

Acer Server Manager

(ASM6)

User's Guide

Copyright © 2004 Acer Inc.
All Rights Reserved

ASM 6.0 User's Guide
Original Issue: March 2004

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.

The information in this User's Guide is provided "as is" and Acer disclaims any and all warranties, express or implied or statutory, including but not limited to the implied warranties of merchantability for fitness for a particular purpose.

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.

Notice

Warranty and 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. 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.

The software license(s) that accompanies your computer system is for use 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, (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.

Table of Contents

Notice 1

Warranty and Limitation of Liability 1

Table of Contents 2

1 Introduction 1

ASM Overview 1

ASM 6.0 (ASM6) Features 2

Using This Guide 2

Frequently Used Terms 2

2 Installing ASM6 5

ASM6 System Requirements 5

System Requirements for ASM6 Agents 5

System Requirements for ASM6 Console 5

Installing ASM6 Agents 6

Installing ASM6 Windows Agents 6

Setting SNMP Configuration 8

Installing ASM6 Linux Agents 9

Installing ASM6 Console 10

Uninstalling ASM6 12

Uninstalling ASM6 Windows Agent 12

Uninstalling ASM6 Linux Agent 12

Uninstalling ASM6 Console 12

3 Quick Guide 13

Starting ASM6 13

ASM6 Console Interface 13

Managed Systems 15

Management Functions 15

Working Area 16

4 Using ASM6 17

Discovering 17

Setting up Subnet 17

Setting Up Discovery Schedule 18

Setting Up Filter 19

History	20
Managing System List	20
Adding a System	21
Searching for a System	22
Deleting a System	23
Adding a Group	24
Deleting a Group	25
Right Clicking on a Target System	26
Authentication	30
Global Authentication Options	30
Authentication Option for a Selected System	31
Viewing System Properties	32
Monitoring System Health	33
Underlying Technology	33
System Health Monitor Interface	35
System Health Monitoring with IPMI / BMC	38
System Health Monitoring with ASM6 Agent	40
Monitoring System Configuration	40
Launching System Monitor	41
System Monitor Interface	42
Storage	44
Managing Through Web Access	46
Launching Web Viewer	46
Adding a URL	46
Using External Tools	46
Adding a New Tool	46
Deleting a Tool	47
Monitoring MegaRAID	47
Monitoring ARMC	49
5 ASM6 Event Manager	51
ASM6 Event Viewer	51
Launching Event Viewer	51
Event Viewer User Interface	52
Viewing Events	52
Event Rules	53
Using Wizard to Create Event Rule	53
Creating Event Rule in Advanced Mode	59
Modifying Event Rule	64
6 Remote Management	67

- Remote Console Overview 67
- ASM6 Remote Admin Console 68
- ASM6 Remote Windows Console 70
- ASM6 Remote Linux Console 72
- Using Terminal Services Console 75
 - Connecting to terminal services 75
 - Using shortcut keys 78
 - Remote Copy, Local Paste 78
 - Remote Application, Local Printing 78
 - Closing Terminal Services Console 79

7 Frequently Asked Questions 81

8 Appendix 85

- Port List 85
 - Port Number List: 86
- Broadcom's ASF Configuration Utility 87

1 Introduction

Congratulations on your purchase of an Acer Altos server, and welcome to the Acer Server Manager (ASM), part of the Acer manageability solution for servers.

Whether your Altos server is going to be used for mission critical applications or as a departmental server, server downtime is becoming more costly and less tolerable nowadays. That is the main reason ASM was designed and is provided to you. The software performs a set of server management functions that monitor and manage your server configuration, operational status, performance indexes, environment health, critical and pre-failure alerts, etc. With the built-in management capabilities, ASM allows the server administrator to remotely manage the server with ease.

This User's Guide is designed to familiarise you with set up and operation procedures, whether you are a first-time user or experienced user looking for specific information. The introduction provides an overview of ASM and the ASM 6.0 features.

ASM Overview

ASM is a set of server and network management software that allows you to spot operational problems or potential malfunctions in servers in a network environment without sacrificing efficiency.

ASM software consists of two major parts: an ASM management console (ASM console) and ASM system agents (ASM agents). The ASM console can be used to monitor all of the managed server systems in the network in which ASM agents have been installed. The ASM agents are the software programs installed on each of the managed server systems in the network that collect and report the information about the managed server systems back to the ASM console.

With ASM, administrators can monitor the operational health and resource utilization of server systems, locally and remotely. The ASM Console has Graphic User Interfaces to facilitate monitoring of critical indicators, including but not limited to: processor / memory / network / hard disk utilization, health monitoring sensors, and event alert notifications.

From ASM Console, the system administrator can monitor any targeted server on the network, provided ASM Agent has been properly installed on that server. When the system administrator selects a system from the managed system list in ASM Console, ASM Console will query the Agent on the managed system, then the Agent will collect information and send it back to the Console. The administrator can then read and interpret the information from the ASM console and take the desired/appropriate management actions.

ASM 6.0 (ASM6) Features

The main features of ASM6 include:

- **Discovery** ---- The administrator can specify an IP address range, and ASM6's discovery engine will search for available systems in the address scope and display the list of discovered systems in the managed system area of the ASM Console. Allows administrators select desired nodes for management.
- **Retrieve System Information** ---- ASM6 allows the user to view hardware, operating system, performance, resource utilization and alerting events information about the system under management.
- **Alerts** ---- ASM Console serves as an alert center. Pre-defined events that occur on all managed nodes are forwarded to the ASM Console. Pre-defined actions can also be assigned alerts, including: pop-up message box, audio alarm, executing a program on the ASM Console, and e-mailing a list of recipients.
- **Remote Management** ---- The administrator can terminate processes that are running on managed systems, shutdown, reset and power on managed systems. Administrators can also operate managed systems remotely with the remote management functions.
- **Unified User Interface** ---- The Console user interface provides a dynamic display of related menu items and management functions in a unified setting, allowing administrators to easily switch views from various managed nodes with different management functions.

Using This Guide

This guide is to help both the new user and experienced reader understand and use ASM6. The guide is divided into seven sections as follows:

- Introduction
Overview and introduction of ASM6 functions and features
- Installing and Uninstalling ASM6
Installation procedures for ASM6
- Configuring and Running ASM6
Quick guide for ASM Console use
- Using the Management Functions
Description of the ASM6 management functions
- Frequently Asked Questions (FAQ)
Answers to likely questions regarding functional capabilities, installation, configuration, or use

Frequently Used Terms

For your reference some of the terminology abbreviations used throughout this guide are explained below:

Acer Server Manager (ASM)

The System Management Software referred to in this guide. It consists of ASM Console and ASM Agents. The ASM Console requests information from ASM Agents running on managed servers.

Baseboard Management Controller (BMC)

BMC is a microcontroller that provides intelligent server management based on the Intelligent Platform Management Interface (IPMI) standard.

1 Introduction

Common Information Model (CIM)

CIM is a data model, a conceptual view of the managed system's environment, which unifies and extends existing system instrumentation and management standards (SNMP, DMI, CMIP) using object-oriented constructs and design.

