Chassis Status	Normal
RDM Status	Good
Fuse Status	Not Available

Power Status

	Power Supply	Fan
No.#1	Not present	Not present
No.#2	Not present	Not present



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.

Power status

Shows the condition of the power supply and its cooling fan. Whenever either one is not working, an alert is generated.

CPU and system voltage

The voltage for each CPU and system power source is shown here. An alert is generated whenever the voltage is out of range.

Fan status

The fan status is monitored through the hardware module of the system; no user configurable setting exists. An alert is generated whenever the fan is not working.

Temperature

The CPU temperature is monitored in two stages. First Console will give out a warning when a rise in temperature is detected. If the temperature continues to rise, a temperature critical alert is issued. In some models, you can set the threshold values in the BIOS setup.

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.

210.63.101.244: DMI BIOS Information - BIOS

BIOS Vendor	ACER	Starting Address Segment
Release Date	04/29/98	ROM Size
Version	V31 R01-BI-ENT1	

Boot Support	Bus	Other feature Support
<input checked="" type="checkbox"/> Selectable Boot	<input checked="" type="checkbox"/> ISA	<input checked="" type="checkbox"/> Plug and Play
<input checked="" type="checkbox"/> CDROM	<input type="checkbox"/> EISA	<input checked="" type="checkbox"/> Automatic Power Manager
<input type="checkbox"/> PCMCIA	<input checked="" type="checkbox"/> PCI	<input checked="" type="checkbox"/> Upgradable BIOS(Flash)
<input type="checkbox"/> I130	<input type="checkbox"/> MCA	<input checked="" type="checkbox"/> Shadow BIOS
<input type="checkbox"/> LS-120	<input type="checkbox"/> VL-VESA	<input checked="" type="checkbox"/> ESCD
<input type="checkbox"/> ATAPI Zip	<input type="checkbox"/> PCMCIA	<input type="checkbox"/> ACPI
	<input type="checkbox"/> USB	<input type="checkbox"/> Smart Battery
	<input type="checkbox"/> AGP	<input checked="" type="checkbox"/> EDD Specification
	<input type="checkbox"/> USB	<input checked="" type="checkbox"/> BIOS ROM is socketed

Other Device Support

Base board

The Base Board page shows the manufacturer, product name, version and serial number of the base board.


HOME TO ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log View](#)

210.63.101.244: DMI BIOS Information - Base Board

Manufacture	Acer
Product Name	M11E
Version	-1
Serial	

Refresh Set Refresh Interval

 Help

Processor

The Processor page shows the type, speed, version number, and other information about each CPU on the server.

HOME TO ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log View](#)

210.63.101.244: DMI BIOS Information - Processor


CPU

Type	Family	Manufacture	Upgrade	Voltage	External Clock	Current Speed
Central Processor	Other	Intel	Other		100	400

Socket

Socket	PID	Version	Status
51060000m98301		1	CPU Socket: Unpopulated CPU Status: Enabled

Refresh Set Refresh Interval

 Help

Memory

The Memory page displays information about the memory controller and the memory module.

HOME | ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log Vi](#)

210.63.101.244: DMI BIOS Information - Memory

Memory Controller

Error Detect Method	64-bit ECC
Error Correct Capability	Single Bit Error Correcting
Supported Interleave	Unknown
Current Interleave	One Way Interleave
Max. Memory Size	384MB
Memory Module Voltage	3.3V
# of Assoc. Memory Slots	3

Capability

Supported Speed		Supported Memory Type	
<input type="checkbox"/> 50ns	<input type="checkbox"/> Standard	<input type="checkbox"/> SIMM	
<input type="checkbox"/> 60ns	<input type="checkbox"/> Fast Page	<input checked="" type="checkbox"/> DIMM	
<input type="checkbox"/> 70ns	<input type="checkbox"/> EDO	<input type="checkbox"/> Burst EDO	

Cache

The Cache page displays attributes of CPU cache devices.


HOME | ADVANCED DESKTOP MANAGEMENT

[Network Topology](#) [Event Action Config](#) [Event Info Config](#) [Event Log Vi](#)

210.63.101.244: DMI BIOS Information - Cache

Designation	Level	Is Socketed	Location	Status	Mode	Max. Size	Installed Size	Supported SRA Type
SL1	1	No	Internal	Enabled	Write back	32 KB	32 KB	Unknown
SL1,SL1	2	No	Internal	Enabled	Write back	512 KB	512 KB	Pipeline Burst

Refresh Set Refresh Interval

 Help

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.


WELCOME TO ADVANCED DESKTOP MANAGEMENT

Network Topology Event Action Config Event Info Config Event Log View

210.63.101.244: DMI BIOS Information - Slot

Designation	Type	Bus Width	Current Usage	Slot Length	ID	Slot Characteristics
P1	PCI	32bit	In use	Half Length	1	Provide 5.0 Volts
P2	PCI	32bit	In use	Full Length	2	Provide 5.0 Volts
P3	PCI	32bit	In use	Full Length	3	Provide 5.0 Volts
P4	PCI	32bit	Available	Full Length	4	Provide 5.0 Volts
P5	PCI	32bit	Available	Full Length	8	Provide 5.0 Volts
I1	ISA	16bit	Unknown	Full Length	N/A	Provide 5.0 Volts
I2	ISA	16bit	Unknown	Full Length	N/A	Provide 5.0 Volts

Refresh Set Refresh Interval

 Help

Connector

The Connector page displays information about the motherboard connectors.


WELCOME TO ADVANCED DESKTOP MANAGEMENT

Network Topology Event Action Config Event Info Config Event Log View

210.63.101.244: DMI BIOS Information - Connector

Internal	Type	External	Type	P
None	SERIAL PORT 1(C)	DB9 pin male	Serial Port 16650A Com	
None	SERIAL PORT 2(C)	DB9 pin male	Serial Port 16650A Com	
None	PRINTER(CN8)	DB25 pin female	Parallel Port ECP/EPP	
None	KEYBOARD(CN9)	PS/2	Keyboard Port	
None	MOUSE(CN9)	PS/2	Mouse Port	
None	USB Port(CN7)	Other	USB	
None	USB Port(CN7)	Other	USB	

Refresh Set Refresh Interval

 Help

Onboard device

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

The screenshot shows the '210.63.101.3: DMI BIOS Information - Onboard Devices' page. At the top, there are navigation links: [Network Topology](#), [Event Action Config](#), [Event Info Config](#), and [Event Log Vi](#). The main content area features a table with the following data:

Type	Status	Description
SCSI	Enabled	On Board SCSI: Adaptec 7880

Below the table are two buttons: 'Refresh' and 'Set Refresh Interval'. A 'Help' icon is located at the bottom left of the main content area.

I/O peripheral information

Displays Peripheral information like keyboard, mouse, serial ports, parallel ports, video ports, and etc.

The screenshot shows the '210.63.101.3: I/O Peripheral Information' page. At the top, there are navigation links: [Network Topology](#), [Event Action Config](#), [Event Info Config](#), and [Event Log Vi](#). The main content area features a table with the following data:

Keyboard	PS/2
Mouse	PS/2
Serial Port#1	Serial Port 16550A Compatible DB9 pin male
Serial Port#2	Serial Port 16550A Compatible DB9 pin male
Parallel Port	Parallel Port ECP/EPP DB25 pin female
Video Type	VGA/EGA

Below the table are two buttons: 'Refresh' and 'Set Refresh Interval'. A 'Help' icon is located at the bottom left of the main content area.

Network information

This page displays information about some of the network interface cards; not all network cards provide this type of information.

WELCOME TO ADVANCED DESKTOP MANAGEMENT

Network Topology Event Action Config Event Info Config Event Log View System Help Refresh Inter

Domain/Workgroup: DONUT

Basic System Information

Operating System

Hardware Environment

DMI BIOS Information

I/O Peripheral Information

Network Information

System Resource Information

Storage Information

Utilization

Backplane Board

Mylex

IPMI

Basic NIC Controller Information

Type	Model Name	MAC Address	IRQ	I/O Port	Memory Address	DMA	Slot#
Ethernet	Intel(R) 82559 Fast Ethernet LAN on Motherboard	000E22EB0DD	52	0x7080	N/A	N/A	N/A

Additional NIC Controller Information(V4.00 only)

Speed	IP Address	Net Mask	Gateway	NIC Driver	NIC Driver Version
10MB/s	10.34.92.89	255.255.255.0	10.34.92.1	E100BNT.SYS	4.02.23.0000

DNS Table(V4.00 Only)

Index	DNS Server Address
0	10.34.1.250
1	210.63.96.2
2	203.67.198.250
3	210.63.92.1
4	139.175.55.244
5	168.95.1.1

Refresh Set Refresh Interval

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.

Basic System Information

Operating System

Hardware Environment

DMI BIOS Information

I/O Peripheral Information

Network Information

System Resource Information

- IRQ
- DMA
- I/O Port
- Memory
- Resource

Storage Information

Utilization

10.34.92.89: System Resource Information -Resource

Number of Entries: 8

Driver Name	IRQ	DMA	I/O Port	Memory
atapic	14	N/A	01F0-01F7,03F6-03F6	N/A
E100B	52	N/A	7080-709D	88300000-8830001D,88200000-8820001D
Floppy	06	02	03F0-03F5,03F7-03F7	N/A
i804prt	01,12	N/A	0060-0060,0064-0064	N/A
Parport	N/A	N/A	0378-037A	N/A
Serial	04	N/A	03F8-03FE	N/A
Serial	03	N/A	02F8-02FE	N/A
VgaSave	N/A	N/A	03E0-03BB,03C0-03DF,01CE-01CF	000A0000-000BFFFF

Refresh Set Refresh Interval

Help

IRQ information

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.

10.34.92.89: System Resource Information-IRQ

Number of Entries: 7

IRQ	Description
1	i8042prt
3	Serial
4	Serial
6	Floppy
12	i8042prt
14	atapi
52	E100B

Refresh Set Refresh Interval

Help

DMA information

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

10.34.92.89: System Resource Information-DMA

Channel	Description
2	Floppy

Refresh Set Refresh Interval

Help

I/O port information

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

10.34.92.89: System Resource Information-I/O Port

Number of Entries: 47

	Range		Description
	Begin	End	
0x60	0x60		8042prt
0x64	0x64		8042prt
0x378	0x37A		Parport
0x3F8	0x3FE		Serial
0x2F8	0x2FE		Serial
0x7080	0x709D		E100B
0x3F0	0x3F5		Floppy
0x3F7	0x3F7		Floppy
0x1F0	0x1F7		atapi
0x3F6	0x3F6		atapi
0x3C0	0x3CF		S3Inc
0x3D4	0x3DB		S3Inc
0x42E8	0x42E9		S3Inc
0x4AE8	0x4AE9		S3Inc
0x22E8	0x22EB		S3Inc
0x86E8	0x86EB		S3Inc
0x8AE8	0x8AEB		S3Inc

Memory address

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

10.34.92.89: System Resource Information -Memory

Number of Entries: 6

Address	Length	Description
0x83300000 - 0x8330001D	0x1E	E100B
0x83200000 - 0x8320001D	0x1E	E100B
0xA0000 - 0xAFFFF	0x10000	S3Inc
0x4000000 - 0x7FFFFFFF	0x4000000	S3Inc
0xC0000 - 0xC7FFF	0x8000	S3Inc
0xA0000 - 0xBFFFF	0x20000	VgaSave

Refresh Set Refresh Interval

Help

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.

The screenshot shows the 'Storage Information-Physical' page in a web browser. The page title is '210.63.101.3: Storage Information-Physical'. On the left is a navigation menu with categories like Basic System Information, Operating System, Hardware Environment, etc. The main content area shows two controller sections:

- Flppy Controller:** A table with columns 'Drive' and 'Type'. Both drive 'a' and 'b' are listed as 'Not present'.
- AIC78XXC:** A section for 'Controller:' with a table of SCSI devices. Below it is a table for 'Device:' with columns 'Type', 'ID', 'Size(KB)', and 'Model'.

Type	ID	Size(KB)	Model
Hard disk:	0	2345490	FUJITSU M2050Q-512 0142
Hard disk:	1	2094482	SEAGATE ST3201519 0126
Hard disk:	2	2345490	FUJITSU M2050Q-512 0142
Hard disk:	3	4458037	IBM DCRS-34560W 897B
Hard disk:	5	8924107	ACER ACER_AA3102R2 0211

At the bottom of the main content area, there are two buttons: 'Refresh' and 'Set Refresh Interval'. A 'Help' icon is also visible.