CIM Object Manager (CIMOM) and CIMOM Repository

The CIM infrastructure consists of the CIMOM and a CIMOM repository. Management applications depend on the CIMOM to handle the interface between CIM consumers and CIM providers. CIMOM facilitates these communications by providing a common programming interface to CIM. The CIMOM repository holds the CIM, extension schemes and data information or data source details.

HP OpenView NNM

HP OpenView Network Node Manager is a well-known industry-leading enterprise management solution.

In-Band

The management scheme which requires the presence of an operating system and management agent.

IPMI

Intelligent Platform Management Interface.

Managed Server / System / Node

The server system being managed by ASM Console.

Management Console

The system on which ASM Console is deployed.

Navigator Window

Left pane of the ASM Console which allows the user to browse and select from various categories of the hardware information of the managed server.

Out-Of-Band (OOB)

Pre-Operating System or Operating System-absent management scheme. The intelligent BMC allows the retrieval of managed server information, and performs remote management functions in the absence of an operating system.

SMART

Short for Self Monitoring, Analysis and Reporting Technology. SMART is implemented as the health indicators and thresholds in the hard disk drive hardware and firmware to predict impending failures. ASM reports two kinds of predictions for hard disk drives through alerting events: Pre-failure predictions and Critical predictions. The types of health indicators and their thresholds are determined by the hard disk drive manufacturer.

SMBIOS

System Management BIOS

Windows Management Instrumentation (WMI)

WMI technology is Microsoft's implementation of the Desktop Management Task Force's (DMTF) Web-based Enterprise Management (WBEM) initiative for Microsoft Windows Operating Systems. It takes advantage of the DMTF CIM to represent managed objects in Windows-based environments.

WMI Consumer

The management application.

1 Introduction

WMI Provider

WMI Providers perform instrumentation on managed objects through WMI-enabled drivers, and supply CIM-compliant instrumentation data to the CIM Object Manager.

Working Area

Right pane of the ASM Console, which displays detailed information of specific management functions.

2 Installing ASM6

Before you start ASM6, the software components need to be properly installed. Two steps need to be followed to complete the installation of ASM6:

- **Install ASM6 Agent on systems to be managed systems**
- **Install ASM6 Console on the network administrator's system**

This section details the installation procedures.

ASM6 System Requirements

In order to run ASM6 properly, it is necessary that your system meet the following requirements:

System Requirements for ASM6 Agents

ASM6 Agents can be installed on a server that meet the following requirements:

- **Hardware Requirements**

Item	Requirement
CPU	Pentium III or higher
Memory	256 MB or above
Video	SVGA supporting 800 x 600 or better resolution
Hard Disk Drive	At least 50MB of free hard disk space
Networking	Ethernet (10/100 MB)

- **Software Requirements**

Windows 2000 Server and Advanced Server
Windows Server 2003
RedHat Linux 7.3, 8.0, 9.0
RedHat Linux 9.0, Red Hat Enterprise Linux AS 3.0 (Altos R310 & Altos G310 only)

System Requirements for ASM6 Console

ASM6 Console needs to be installed on the system intended to be the ASM6 Management Console.

- **Hardware Requirements**

Item	Requirement
CPU	Pentium III or higher
Memory	256 MB or above
Video	SVGA supporting 800 x 600 or better resolution
Hard Disk Drive	At least 120MB of free hard disk space
Networking	Ethernet (10/100 MB)

- **Software Requirements**

Windows 2000 Professional
Windows 2000 Server and Advanced Server
Windows XP professional
Windows Server 2003
Microsoft Internet Explorer 6.0 or higher (Recommended)

Installing ASM6 Agents

The ASM Agents run on managed systems by interpreting and responding to requests from an ASM Console, to retrieve data by executing lower level operations, and send the data back. ASM6 Agents are operating system dependent which means that the operating system specific versions of agents are required for that run-time environment. ASM Agents are also hardware dependent which means that hardware specific agent is required to perform instrumentation for the underlining technology used such as IPMI or SMBIOS.

ASM6 installation provides automatic detection capability. Once you specify that you are installing ASM Agent on a server, the ASM6 Agent installation process will automatically detect the operating system environment and the underlining technology, and select the proper ASM6 Agent version for installation with no manual recognition or selection needed.

Installing ASM6 Windows Agents

In Microsoft Windows, the native Windows Management Instrumentation (WMI) is available by default with the installation of a Windows Operating System. WMI provides large amount of system information that is also used by ASM6. So, ASM6 makes maximum use of the Windows WMI information in an approach known as Agent-less design.

The ASM Windows Agent extends standard WMI functions to cover the hardware dependent system health monitoring. ASM6 Windows Agents include two WMI providers, the SMBIOS provider and the IPMI provider; but the ASM6 Windows Agent installation process will automatically detect and select the right provider to be installed.

- 1 Make sure the Windows Operating System is installed successfully, and the server is connected to the network. This procedure will allow you to correctly detect and resolve networking issues before you start to configure the ASM Agent.
- 2 Logon to Windows Operating System using an **Administrator** account.
- 3 Make sure Windows SNMP component is installed.
- 4 Insert the ASM6 Management CD into the optical drive.

2 Installing ASM6

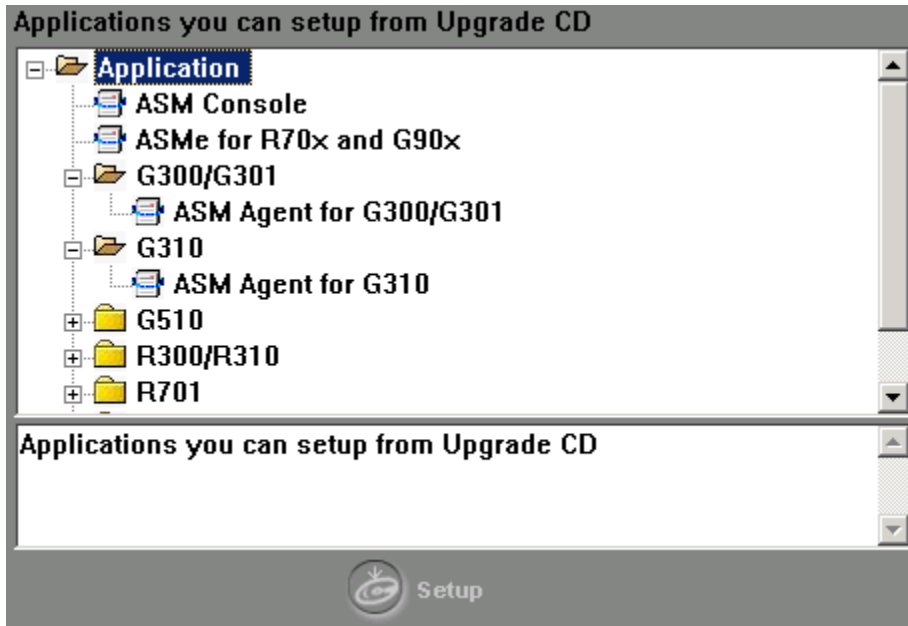
- 5 The License Agreement screen will appear after a few seconds. Click Accept and the following screen should appear:



- 6 Click the **Applications** icon:  to install applications software.

2 Installing ASM6

- 7 In the Application screen that follows, click on the + next to **Application** to expand the application options. Then choose an appropriate agent form the model list that matches your system and then click the **Setup** icon at the bottom of the window..



- 8 The ASM6 Agent InstallShield wizard will launch, click **Next** to continue.
- 9 Enter customer information, when prompted.
- 10 Specify the user name and the company name and click **Next**, you will be prompted to choose a destination location. Though you can specify your own destination directory where you want to install the agents by clicking the Browse button, it is recommended to install in the default directory:

C:\Program Files\ASM Agents

Click **Next** to continue.

- 11 Click **Next** to start the installation. You will see a progress bar during the installation.
- 12 A pop-up screen will appear when the installation is completed. Click **Finish** to exit the installer.

Setting SNMP Configuration

To make ASM6 work, you need to set the SNMP configuration first in order to allow the agents to send traps to the console.

- 1 Click Start | Settings | Control Panel | Administrative Tools | Services. The Services list window will appear. Double click SNMP Service to bring up the SNMP Service Properties window.
- 2 Click the Security tab.
Check **Send authentication trap**. Click the **Add** button to bring up the SNMP Service Configuration dialog box. Choose READ ONLY/READ WRITE/READ CREATE from the Community rights drop-down list; set Community name as public. Click Add.
Check **Accept SNMP packets from any host**.
- 3 Click the Traps tab.
Set Community name as public. Click the **Add** button to bring up the SNMP Service Configuration dialog box. Enter the IP address of the trap destination (IP address of the console). Click Add.
- 4 Click OK.

2 Installing ASM6

Note:

There is no entry in Programs menu for ASM Agents. If you want to remove ASM Agents, please use Add/Remove Programs in Control Panel.

Installing ASM6 Linux Agents

The ASM Agents use some dedicated ports to communicate with ASM Console. You have to adjust the firewall settings of the Linux server to make the following ports accessible.

The ASM6 System Monitor agent and Health Monitor agent in Linux environments are based on the Linux SNMP service, therefore the Linux SNMP service needs to be installed first, and the firewall settings need to be adjusted to allow SNMP service accessible from other hosts. To achieve this, the UDP port 161 for SNMP service should be opened.

Packages

- 1 There are two sub-directories in current directory:
AltosG310_R310 folder is for Altos G310, R310
AltosServer folder is for Altos G300, G301, G510, G700, G701, G900, G901, R300, R701
- 2 For Altos G310, R310, only Red Hat 9.0 and enterprise AS 3 are supported
For other models listed before, Red Hat 7.3 and 8.0 are supported
- 3 Three package group are required:
 - a. UCD-SNMP and UCD-SNMP utility (ForR310 and G310,NET-SNMP is required)
 - b. Pegasus

The ASM Agents use some dedicated ports to communicate with ASM Console. You have to adjust the firewall settings of the Linux server to make the following ports accessible.

- **UDP/161 (SNMP)**
- **TCP/5988 (Pegasus CIM Server)**
- **TCP/5989 (Pegasus CIM Server)**
- **TCP/4400 (Remote Linux Console Agent)**
- **UDP/5500 (Remote Linux Console Agent)**

You should know the platform type (model name), and change to the right directory(basing on managed server's model name). The remainder of this guide will use \$ROOTDIR\$ to stand for the root dir of the right directory. For example, if managed server's model name is "Altos R310" or "Altos G310", \$ROOTDIR\$ equals to "/mnt/cdrom/asm/LinuxAgent/AltosG310_R310", or , it equals to "/mnt/cdrom/asm/LinuxAgent/AltosServer"

Before installing ASM6 Linux Agents, you should install UCD-SNMP v4.2.3 (or NET-SNMP) and Pegasus package first.

To install UCD-SNMP v4.2.3 (for Red Hat 7.3 and Red Hat 8.0 only):

- 1 If you have installed a different version of UCD-SNMP, uninstall it.
To check if UCD-SNMP v4.2.3 is already installed, use the command:
rpm -qa |grep ucd-snmp-4.2.3-1
To uninstall UCD-SNMP of a different version, use the command:
rpm -e ucd-snmp-* (* is the version number)

When you remove these packages, remove them in such an order that it eliminates dependency error messages. For example, if a dependency error message appears, remove the package mentioned in the error message. Continue removing the dependent packages this way until the error messages stop.

2 Installing ASM6

Note: the default installation may be NET-SNMP for Red Hat 8.0 or later versions. You should remove it the same way you remove UCD-SNMP.

- 2 Insert the ASM6 Management CD into the Linux server CD-ROM drive. The CD should automatically be mounted by the system. If not, you can mount the CD using the command:

mount /mnt/cdrom

Change directory to **\$ROOTDIRS/dependency/**, run the following command to install the UCD-SNMP daemon:

rpm -i ucd-snmp-4.2.3-1.i386.rpm

Note:

for Red Hat V9.0 or later versions, ucd-snmp is not required, but you should make sure net-snmp and net-snmp utility packages are installed before installing ASM Agents. And, you'd better install these packages with the original Red Hat CD.

To install Pegasus package

- 1 Change the working directory to **\$ROOTDIRS/Pegasus**
- 2 Run the command **./pgpkg install** (add EXECUTE mode to this file if necessary)
- 3 Pegasus will be installed to **/usr/local/share/pegasus**.
- 4 Configure authentication method
- 5 After the installation is finished, you will be prompted to configure if the user authentication will be required. If it is not, anonymous login will be allowed, thus anyone can manage this server. If you choose to enable it, you will be prompted to add users that will be configured as managers.

Noticed that only valid users of the local system can be added.

Note: These settings can be modified after installation with **cimauthconf**, the configuration tool, which is in the folder **/usr/local/share/pegasus**. You can get more information on how to use this utility with **-h** option.

To install the ASM Agents:

- 1 Insert the ASM6 Management CD into your computer's optical drive.
- 2 Mount the CD-ROM with the command **mount /dev/cdrom /mnt/cdrom**.
- 3 Change the working directory to **\$ROOTDIRS**
- 4 To install the ASM Linux Agents, type in the command **./asmsetup install** (add EXECUTE mode to this file if necessary).

Follow the prompted installation guide.

- 5 Umount the CD-ROM Drive with the command **umount /mnt/cdrom**.

To start or stop the ASM Agents

- 1 To start ASM Agents, use the command: **asmagent start**
- 2 To stop ASM Agents, use the command: **asmagent stop**

Note:

The utility, **asmagent**, has been installed into the hard disk and can be launched in any directory.