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.

The screenshot shows the ASM Management Pages interface. The main content area displays 'Storage Information -Logical' for the host 210.63.101.3. It indicates there are 7 volumes. A table provides details for each volume:

Volume	Total Size(KB)	Free-Size(KB)
MS-DOS_(FAT)C:	104170	85400
NT SYSTEM[NTFS]D:	1028128	298714
ASM&ADM SRC[NTFS]E:	1212875	674661
FTP[NTFS]F:	2337434	239660
VSS[NTFS]G:	4448972	1320000
BACKUP[NTFS]I:	2089416	464032
RAID[NTFS]R:	8916040	2592160

Below the table are buttons for 'Refresh' and 'Set Refresh Interval'. A 'Help' icon is also visible.

Utilization

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

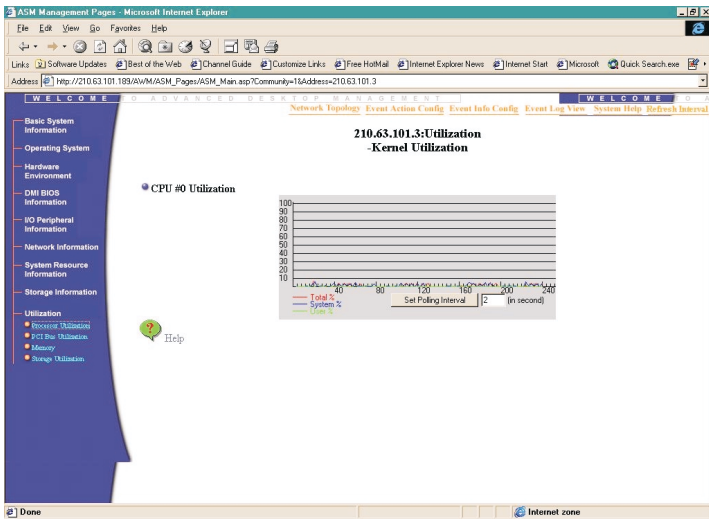
Polling interval

The polling interval determines how frequently the Console polls the Agents to update its data.

To change the polling interval, type the number of seconds and then click **Set Polling Interval**. The polling intervals must be from 1 to 60 seconds.

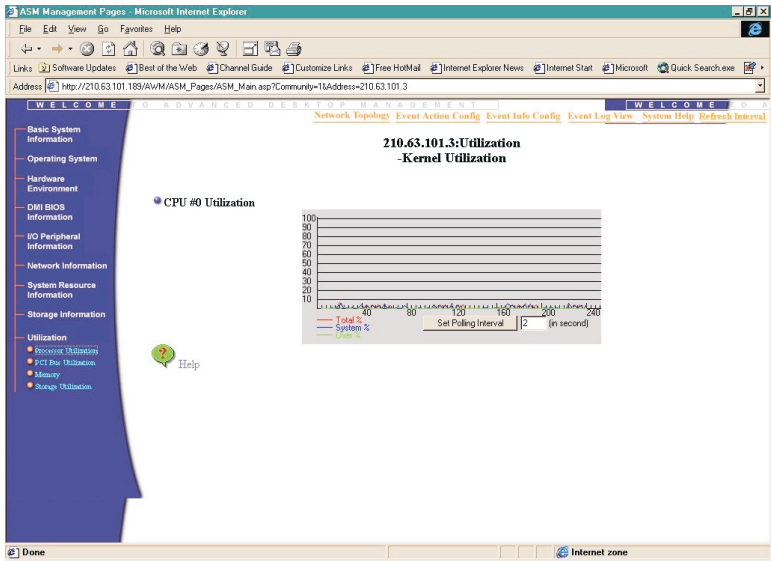
Processor utilization

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.



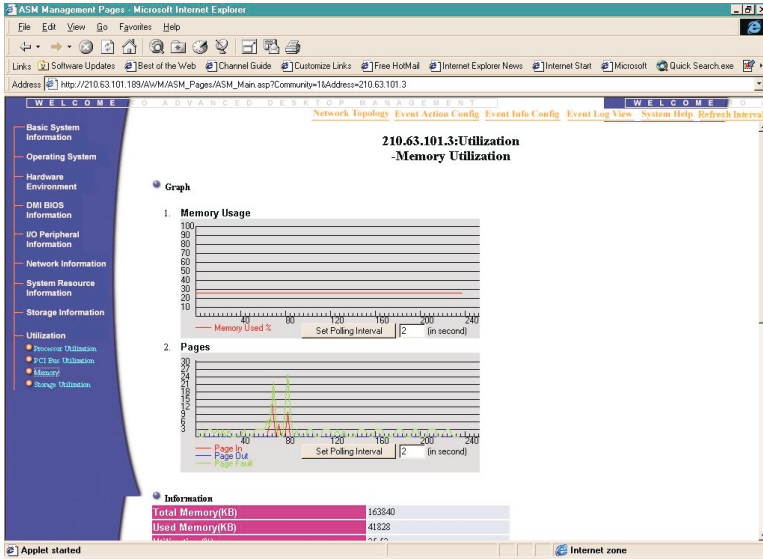
PCI bus utilization

This page displays a line graph showing the current load of each PCI (Central Processing Unit) bus installed in the system.



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.

The screenshot displays the '210.63.101.216:Utilization - Storage Utilization' page. It features a navigation menu on the left and a main content area with two tables and a graph.

Disk Utilization Table:

Disk Type	Disk Busy Ratio	Average Disk R/W Time	Byte Transferred	Number Transferred	Bytes/Read	Bytes/Write	Bytes/Transfer	Seconds/Read	Seconds/Write	Seconds/Transfer	Operations per sec	Read	Write
Hard disk	0	0	0	0	???	???	???	???	???	???	???	???	???
CD-ROM drive	0	0	0	0	???	???	???	???	???	???	???	???	???

File System Utilization Table:

Volume	Total Size(KB)	Used Size(KB)	Utilization(%)	Threshold(%)	Graph
WINNT(C:)	1023824	724480	70.76	100	
APD(D:)	1035920	531536	51.31	100	

Buttons: Submit, Refresh, Set Refresh Interval

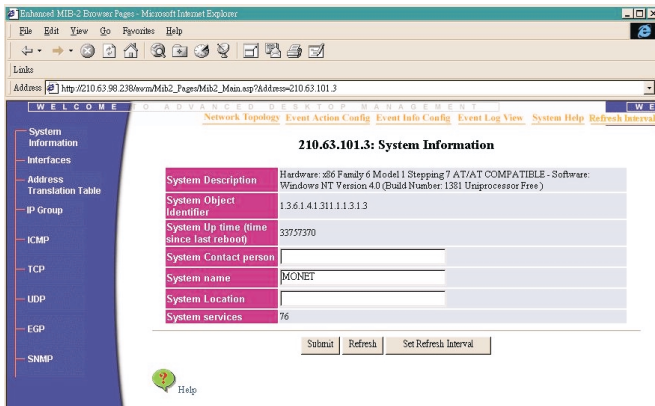
MIB-II configuration information

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.

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.



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

Parameter	Description
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: <ol style="list-style-type: none"> 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.

The screenshot shows a web browser window with the address `http://210.63.98.238/wwn/Mib2_Pages/Mib2_Main.asp?Address=210.63.101.3`. The page title is 'Detailed Interface Information'. The left sidebar contains a navigation menu with the following items: System Information, Interfaces, Address Translation Table, IP Group, ICMP, TCP, UDP, EGP, and SNMP. The main content area displays the following data:

Index	Value
Description	M3 TCP Loopback interface
Media type	softwareLoopback
Administrative status	up
Operational Status	up
Maximum Transmission Unit	1500
Speed(Bits Per Sec)	10000000
Media address	
Status last changed on	0
Input: Bytes received	15483
Input: Unicast packets received	193
Input: Non unicast packets received	0
Input: Discarded packets	0
Input: Receive errors	0
Input: Unknown protocol packets	0
Output: Bytes sent	15483
Output: Unicast packets	193
Output: Non unicast packets	0
Output: Discarded packets	0
Output: Transmit errors	0
Output: Queue length	0
Media specific MIB OID	0.0

At the bottom of the page, there are buttons for '< Go Back', 'Refresh', and 'Set Refresh Interval', along with a 'Help' icon.

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
Speed	The desired state of the interface. The testing (3) state indicates that no operational packets can be passed
Media Address	
Status Last Change	
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

Parameter	Description
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	
Output: Bytes Sent	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
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	
Media Specific MIB OID	

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.

210.63.101.3: Address Translation Table

Interface Index	Media address	Network address
3	210.63.101.1	00:20:9c:08:a7:42
3	210.63.101.109	00:60:67:70:64:5a
3	210.63.101.127	00:00:a2:15:04:18
3	210.63.101.154	00:60:67:08:fa:71
3	210.63.101.157	00:60:67:36:21:5e
3	210.63.101.226	00:20:a4:40:3b:cb
3	210.63.101.244	00:00:a2:03:c7:c1
3	210.63.101.246	00:00:a2:0c:9b:ad

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)

Implementation of the IP group is mandatory for all systems.

IP Protocol configuration page

210.63.101.3: IP Protocol configuration

Forward IP Datagrams Between IP Interfaces?	not-forwarding
Default Value of Time to Live	128

Refresh Set Refresh Interval

Help

IP Statistics page

210.63.101.3: IP Statistics

Input: Datagrams received	1425676
Input: Header errors	26076
Input: Address errors	6742
Input: Datagrams forwarded	0
Input: Unknown protocols	0
Input: Datagrams discarded	0
Input: Datagrams delivered	1399213
Output: Number of datagrams	1341374
Output: Datagrams discarded	0
Output: Number of routing failures	0
Number of discarded datagrams	0
Reassembly requests	0
Reassembly timeouts	60
Reassembly successes	0
Reassembly failures	0
Fragmentation success	0
Fragmentation failures	0
Number of fragments	0

Refresh Set Refresh Interval

Help

IP Address table page

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

Enhanced MIB-2 Browser Pages - Microsoft Internet Explorer

Address: http://210.63.98.238/wvwa/Mib2_Pages/Mib2_Main.asp?Address=210.63.101.3

W E L C O M E O A D V A N C E D W E B - B A S E D M A N A G E M E N T

Network Topology Event Action Config Event Info Config Event Log View System Help Refresh Interval

210.63.101.3: IP Address Table

IP Address	Interface index	Subnet mask	Broadcast Address	Maximum datagram size
127.0.0.1	1	255.0.0.0	1	65535
192.9.210.1	2	255.255.255.0	1	65535
210.63.101.3	3	255.255.255.0	1	65535

Refresh Set Refresh Interval

Help

IP Routing table page

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

Enhanced MIB-2 Browser Pages - Microsoft Internet Explorer

Address: http://210.63.98.238/wvwa/Mib2_Pages/Mib2_Main.asp?Address=210.63.101.3

W E L C O M E O A D V A N C E D W E B - B A S E D M A N A G E M E N T

Network Topology Event Action Config Event Info Config Event Log View System Help Refresh Interval

210.63.101.3: IP Routing Table

Destination	Interface index	Next hop address	Route type	Routing protocol	Age	Routing Mask	Object identifies for routing protocol specific mib	Routing metric 1	Routing metric 2	Routing metric 3	Routing metric 4	Routing metric 5
0.0.0.0	3	210.63.101.1	indirect	local	339603	0.0.0.0	0.0	1	-1	-1	-1	-1
127.0.0.0	1	127.0.0.1	direct	local	339609			1	-1	-1	-1	-1
				local		255.255.255.0	0.0					
192.9.210.1	1	127.0.0.1	direct	local	339603			1	-1	-1	-1	-1
				local		255.255.255.255	0.0					
210.63.101.0	3	210.63.101.3	direct	local	339603			1	-1	-1	-1	-1
				local		255.255.255.255	0.0					
210.63.101.255	3	210.63.101.3	direct	local	339603			1	-1	-1	-1	-1
				local		224.0.0.0	0.0					
255.255.255.255	2	192.9.210.1	direct	local	339603	255.255.255.255	0.0	1	-1	-1	-1	-1

Refresh Set Refresh Interval

Help

Internet zone

IP ARP table page

The screenshot shows the Mikrotik WinBox interface for the IP ARP Table. The browser address bar shows the URL: `http://210.63.98.238/wwn/Mik2_Page/Mik2_Main.asp?Address=210.63.101.3`. The page title is "210.63.101.3: IP ARP Table".