Installing ASM6 Console

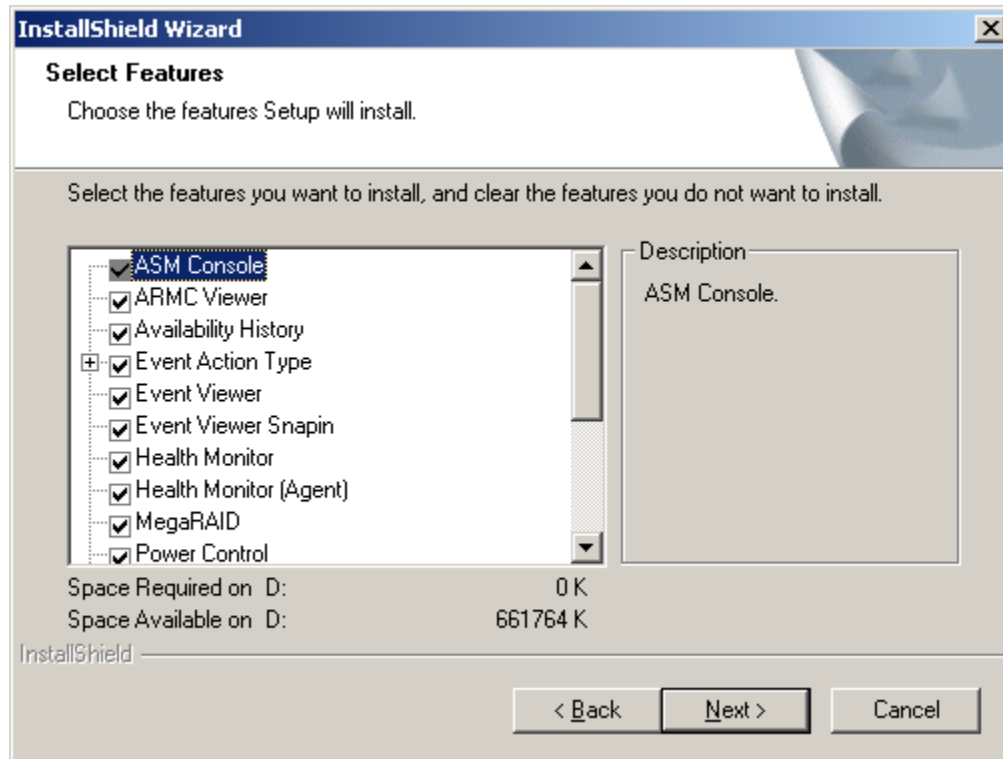
The ASM6 Console needs to be installed on the system intended to be the ASM6 Management Console. The ASM6 Console provides administrative functions, allowing system administrators to remotely access and manage servers with ASM Agents installed.

To Install ASM Console:

- 1 Make sure the Windows Operating System is installed successfully, and the server is connected to the network. Logon to Windows Operating System using an Administrator account.
- 2 Insert the ASM6 Management CD into the optical drive.
- 3 Follow the initial installation steps by choosing the ASM Console in the applications selection screen. The welcome screen should appear in a few seconds.
- 4 Click **Next**, and enter customer information as prompted.
- 5 Specify the user name and the company name and click **Next**. You will be prompted to select an installation type. There are two installation types:
Typical -- The ASM6 Console will be installed with the most common options. This is recommended for most users.
Custom -- You can choose customized installation options as you need. This is recommended for advanced users only.
- 6 Click **Next**, you will be prompted to choose a destination location. You may specify the destination directory where you want to install ASM6 by clicking the Browse button, or you may use the default directory which is:
C:\Program Files\ASM
- 7 Click **Next** to continue.

2 Installing ASM6

- 8 The following screen allows you to choose the custom installation options (This step will be skipped if you selected **Typical** installation earlier)



- 9 Click **Next** to continue.
- 10 Click **Next** to start the installation. You will see a progress bar during the installation.
- 11 A pop-up screen will appear when the installation is completed. Click **Finish** to exit the installer.

Note:

If you are installing ASM Console in a clean Windows 2000 without SP4 or later installed, after you click the **Finish** button, the installation program may require you to reboot the system. Please just click **Yes** to reboot the system.

Uninstalling ASM6

The following procedures should be followed if you need to remove ASM6 from your computer. In addition, you may also need to uninstall ASM6 before you reinstall or upgrade the ASM software.

Uninstalling ASM6 Windows Agent

To uninstall ASM Agent, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**. Select ASM Agent and then click the Add/Remove button, follow the on-screen instructions to remove the ASM Agent.

Uninstalling ASM6 Linux Agent

- 1 Uninstall ASM agent with the command:

2 Installing ASM6

asmsetup uninstall

Note:

The utility, asmsetup, has been installed into the hard disk and can be launched in any directory.

- 2 Uninstall pegasus server with the command:

pgpkg uninstall

Note:

The utility, pggkg, has been installed into the hard disk and can be launched in any directory.

IMPORTANT: Make sure to do uninstallation in the correct order: uninstall ASM Agents first and then uninstall Pegasus.

Uninstalling ASM6 Console

To uninstall ASM6 Console, please click the following items in turn:

Start | Programs | Acer Server Manager | Uninstall.

You can select **Remove** and click **Next** to remove the ASM Console.

3 Quick Guide

In this section, you will be given a quick guided tour of ASM6 to get yourself familiarized with the starting procedure and user interface.

Starting ASM6

After you have installed ASM Agent on a managed system, ASM6 Services will be added to the Windows Operating System. The ASM6 Services will start additional processes. No action is required for the user to start/stop these processes. The processes will be started automatically when your Windows Operating System is started.

To start the ASM Console on the administrator's ASM6 system where ASM Console has been installed, please click the following items in turn:

Start | Programs | Acer Server Manager | Acer Server Manager.

ASM6 Console Interface



The ASM Console window is the main interface to interact with the program. It is from this window that you will be doing all your work. The ASM Console window consists of three areas:

Managed System area - Displays a list of systems managed by the ASM Console.



Management Function area - Displays the management function list available for a selected system.

Working area - The window where the manageable information is displayed and the management operations are carried out.

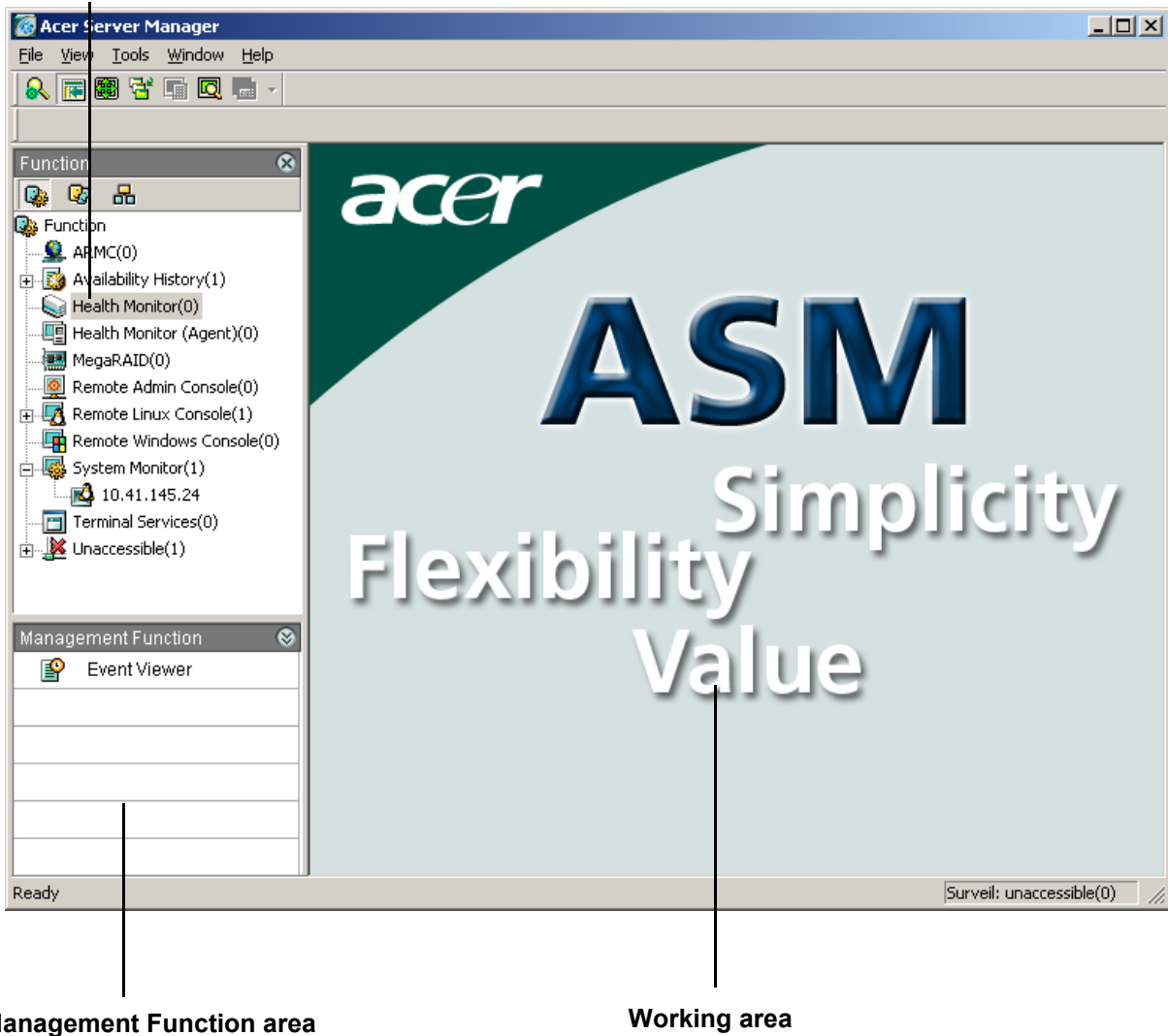
The terms "Managed System Area" and "Managed System List" will be used interchangeably, as will "Management Function Area" and "Management Function List."

The Managed System Area and the Management Function Area are called Navigator Windows. You can click the Navigator button  to show or hide the window, or you can also click the  button to close the window.

3 Quick Guide

Clicking the  and  button can expand and collapse the windows respectively..

Managed System area



When a specific managed system is selected or expanded in the Managed System List, the descriptive information retrieved from that system (according to administrator's selection) will be shown in the working area, the larger window on the right.

Managed Systems

The managed systems are listed in the Managed System Area in the upper left corner of the ASM Console user interface. You can manage the monitored systems listed in this pane.

There are three types of views in which you can group and view monitored systems:

Subnet View -- The managed systems are grouped and viewed by subnets. The number of systems belonging to that subnet is indicated by the number in the brackets to the right of the subnet name.

Group View -- The managed systems are grouped and displayed by groups. They can be grouped by department, location, etc. The groups can be recursive. A system can be moved to a different group manually by dragging and dropping.

Function View -- The managed systems are grouped and viewed by different functions.

Management Functions

ASM Console provides a variety of powerful management functions including:

System Monitor -- This function provides system configuration information with an easy-to-use interface that displays the managed system's hardware and software configuration.

Availability History -- Shows the availability status history of a managed system.

Health Monitor -- This function monitors a managed system's environmental health status.

Event Viewer -- When an alerting event occurs, whether a hardware error or a particular threshold setting has been exceeded, the ASM agent detects the condition and sends an event, sometimes called a trap, to inform the system administrator. The Event Manager logs the event in a real time log, and allows the system administrator to view and to handle the event accordingly.

Web Viewer -- This function links to pre-set, system-specific contents through Web access. For example, to an Acer Remote Management Card contents page.

Admin Console -- This powerful function links to pre-OS, text-based console redirection which redirects BIOS, OS administration information, and remote diagnostics operation from the managed system to the ASM console no matter which operational stage a managed system is in.

Remote Console -- This function redirects Windows and Linux system's graphic console from the managed system to the ASM Console.

Terminal Services -- This function allows you to remotely access the managed system through Windows Terminal Services.

MegaRAID -- This function allows you view MegaRAID information.

Power Control -- This function allows you to set the power state of a managed system.

ARMC Viewer -- This function allows you to perform remote management and monitoring of systems with Acer Remote Management Cards (ARMC).

Event Rule Setup -- This function allows you to target systems and events you are interested in, the specific conditions you want to distinguish (critical temperature, high bus utilization, etc.), the alert methods you prefer, and the response you would like taken on receipt of event notification/occurrence.

Remote Configuration -- This function allows you to set SNMP trap and threshold options.

Working Area

The Working Area is the large area on the right of the Navigator Window where information retrieved from ASM

3 Quick Guide

Agents is displayed. Administrators can also use this area to remotely monitor and manage targeted systems.

4 Using ASM6

In this section, you will be guided through various features and procedures of using ASM to perform server management functions.

Discovering

The first step to effectively managing the systems in your network is to “discover” or locate them on the network. ASM Console provides an automatic discovery tool for easily connecting to all the managed systems on your network.

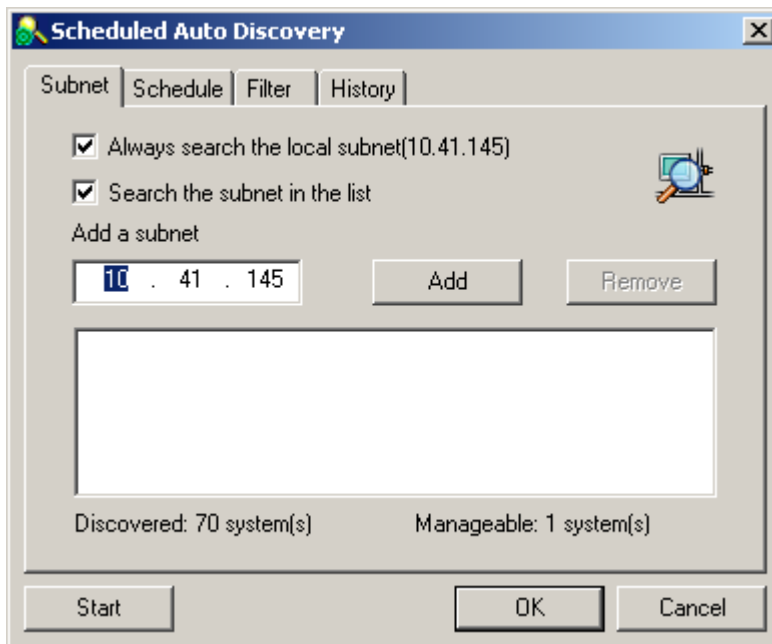
To set up the ASM auto discovery, select the following items in turn:

Tools | Auto discovery...

Then the Schedule Auto Discovery window will pop up, with four tabbed pages for you to set the auto discovery preferences.

Setting up Subnet

The Subnet page can be used to add and to remove subnet(s) for the auto discover engine to search..