Interface index	Media address	IP Address	Entry type
3	00:20:9e:08:47:42	210.63.101.1	dynamic
3	00:60:67:70:64:5a	210.63.101.109	dynamic
3	00:00:a2:15:e4:18	210.63.101.127	dynamic
3	00:60:67:08:fa:71	210.63.101.154	dynamic
3	00:60:67:36:21:3e	210.63.101.157	dynamic
3	00:20:af:40:3b:cb	210.63.101.226	dynamic

Below the table, there are two buttons: "Refresh" and "Set Refresh Interval". A "Help" icon is also visible.

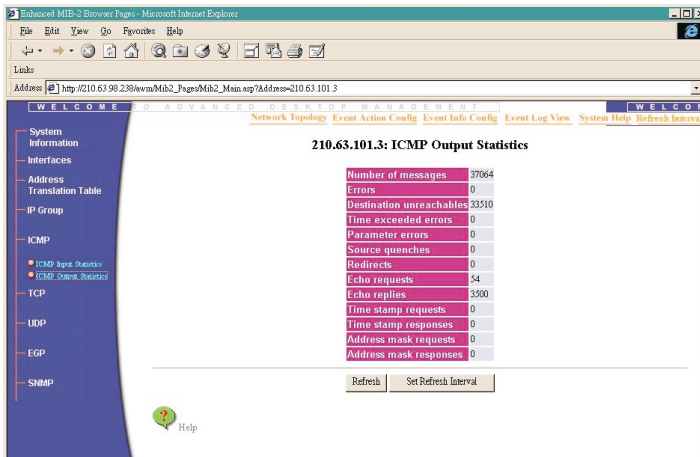
ICMP (Internet Control Message Protocol)

Implementation of the ICMP group is mandatory for all systems.

The screenshot shows the Mikrotik WinBox interface for the ICMP Input Statistics. The browser address bar shows the URL: `http://210.63.98.238/wwn/Mik2_Page/Mik2_Main.asp?Address=210.63.101.3`. The page title is "210.63.101.3: ICMP Input Statistics".

Number of messages	2714
Errors	1
Destination unreachables	186
Time exceeded errors	0
Parameter errors	0
Source quenches	0
Redirects	0
Echo requests	3499
Echo replies	22
Time stamp requests	0
Time stamp responses	0
Address mask requests	0
Address mask responses	0

Below the table, there are two buttons: "Refresh" and "Set Refresh Interval". A "Help" icon is also visible.



Parameter

Description

Input/Output Number of 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 Destination Unreachables

The number of Destination Unreachable messages received/sent.

Input/Output Time Exceeded Errors

The number of Time Exceeded messages received/sent.

Input/Output Parameter Errors

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 Echo Requests

The number of Echo (request) messages received/sent.

Parameter	Description
Input/Output Echo Replies	The number of Echo Reply messages received/sent.
Input/Output Time Stamps Requests	The number of Timestamp (request) messages received/sent.
Input/Output Time Stamp Replies	The number of Timestamp Reply messages received/sent.
Input/Output Address Masks Requests	The number of Address Mask Request messages received/sent.
Input/Output 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

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
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

TCP Connection table page

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

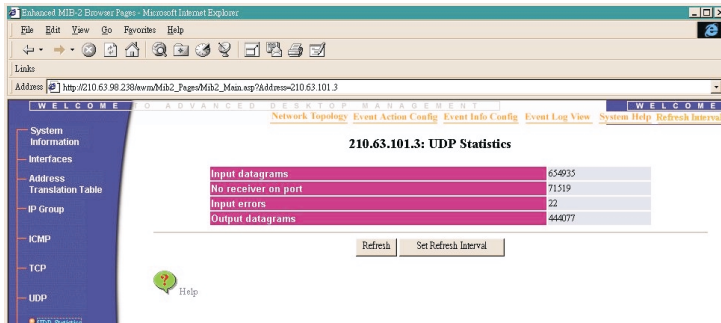
Local Address	Local port	Remote Address	Remote port	Connection state
0.0.0.0	21	0.0.0.0	43129	listen
0.0.0.0	23	0.0.0.0	43100	listen
0.0.0.0	42	0.0.0.0	2146	listen
0.0.0.0	42	0.0.0.0	43162	listen
0.0.0.0	135	0.0.0.0	26830	listen
0.0.0.0	135	0.0.0.0	35016	listen
0.0.0.0	161	0.0.0.0	10326	listen
0.0.0.0	954	0.0.0.0	26705	listen
0.0.0.0	1046	0.0.0.0	51333	listen
0.0.0.0	1049	0.0.0.0	2288	listen
0.0.0.0	1050	0.0.0.0	2224	listen
0.0.0.0	1055	0.0.0.0	2127	listen
0.0.0.0	1057	0.0.0.0	34876	listen
0.0.0.0	3000	0.0.0.0	42227	listen
0.0.0.0	6157	0.0.0.0	59462	listen
127.0.0.1	1038	0.0.0.0	43226	listen
127.0.0.1	1038	127.0.0.1	1046	established
127.0.0.1	1046	127.0.0.1	1038	established
127.0.0.1	1047	0.0.0.0	59619	listen
127.0.0.1	1047	127.0.0.1	1050	established
127.0.0.1	1048	0.0.0.0	18443	listen
127.0.0.1	1050	127.0.0.1	1047	established
127.0.0.1	1056	0.0.0.0	19497	listen
192.9.210.1	137	0.0.0.0	51253	listen
192.9.210.1	138	0.0.0.0	24679	listen
192.9.210.1	139	0.0.0.0	59443	listen
192.9.210.1	139	192.9.210.27	3177	established

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.

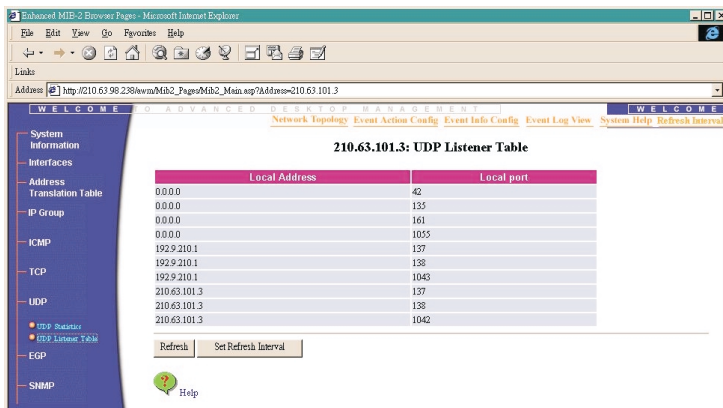
UDP Statistics page



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 endpoints 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

EGP (Exterior Gateway Protocol)

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
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

Parameter	Description
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'
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'

▶ Event action configuration

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 Event Action Configuration link to access the Event Action Configuration page.
2. Type the IP address and then click an event on the left frame.
3. 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 Configure It! button to access the Event Action Configuration page.
2. Enable or disable event actions as you like.

Event Action Configuration - Microsoft Internet Explorer

Address: http://210.63.98.238/awm/EventActionCfg/Start.asp

WELCOME

Network Topology Event Action Config **Event Action Config** Event Log View System Help Refresh Interval

IP Address: 210.63.101.3

Event: All Events

Available Events:

- SNMP
- ASM_PRIVATE_COMM

Event Actions Setup For:
IP=210.63.101.3 and Event=All Events

Browser Notify:

Enable Disable Not Set

Send E-Mail:

Enable Disable Not Set

SMTP Server: 263.net

Mail From: webmaster@company.com

Mail To: webmaster@company.com

Subject: [AWM Event notification]

Call Pager:

Enable Disable Not Set

Telephone Number: 88888888

Message Code: 1234#

Delay: 20 (second)

Submit



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

- 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.

► Event information configuration

The event information configuration allows you to set event name and description. All the events are classified by their type and listed in the left frame in tree view.

To edit sub agents or event type:

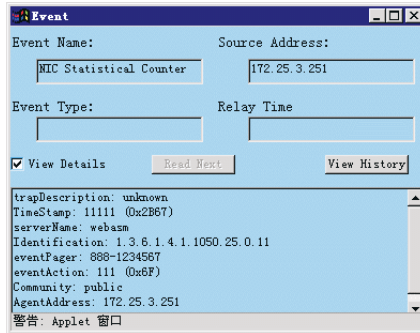
1. Click the subagent name or event type in the left frame to display its form.
2. Edit the contents of the form and then click the Set button to save your changes.



.....
Note: If you change the subagent name or event name, the name list in the left frame won't change until you refreshes the whole page.

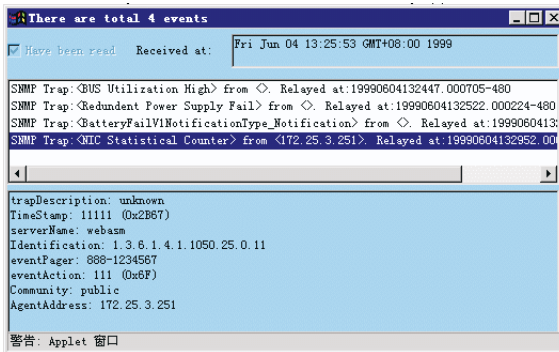
► Real time monitoring

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.



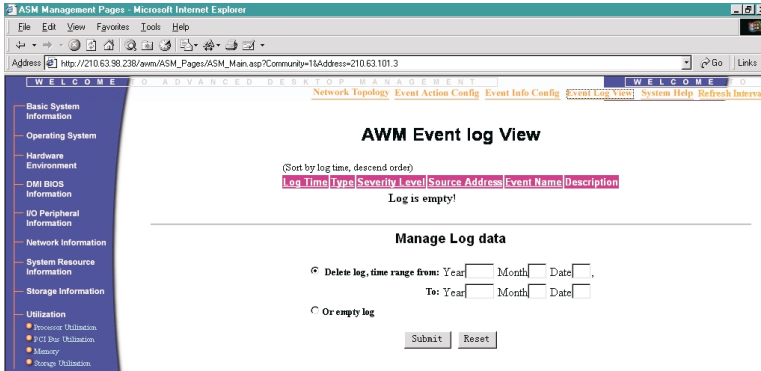
It includes information such as event name, event type, source address, and relay time. To view details, click the View Details checkbox.

To view the event history, click the View History button. The View History window displays.



▶ Event log view

Event Log View gathers event information in the systems being monitored and saves them in the event log file for future reference. To access the Event Log View, click the Event Log view link in the main page. The Event Log View page appears.



Note: You can sort the information in the table by clicking on the table heading.

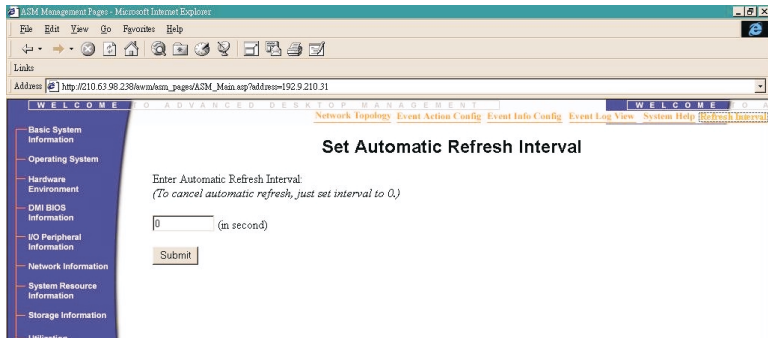
The lower section of the page allows you to delete event logs from the table.

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.

To delete all the log files; Click the Or Empty Log radio button and then click Submit to delete all the log entries.