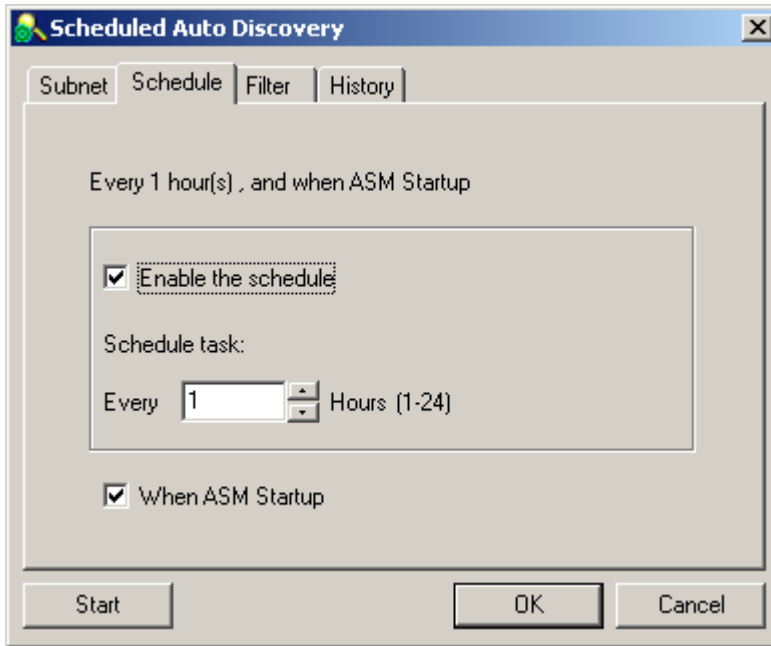


- **Always search the local subnet** - Search all systems in local subnet(s).
- **Search the subnet in the list** - Specify subnet(s) in which to search for systems.

In the Add a subnet field, enter the subnet and click the Add button to add it to the list. You can add several subnets. If a new subnet needs to be added into discovery, simply type in the subnet address, and click the Add button to add it.

Setting Up Discovery Schedule

The Schedule page can be used to set up the time interval for the auto-discovery. .

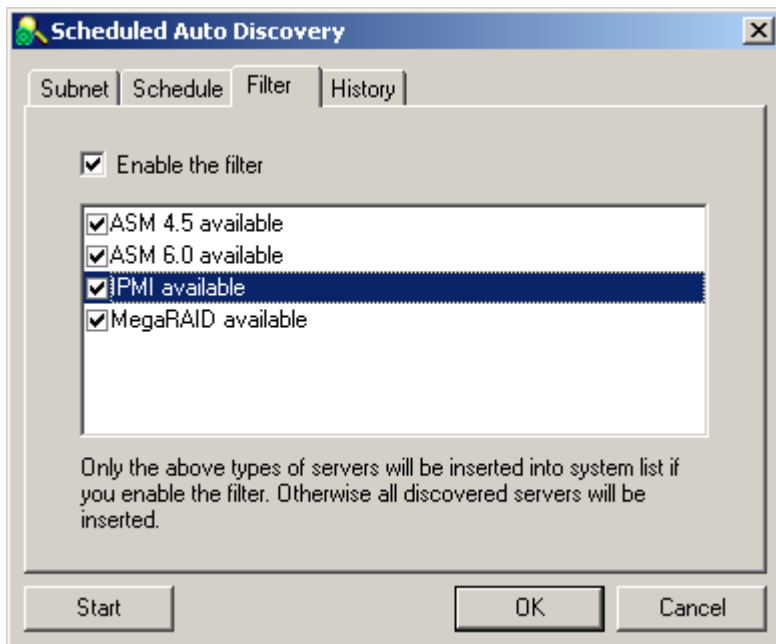


On the Schedule page, check Enable the schedule and enter the desired time interval to run auto discovery.

If As ASM Startup is checked, auto discovery will be enabled as ASM starts. Otherwise you should click the Start button to start auto discovery. Discovery will be performed automatically at the scheduled interval.

Setting Up Filter

The Filter page can be used to select specific groups of systems to be discovered.



On the Filter tabbed page, check Enable the filter and then check the filtering options as desired:

ASM 4.5 available - Only search for systems with ASM 4.5 Agent pre-installed.

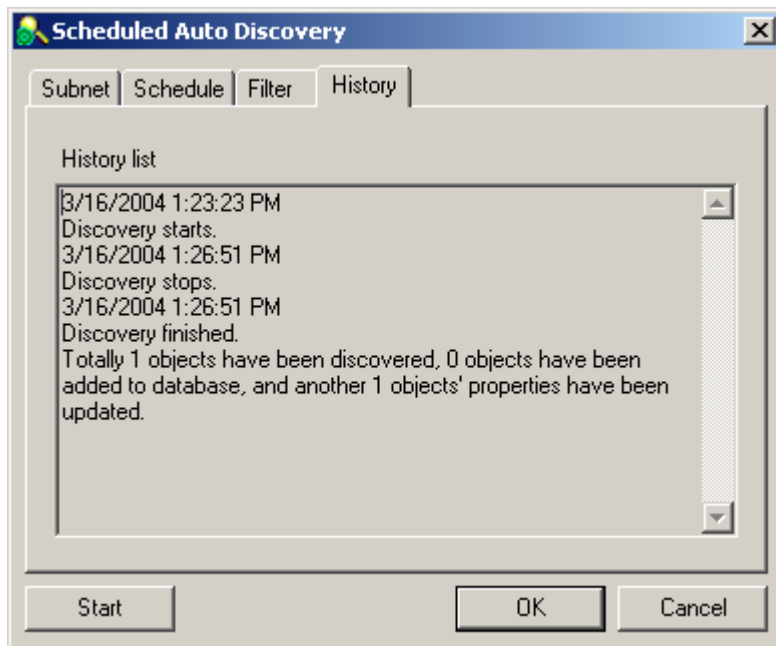
ASM 6.0 available - Only search for systems with ASM 6.0 Agent pre-installed.

IPMI available - Only search for systems with IPMI enabled.

MegaRAID available - Only search for systems with MegaRAID enabled.

History

The History page displays the auto-discovery history..



After you have set up all of your preferences, click the Start button to run auto discovery. All systems in the specified subnets will be tried and discovered automatically and listed in the Managed System List.