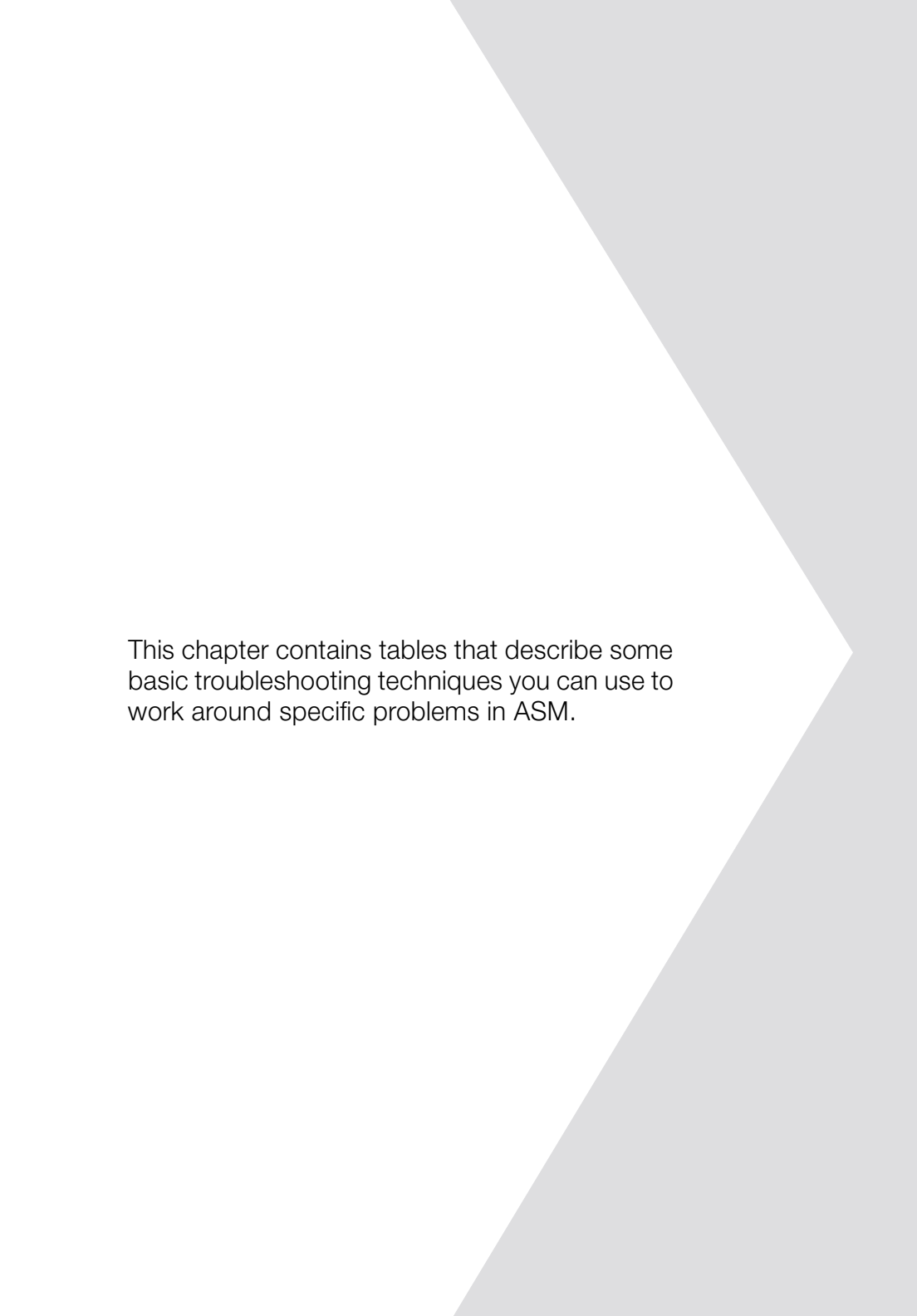
► Setting automatic refresh interval



Type the number of seconds in the textbox to determine the frequency of refreshing information on each page. The refresh intervals must be from 1 to 60 seconds. The default refresh interval is 2 seconds.



A Troubleshooting



This chapter contains tables that describe some basic troubleshooting techniques you can use to work around specific problems in ASM.

► General ASM troubleshooting

The following table describes the error message for different functions in ASM. 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 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 GetSysProductName Address Error	Cannot get GetSysProductName Address from admmisc.dll	Check if admmisc.dll is existent
Utility/CMOS Setup	Call GetSysProductName Error	Cannot call GetSysProductName 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 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	llistat, 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	llistat, 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/m SCSI	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
gethostname 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= fail, xselect	Check /dev/gamdev installed or not 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_alm(), 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 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/netmgmt/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_irqDmaloportMemTable:		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 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 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 Windows NT troubleshooting

Function	Message	Description	Action
ASM AGENT	Cannot Initialize NIC driver	NIC error	Reinstall NIC Adapter/driver
	Cannot create event for SnmpExtension Init	Snmp extended agent error	Reinstall SNMP
ASM 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 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 AGENT	Cannot Initialize NIC driver	NIC error	Reinstall NIC Adapter/driver
	Cannot create event for SnmpExtension Init	Snmp extended agent error	Reinstall SNMP
ASM 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
ASMC1	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 "ASMC1.EXE" will not be loaded	Win32SL service cannot load "ASMNT.MIF". ASMC1.EXE cannot be executed	Reinstall ASM 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 console cannot initialize socket	Please reboot your console system

Function	Message	Description	Action
Asset Manager	Cannot find the asset log file.	ASM 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 MIB Browser	No selected item	No selected query item	Select a query
ASM MIB Browser	No Machine selected!	User didn't select any machine in query	Input machine name
ASM MIB Browser	Please enter an integer between 1 and 60	User input invalid polling interval	Input valid polling interval
ASM MIB Browser	Load Images Error	ASM Browser load MIB data fail. The MIB database maybe corrupted	Initialize MIB database
ASM 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 MIB Browser	User can choose single or table OIDs only
ASM MIB Browser	Number of Table OID exceeds 128	User choose too many OIDs to view	Unselect some OIDs

Function	Message	Description	Action
ASM MIB Browser	Only the single item will be added	When user add a whole subtree into select window. ASM MIB Browser will add the single OIDs under this node	
ASM 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 MIB Browser finds the OIDs defined in this sub-tree are different to the MIB file	Use the same MIB file.
ASM MIB Browser	Can't open initial MIB file	ASM MIB Browser cannot find the initial MIB file, origin.mib.	Search origin.mib and put it into the ASM Console directory.
ASM MIB Browser	Set Operation Fails!	User cannot set the OID value	Check if the OID is protected by password or not.
ASM 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 MIB Browser	This OID is readonly	The access mode of this OID is read-only.	

Function	Message	Description	Action
ASM MIF Browser	Cannot register XXX	ASM 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 MIF Browser	You reach the last row	When user access the the last row for a attributes table	
ASM MIF Browser	Set Operation fails	The set operation for a attribute is failed	
ASM MIF Browser	Can't view different tables together	You want to put attributes in different group to view	Select one group each time
ASM 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 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 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 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

C 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.

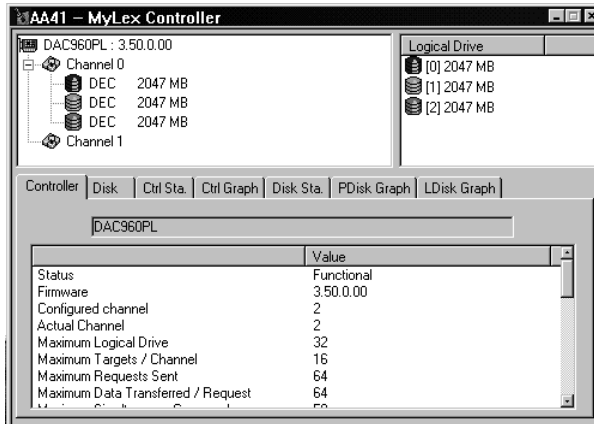
▶ ASM Mylex RAID utility

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.

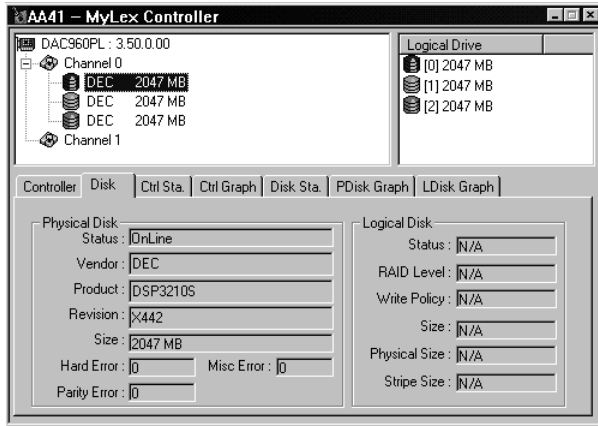
Controller tab

Click the Controller tab to monitor Mylex RAID Controller Information. Click on a controller to show controller information.



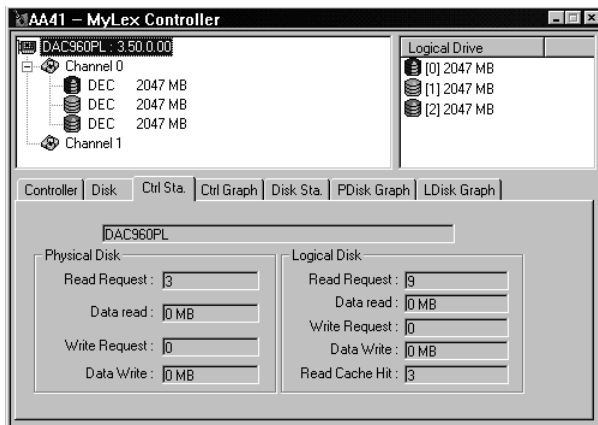
Disk tab

Click the Disk tab to monitor Mylex RAID Controller disk information. Highlight a hard disk to show physical disk information.



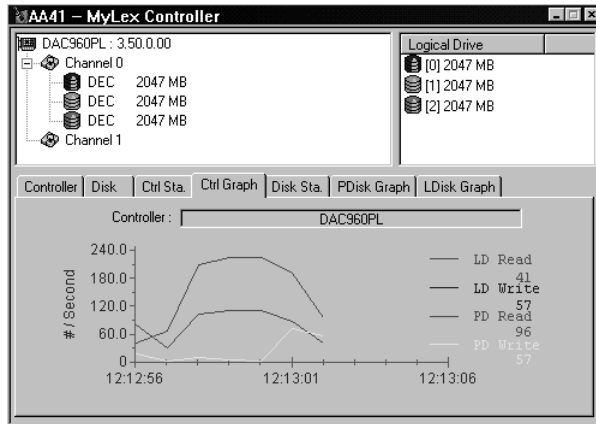
Controller statistic tab

Click the Controller: Statistic tab to monitor Mylex RAID Controller statistics information.

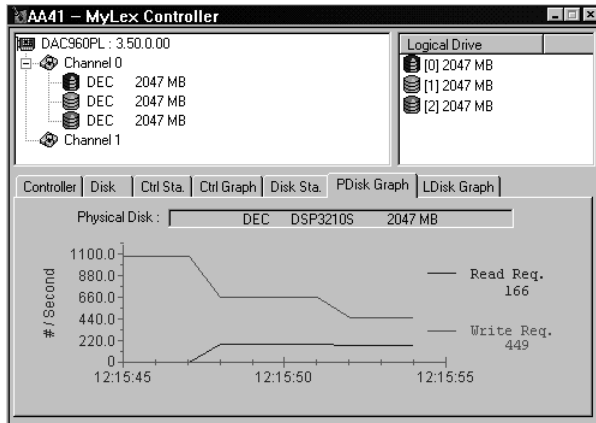


Disk statistic tab

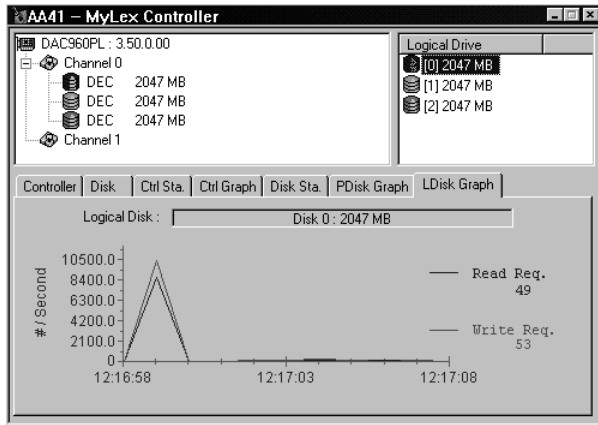
This window is used to monitor Mylex RAID Controller disk statistic information. Under this tab, the displayed information is as shown below:



Physical disk statistic graph tab



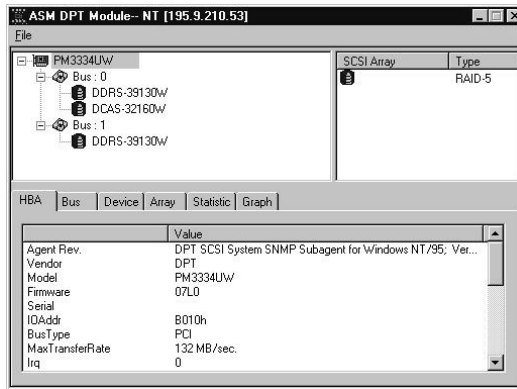
Logical disk statistic graph tab



▶ ASM 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.