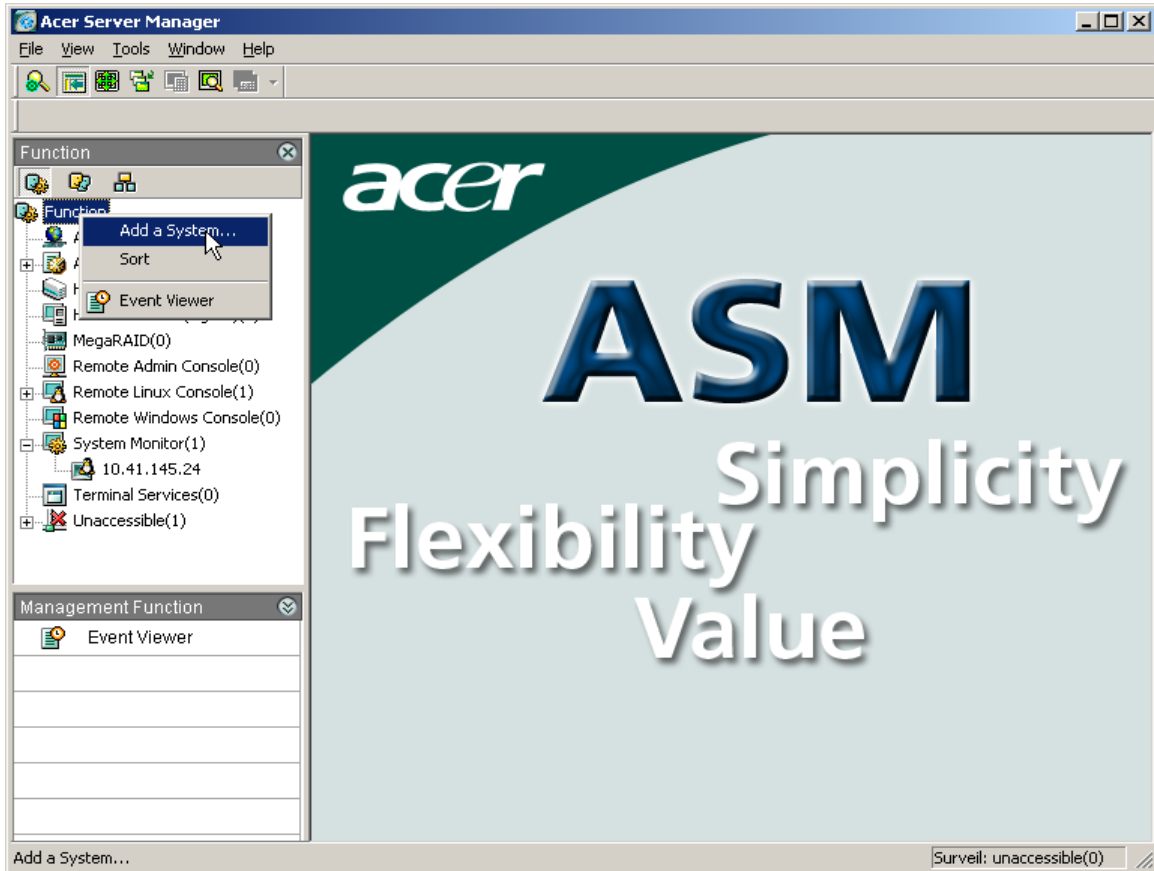
Managing System List

After running auto discovery, all found systems are listed in the Managed System area of the ASM Console user interface. They are grouped automatically according to their subnets in Subnet view and functions in the Function view respectively. You can add, delete or rename systems manually, and group the systems according to your needs.

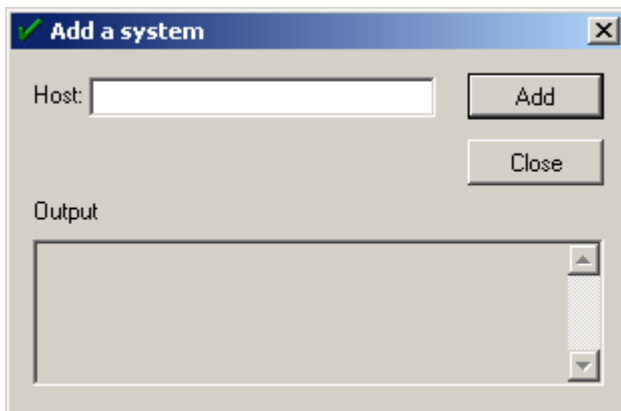
Adding a System

With ASM Console, you can manually add a computer to the Managed System List by its hostname or IP address, or from a computer list generated by the auto discovery process.

- 1 In the Managed System Area, in any of Subnet, Group, Function views, right-click the title (Subnet, Group, Function) and select **Add a system...** from the drop down menu..



- 2 An **Add a system** window will appear. Type in the IP address or the computer name you want to add and then click the Add button. The new system will be added to the managed systems..



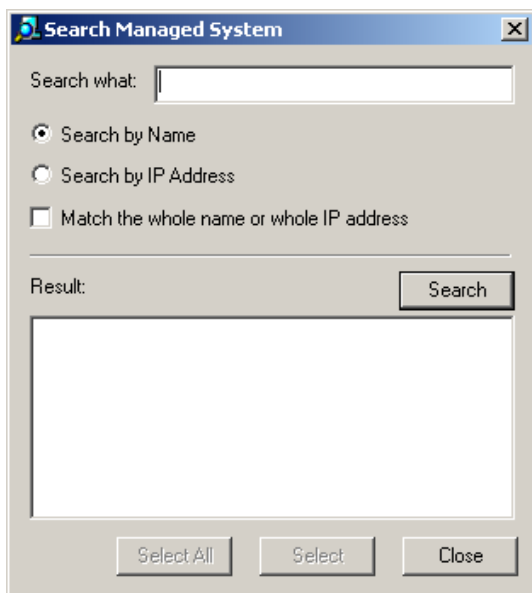
Searching for a System

Sometimes there could be too many managed systems, making it difficult to locate the system you need quickly. ASM6 also has a search tool to quickly locate the desired system.

To search for a managed system, do one of the following:

- Click the Search button  on the toolbar.
- Choose Search Managed System... from the View menu.

A Search Managed System dialog box will appear..



Set your searching options.

- **Search by Name.** The search will be performed according to the name you enter.
- **Search by IP Address.** The search will be performed according to the IP address you enter.

Match the whole name or whole IP address. This feature is useful to search for systems with specific pattern in their name. Without this feature checked, the search finds any systems with matching string, whether it is a fragment of a longer string. With this feature checked, the search finds the system that matches the pattern string, or IP address that contains the IP string you entered.