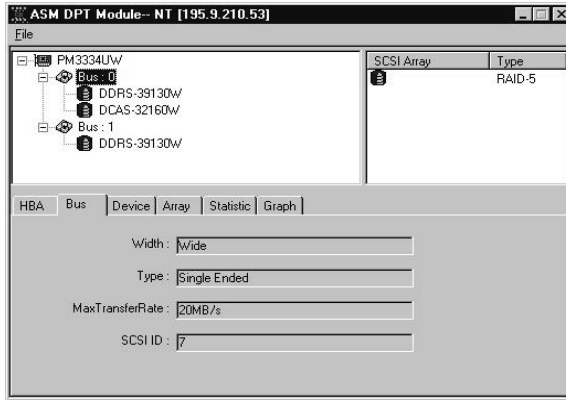
HBA (Host Bus Adapter) tab



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
Bus Type	Host bus type of the computer system to which the HBA is attached to

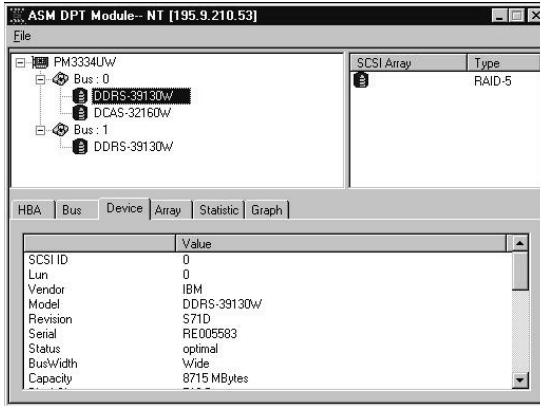
Item	Description
Max Transfer Rate	Maximum possible transfer rate in MB/seconds
IRQ	HBA controller interrupt level
IRQ Type	HBA controller interrupt type
DMA	HBA controller DMA channel. Only applicable if an ISA HBA
RAID Module	HBA Disk Array Module. With the addition of the DM4000 Disk Array Module 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
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

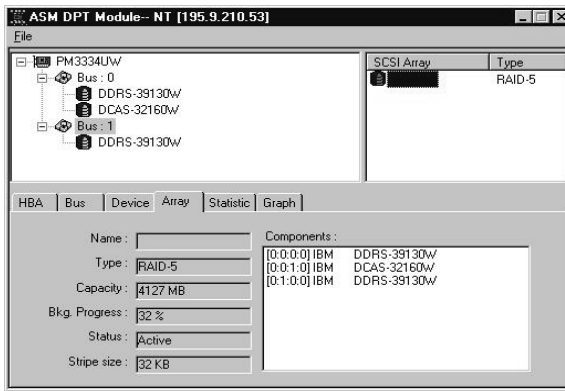


Item	Description
SCSI ID	SCSI ID for the device
LUN	SCSI Logical Unit Number (LUN) for the device
Vendor	Vendor name of the device
Model	Model name of the device
Revision	Device revision level
Serial Number	Device serial number
Status	Administrative state of the device
Bus Width	Value of this object 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)
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

Item	Description
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

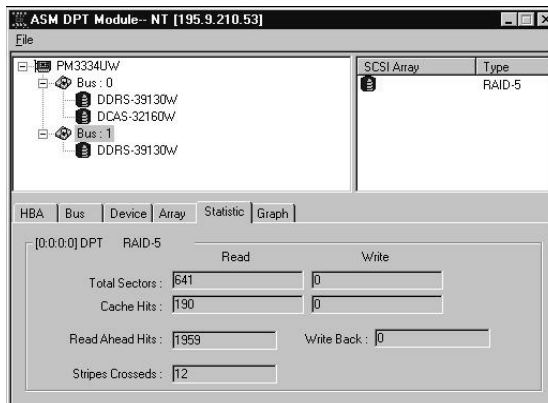
Array tab



Item	Description
Type	RAID Array Group type
Name	Name of the RAID Array Group
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)

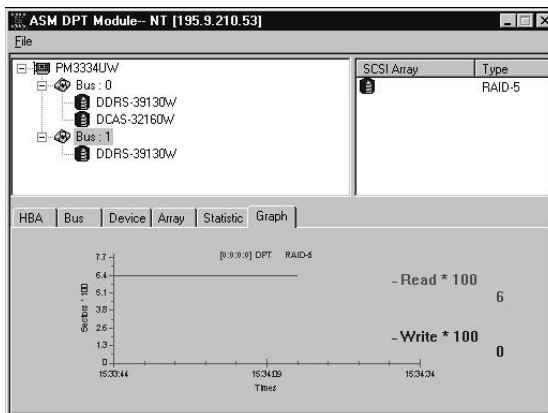
Item	Description
Status	Invalid(1), 'active'(2), which indicates that the conceptual row is available for use by the managed device; 'notInService'(3), which indicates that the conceptual row exists in the agent, but is unavailable for use by the managed device; 'notReady'(4), which indicates that the 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

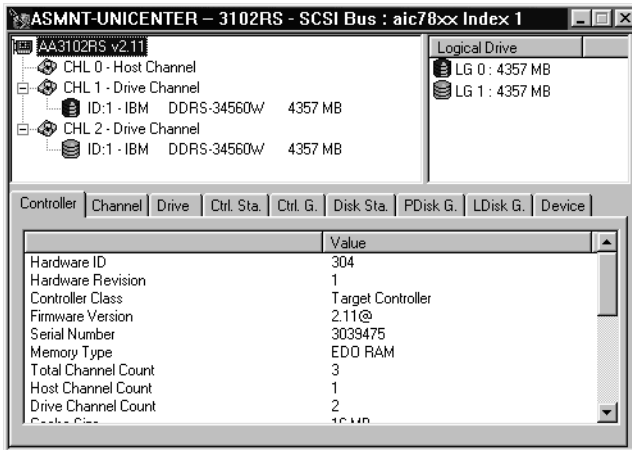
► AcerAltos 3102RS utility

AcerAltos 3102 RAID Controller monitor window

This window is used to monitor the AcerAltos 3102 RAID Controller information. The upper left window displays the hierarchical view of the controller structure, and the upper right window shows the logical drive information.

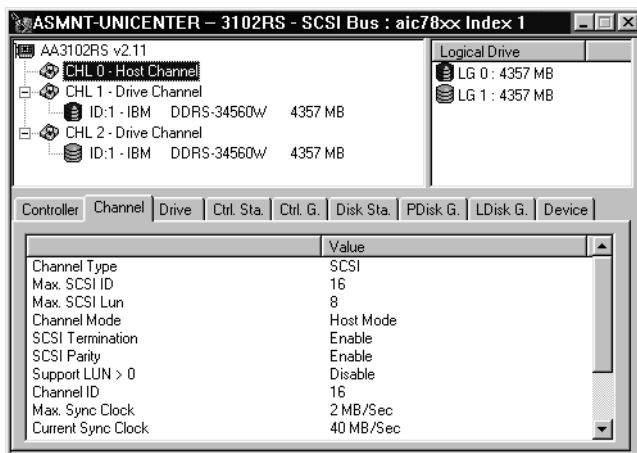
Controller tab

This window is used to monitor the AcerAltos 3102RS RAID Controller Information.



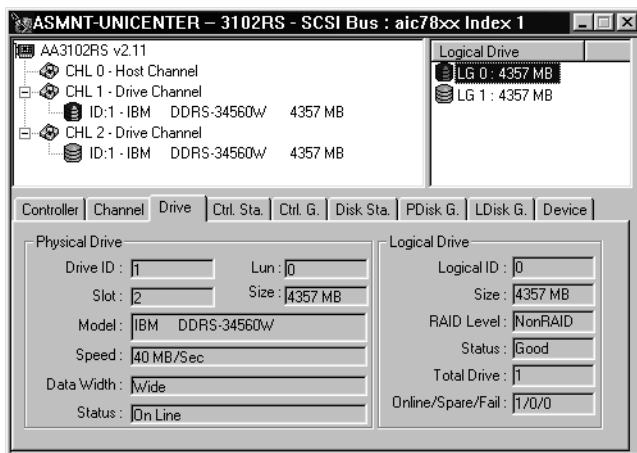
Channel tab

This window is used to monitor the AcerAltos 3102RS RAID Controller Channel information.



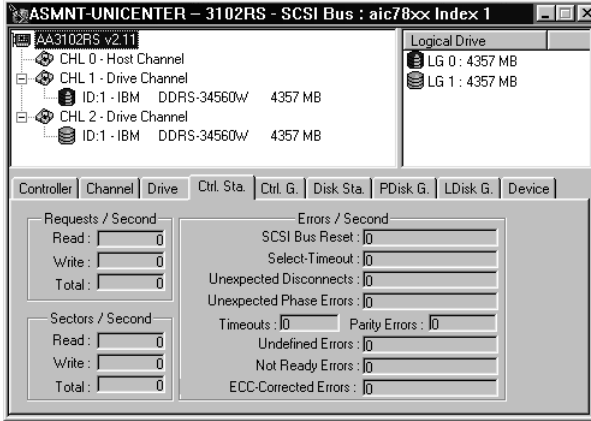
Drive tab

This window is used to monitor the AcerAltos RAS700 RAID Controller Drive information.

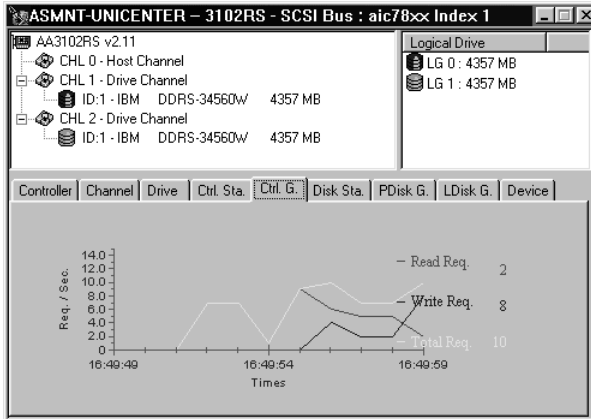


Controller statistic tab

This window is used to monitor the AcerAltos 3102RS RAID Controller Statistic information.

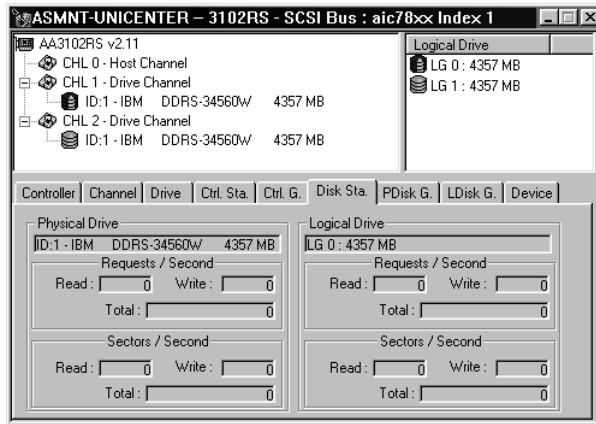


Controller statistic graph tab

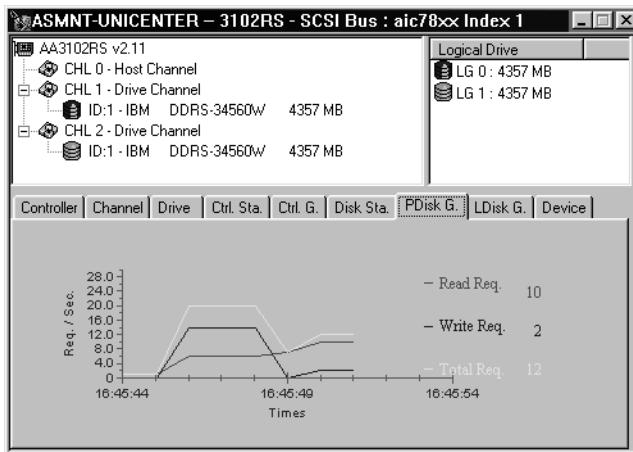


Disk statistic tab

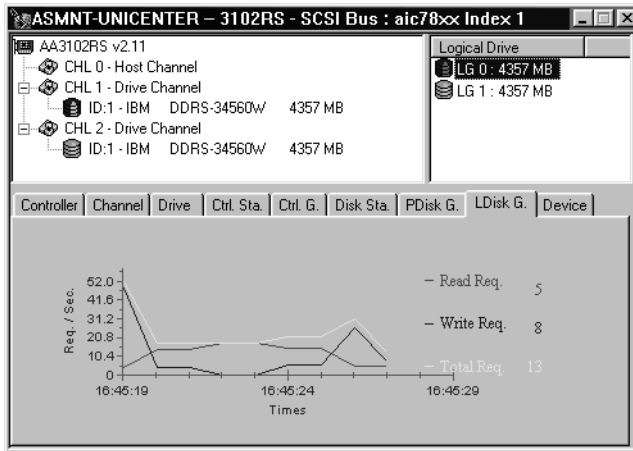
This window is used to monitor the AcerAltos 3102RS RAID Controller Disk Statistic information.



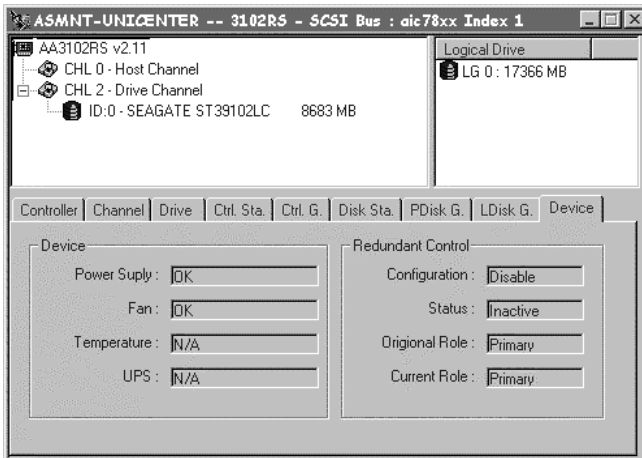
Physical disk statistic graph tab

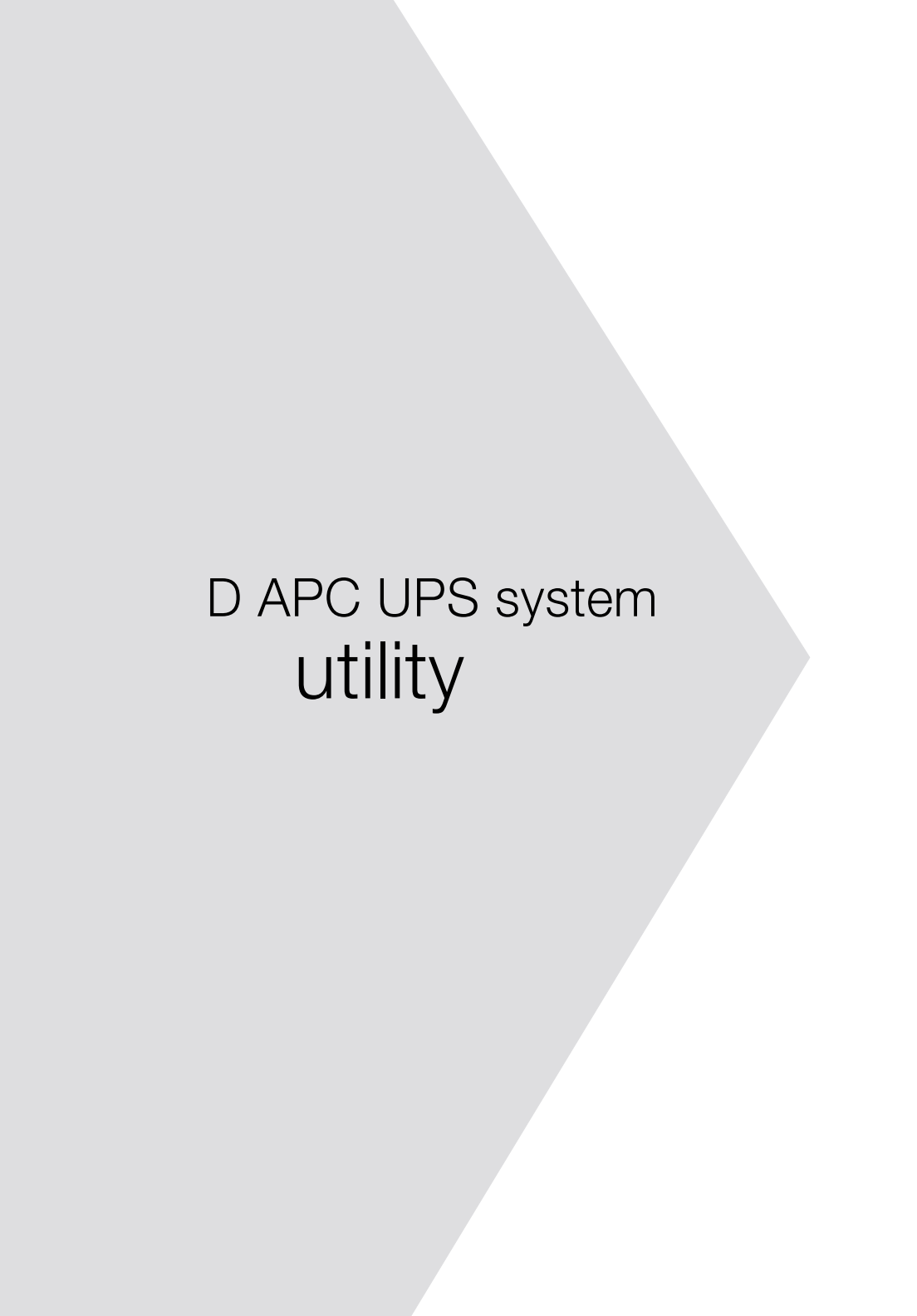


Logical disk statistic graph tab



This window is used to monitor the AcerAltos RAS700 RAID Controller peripheral box information. The displayed information is shown below:



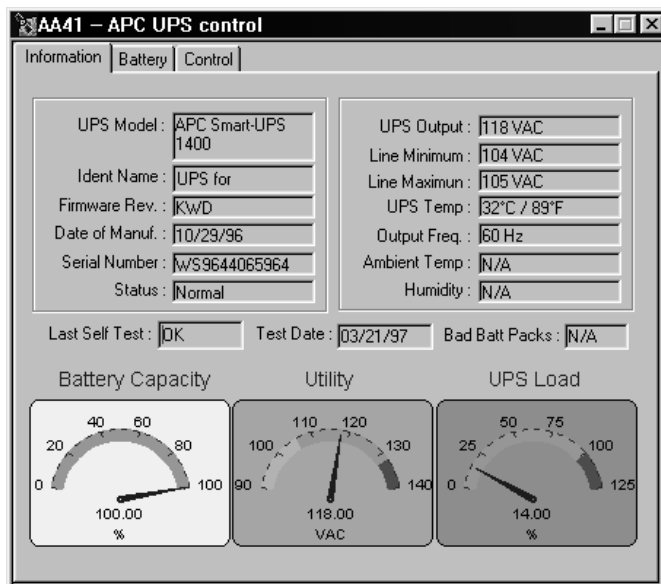


D APC UPS system
utility

If the system has an APC UPS system installed and has the APC UPS system subagent running (for Windows NT and NetWare available right now) then you can monitor and control the APC UPS system remotely through ASM Console.

There are three parts to the APC UPS System Control window: Information, Battery and Control.

Information tab



Item	Description
UPS Model	Model ID of the UPS device
Ident Name	An 8 byte ID string identifying the UPS. This object can be set by the administrator
Firmware Rev.	Firmware revision of the UPS system's microprocessor
Date of Manuf.	Manufacturing date of the UPS in mm/dd/yy format

Item	Description
Serial Number	An 8 byte string identifying the serial number of the UPS internal microprocessor. This number is set at the factory. NOTE: This number does NOT correspond to the serial number on the rear of the UPS
Status	Status of the UPS batteries. Low value indicates the UPS will be unable to sustain the current load, and its services will be lost if power is not restored
UPS Output	Output voltage of the UPS system in VAC
Line Minimum	Minimum utility line voltage in VAC over the previous 1-minute period
Line Maximum	Maximum utility line voltage in VAC over the previous 1-minute period
UPS Temp	Current internal UPS temperature
Output Freq.	Current output frequency to the UPS system in Hz
Ambient Temp	Ambient temperature
Humidity	Relative humidity as a percentage
Last Self Test	Results of the last UPS diagnostics test performed
Test Date	Date the last UPS diagnostics test was performed in mm/dd/yy format
Bad Batt Packs	Number of external battery packs connected to the UPS that are defective. If the UPS does not use smart cells then the value is N/A
Battery Capacity	Remaining battery capacity expressed in percent of full capacity
Utility	Current utility line voltage in VAC
UPS Load	Current UPS load expressed in percent of rated capacity

▶ Battery tab

The screenshot shows the 'AA41 - APC UPS control' window with the 'Battery' tab selected. The window contains the following information:

- Battery Section:**
 - Basic Time: 00:00:00
 - Time Remaining: 01:29:00
 - Last Replace Date: 10/29/99
 - Status: OK (indicated by a battery icon)
 - Need Replace: NO (indicated by two battery icons)
 - Battery Packs:
 - Total: N/A
 - Bad: N/A
- Voltage Section:**
 - Input:
 - Phase: 1
 - Voltage: 105 VAC
 - Frequency: 60 Hz
 - Output:
 - Phase: 1
 - Voltage: 118 VAC
 - Frequency: 60 Hz
 - Input Line Fail Case: Brown out
 - Output Status: On Smart boost
 - Input Max Line Voltage: 105 VAC
 - Output Load: 14 %
 - Input Min Line Voltage: 104 VAC
 - Output Current: N/A

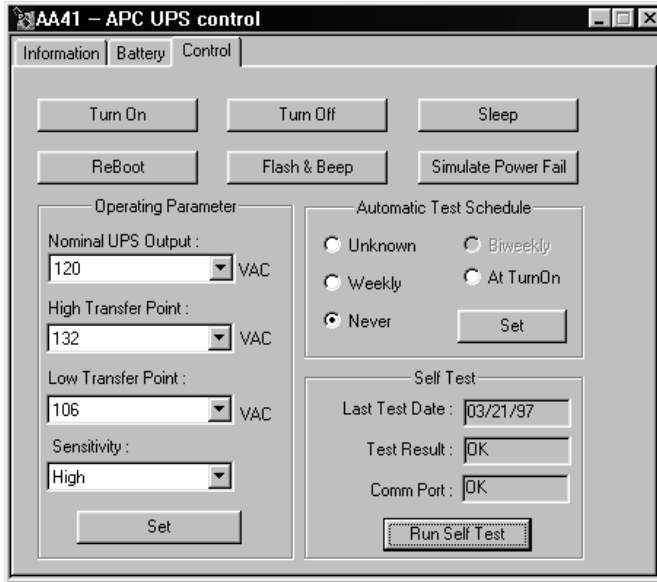
Item	Description
Basic Time	Elapsed time since the UPS has switched to battery power
Time Remaining	UPS battery run time remaining before battery exhaustion
Last Replace Date	Date when the UPS system's batteries were last replaced in mm/dd/yy format. For Smart-UPS models, this value is originally set in the factory. When the UPS batteries are replaced, this value should be reset by the administrator
Status	Unknown, OK, or Low for status of UPS batteries
Need Replace	Indicates whether the UPS batteries need replacing

Item	Description
Battery Packs/ Total	Number of external battery packs connected to the UPS. If the UPS does not use smart cells then the value is N/A
Battery Packs/ Bad	Number of external battery packs connected to the UPS that are defective. If the UPS does not use smart cells then the value is N/A
Phase	Current input/output phase
Voltage	Input/output voltage of the UPS system in VAC
Frequency	Current input/output frequency to the UPS system in Hz

Item	Description
Input Line Fail Case	<p>The reason for the occurrence of the last transfer to UPS battery power. The variable is set to:</p> <p>NoTransfer(1) if there is no transfer yet</p> <p>HighLineVoltage(2) if the transfer to battery is caused by an over voltage greater than the high transfer voltage</p> <p>Brownout(3) if the duration of the outage is greater than five seconds and the line voltage is between 40% of the rated output voltage and the low transfer voltage</p> <p>Blackout(4) if the duration of the outage is greater than five seconds and the line voltage is between 40% of the rated output voltage and ground</p> <p>SmallMomentarySag(5) if the duration of the outage is less than five seconds and the line voltage is between 40% of the rated output voltage and the low transfer voltage</p> <p>DeepMomentarySag(6) if the duration of the outage is less than five seconds and the line voltage is between 40% of the rated output voltage and ground</p> <p>SmallMomentarySpike(7) if the line failure is caused by a rate of change of input voltage less than ten volts per cycle</p> <p>LargeMomentarySpike(8) if the line failure is caused by a rate of change of input voltage greater than ten volts per cycle</p>
Output Status	<p>The current state of the UPS. If the UPS is unable to determine the state of the UPS this variable is set to unknown(1). There are 12 defined values:</p> <p>unknown(1) off(7)</p> <p>onLine(2) rebooting(8)</p> <p>onBattery(3) switchedBypass(9)</p> <p>onSmartBoost(4) hardwareFailureBypass(10)</p> <p>timedSleeping(5) sleepingUntilPowerReturn(11)</p> <p>softwareBypass(6) onSmartTrim(12)</p>

Item	Description
Input Max Line Voltage	Maximum utility line voltage in VAC over the previous 1-minute period
Input Min Line Voltage	Minimum utility line voltage in VAC over the previous 1-minute period
Output Load	Current UPS load expressed in percent of rated capacity
Output Current	Current in amperes drawn by the load on the UPS

► Control tab



Item	Description
Turn On	Pressing this button causes the UPS to be turned on immediately. This action is only available with the APC Mini-SNMP Adapter
Turn Off	Pressing this button causes the UPS to shut off. When in this state, the UPS will not provide output power regardless of the input line state. The ON/OFF switch on the UPS must be toggled for the UPS to return to operation
Sleep	Pressing this button causes the UPS to go to sleep. When in sleep mode, the UPS will not provide output power regardless of the input line state. Once the specified time has elapsed, output power will be restored

Item	Description
Reboot	Pressing this button causes the UPS to shut off and turn back on
Flash & Beep	Pressing this button to cause the UPS to beep and at the same time turn on the UPS front panel lights (Smart-UPS only)
Simulate Power Fail	Pressing this button causes the UPS switch to battery power
Operating Parameter/ Nominal UPS Output	<p>The nominal output voltage from the UPS in VAC. Possible values are 100, 120, 208, 220, 225, 230 and 240</p> <p>NOTE: Only units that are 220, 225, 230 and 240 can be changed. Allowable set values are 220, 225, 230, and 240</p> <p>For these adjustable units, if a value other than a supported value is provided in a set request, the UPS interprets it as the next lower acceptable value. If the provided value is lower than the lowest acceptable value, the lowest acceptable value is used</p>
Operating Parameter/High Transfer Point	<p>The maximum line voltage in VAC allowed before the UPS system transfers to battery backup</p> <p>Allowed values depend on the UPS used:</p> <ul style="list-style-type: none"> 100 volt units allow settings of 108, 110, 112, and 114 120 volt units allow settings of 129, 132, 135, and 138 208 volt units allow settings of 224, 229, 234, and 239 230 volt units allow settings of 253, 264, 271, and 280 <p>NOTE: Matrix units configured for 208V input allow settings of 240, 244, 248, and 252. Matrix units configured for 240V input allow settings of 276, 264, 253, and 282. If a value other than a supported value is provided in a set request, the UPS interprets it as the next lower acceptable value. If the provided value is lower than the lowest acceptable value, the lowest acceptable value is used</p>

Item	Description
Operating Parameter/Low Transfer Point	<p>The minimum line voltage in VAC allowed before the UPS system transfers to battery backup</p> <p>Allowable values depend on the UPS used:</p> <ul style="list-style-type: none"> 100 volt units allow settings of 81, 83, 85, 87 120 volt units allow settings of 97, 100, 103, 106 208 volt units allow settings of 168, 172, 177, 182 230 volt units allow settings of 188, 196, 204, 208 <p>NOTE: Matrix units configured for 208V input have a fixed low transfer voltage of 156 volts. Matrix units configured for 240V input have a fixed low transfer voltage of 180 volts. If a value other than a supported value is provided in a set request, the UPS interprets it as the next higher acceptable value. If the provided value is higher than the highest acceptable value, the highest acceptable value is used</p>
Operating Parameter/Sensitivity	Sensitivity of the UPS to utility line abnormalities or noises
Automatic Test Schedule	UPS system's automatic battery test schedule
Self Test/Last Test Date	Date the last UPS diagnostics test was performed in mm/dd/yy format
Self Test/Test Result	Results of the last UPS diagnostics test performed
Self Test/Comm Port	Status of agent's communication with UPS



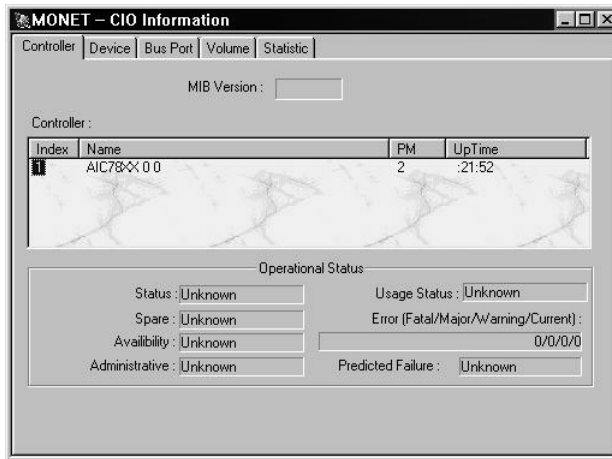
E ASM Adaptec CI/O
utility

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.

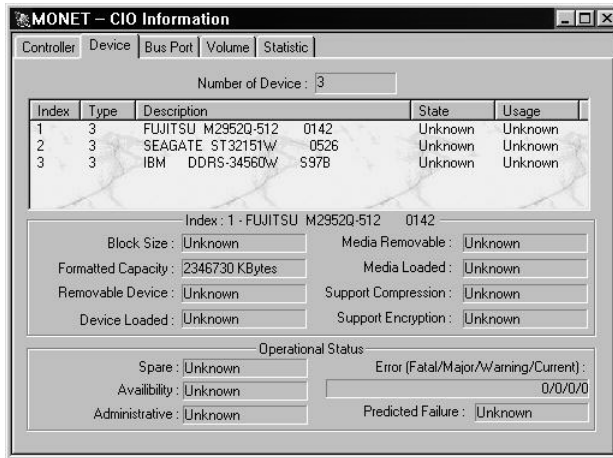
Controller tab

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

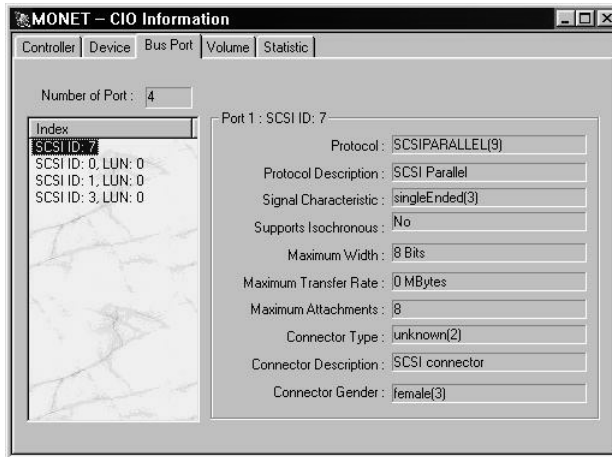


This window is used to monitor the Adaptec C/I/O Device Information. Under this tab the displayed information is as shown below:

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

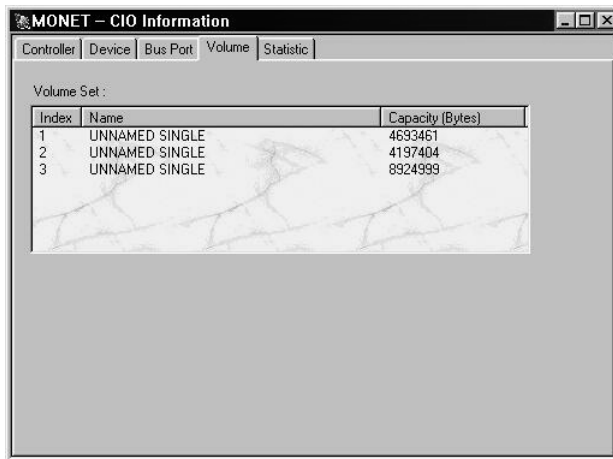


This window is used to monitor the Adaptec CI/O Controller Device information. Under this tab, the displayed information is as shown below:

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



MONET - CIO Information

Controller | Device | Bus Port | **Volume** | Statistic

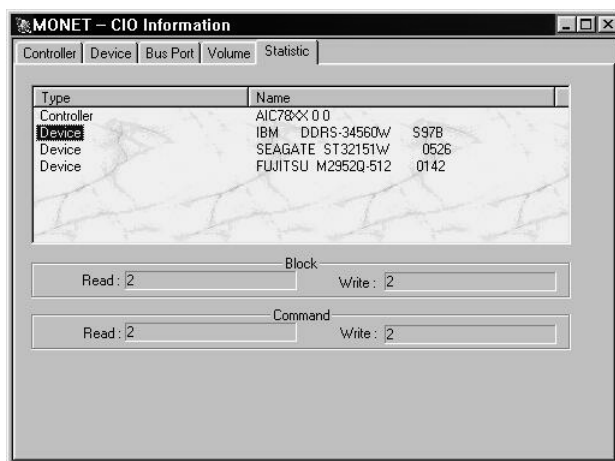
Volume Set :

Index	Name	Capacity (Bytes)
1	UNNAMED SINGLE	4693461
2	UNNAMED SINGLE	4197404
3	UNNAMED SINGLE	8924999

This window is used to monitor the Adaptec CI/O Volume information. Under this tab, the displayed information is as shown below:

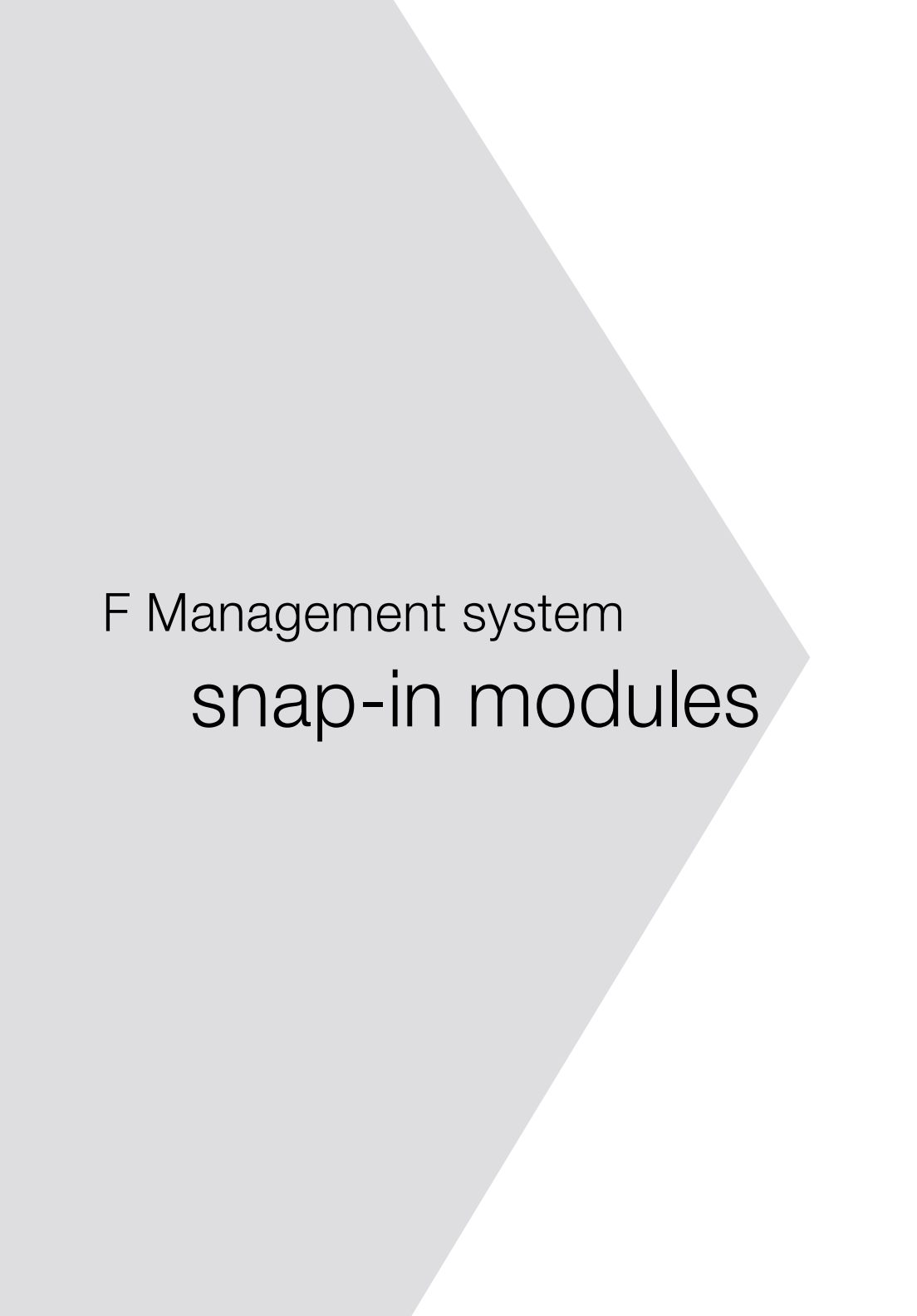
Item	Description
Index	A unique index value for each volume set beginning with 1
Name	The name of the volume set
Capacity	The total size in bytes of the user data space of this volume set

Statistic tab




This window is used to monitor the Adaptec C/I/O 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



F Management system
snap-in modules



This appendix describes how to install and use various Snap-in modules with the management system.

► CA Unicenter TNG



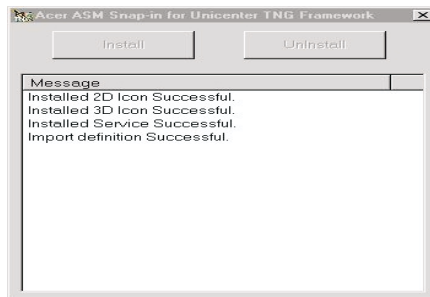
Note: Before installing the snap-in module, make sure that the CA Unicenter TNG Framework and ASM Console have been installed.

To install the snap-in module, run Setup.exe from the installation CD under the directory \Console\CA\ to install/uninstall the ASM snap-in module.

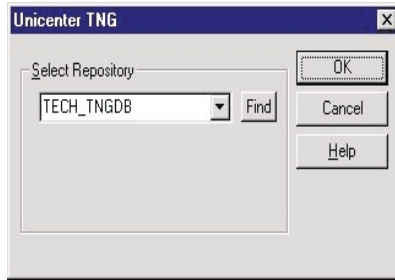
This module creates classes and objects in the repository of Unicenter TNG. The ASM Agent object is created automatically when a new host is added into the repository (manually added or by auto discovery).

To launch ASM Console from Unicenter WorldView:

1. Find the node you want to monitor.
2. Double-click the node's icon.



3. Right-click the ASM Agent's icon and launch ASM Console from the context menu.



If ASM Agent is previously installed, an ASM Agent's icon will appear.

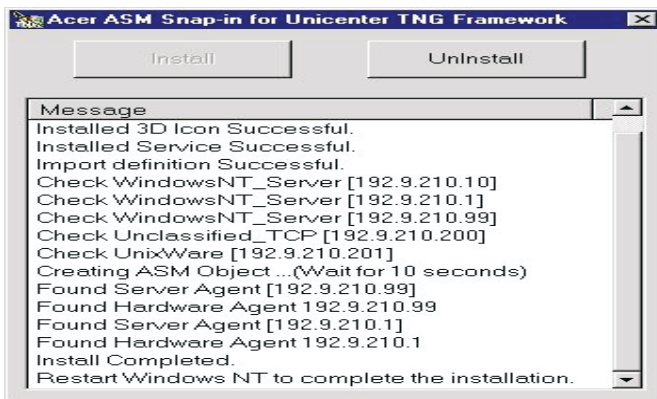
▶ HP OpenView



Note: Before installing the snap-in module, make sure that the HP OpenView Network Node Manager and ASM Console have been installed.

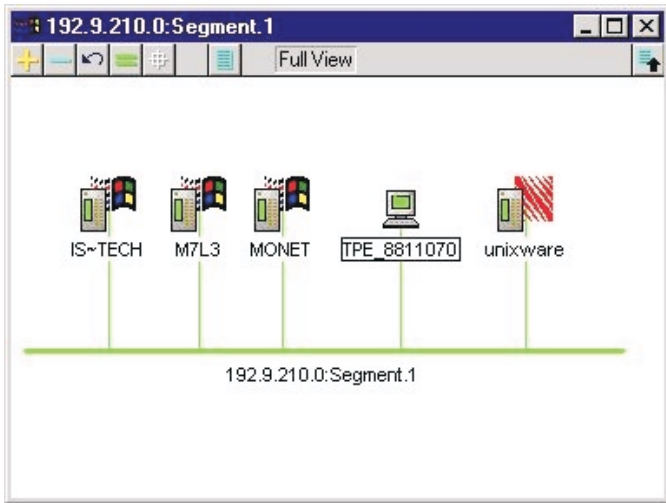
To install the snap-in module, run Setup.exe from the installation CD under the directory \Console\OpenView\.

Launch HP OpenView Management Console and select the "Misc\ASM/ADM Snap in:ASMMon" menu item to auto-discover ASM machines. Select one ASM machine and then click on the Tools > ASM menu. The ASM Console launches.



Intel LDCM

Before launching LCDM from ASM Console, make sure that Intel LDCM has been installed in the system you want to monitor.



The ASM Console auto-detects the existence of Intel LDCM in the system. If LDCM was installed, ASM Console automatically adds a menu item in the Tools menu.

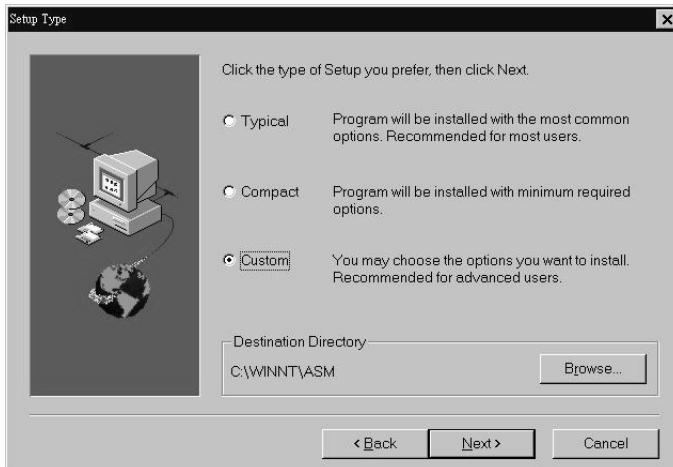
► MMC (Microsoft Management Console)

The MMC snap-in module is included in the ASM Server Agent installation when installed in Windows NT servers.

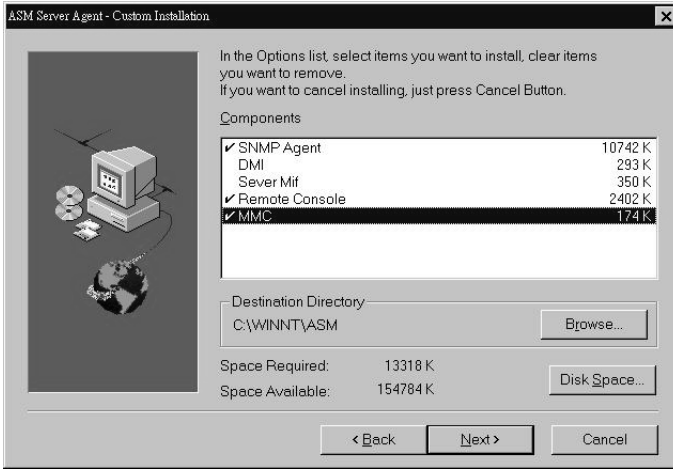
Follow the setup wizard during installation and click the Next button to go to the next page. You can also click the Back button to go back to the previous screen. Choose MMC when prompted to install snap-in components. A check indicates that the snap-in component will be installed into your machine.

To install and run the MMC:

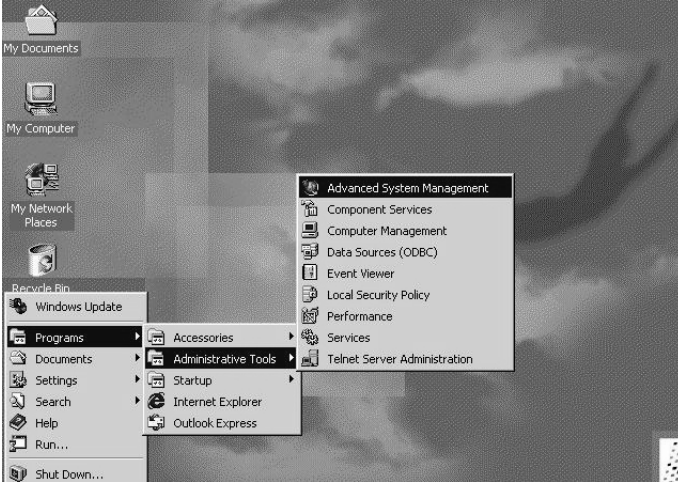
1. Choose Custom setup and then click Next.



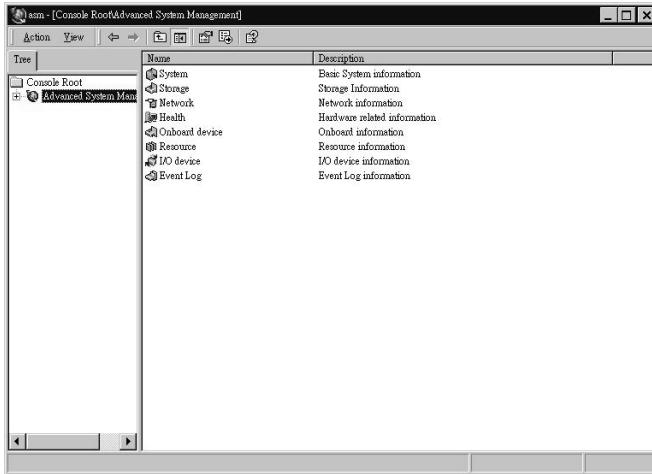
- Click MMC and then click Next.



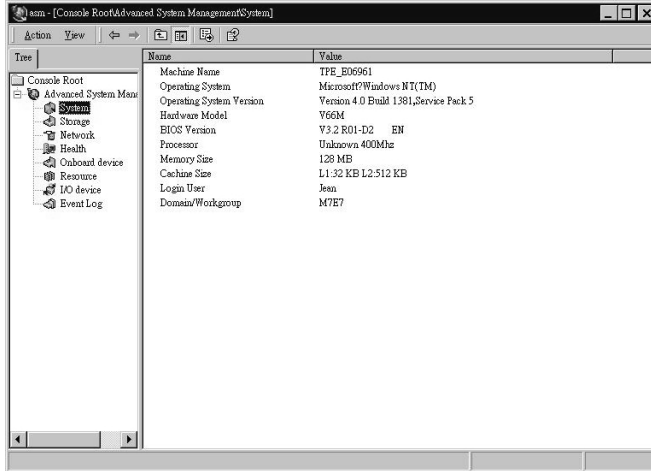
- To run MMC, click the Start button in Windows NT and then choose Programs, Administrative Tools, and then Advanced System Management.



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 206
 - I/O Device Information 209
 - LAN Adapter, TCP/IP and Modem setting 199
 - Physical and Partition Information 196
 - Resource 208
 - System Health Status 204
 - System Performance Information 201
- 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 13
 - installing SCO Openserver Agent 15
 - installing SCO Unixware Agent

- 17
- 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
- asmcfg for SCO UnixWare
 - Config>ASM_Password 166
 - Config>Event_Actions 168
 - Config>Manager_Info 167
 - Config>SNMP 165
 - Config>Threshold 167
- asmcfg 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, 128
 - Hardware Errors 129

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
 - managing 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 108
 - ICMP 116, 425
 - Internet Control Message Protocol 116, 425
 - Internet Protocol 113, 422
 - IP 113, 422
 - Simple Network Management Protocol 122
 - SNMP 122
 - System 108
 - TCP 118, 427
 - Transmission Control Protocol 118, 427
 - UDP 121, 429
 - User Datagram Protocol 121, 429

- Microsoft Windows NT
 - installation 18

- MIF 3
- MIF Browser
 - running 239
 - what is... 3, 239

N

- Network 2
- Novell Netware Agent
 - installation 13

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 17
- 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, 411
- 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