Deleting a System

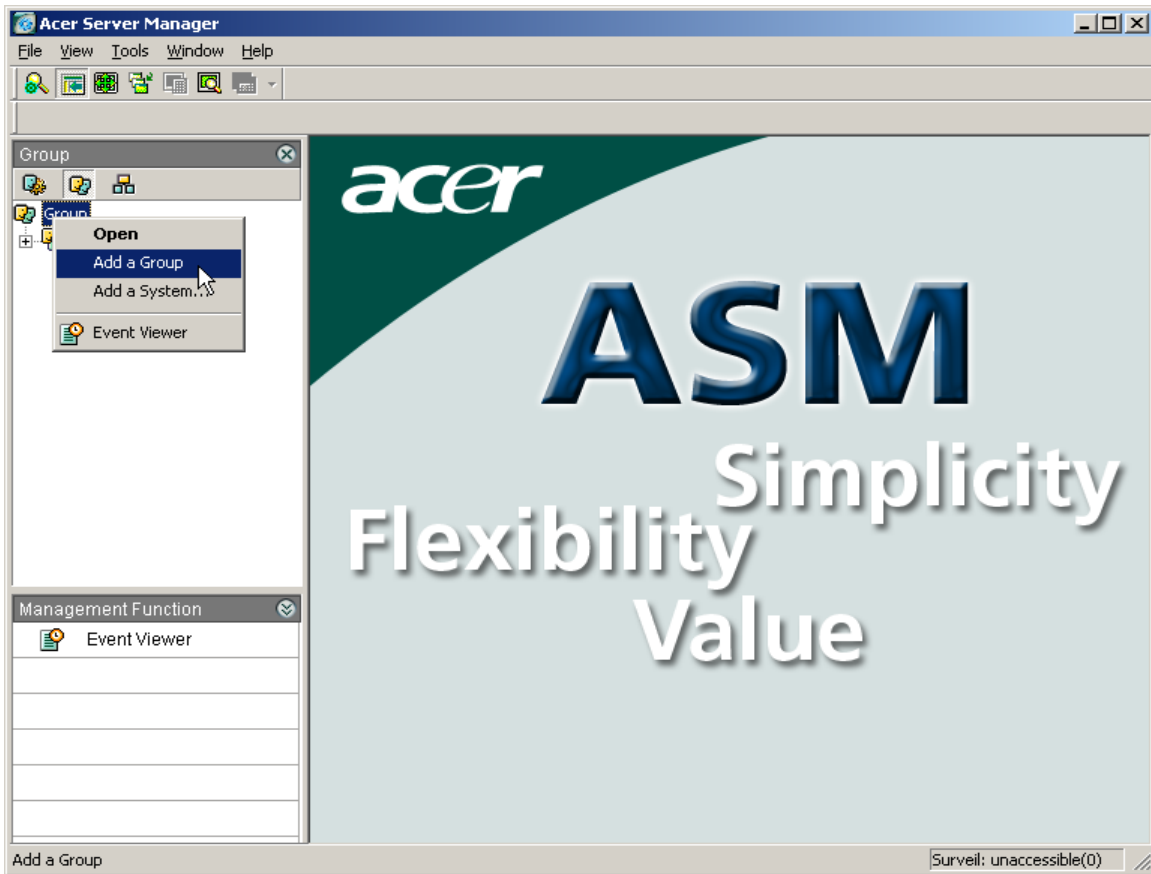
From the Managed System List, right-click the system you want to delete and select Delete system. The system will be deleted after confirmation. You can also delete a system by selecting the system and pressing the <Delete> key on the keyboard..



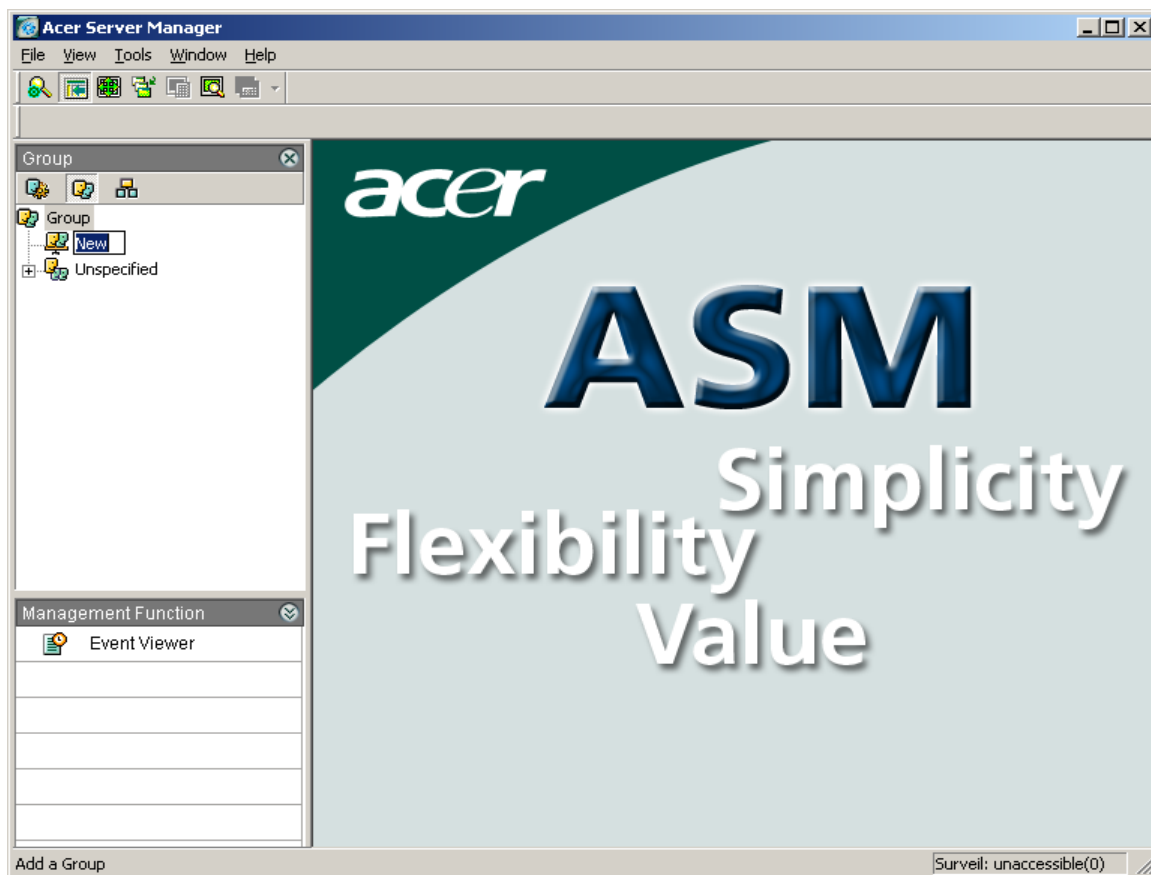
From the Managed System Area Group View, you can add a group into the managed system list manually.

Adding a Group

- 1 In the Managed System Area, right-click the Group title and select **Add a Group...**



- 2 Type in the new group name, and the new group will be added..



Deleting a Group

From the Managed System List, right -click the group you want to delete and select **Delete**. The group will be deleted after confirmation. You can also delete a group by selecting the group and pressing the <Delete> key on the keyboard.

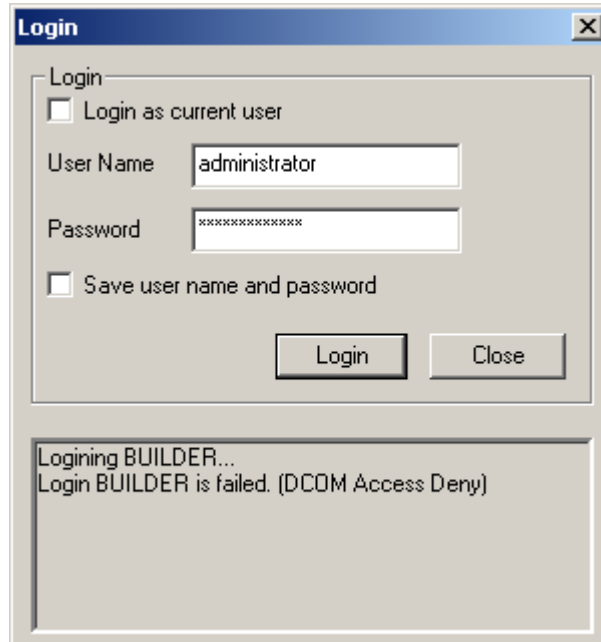
Right Clicking on a Target System

ASM6 provides a convenient way -- right clicking on a system -- to launch management functions. They include Remote Configuration, Power Control, Web Viewer, Surveil, Refresh Selected System, and Properties.

Remote Configuration

Remote Configuration allows you to set the SNMP trap destination and threshold on the selected system. If the threshold is exceeded, the trap will be sent to the destination you specified.

To use the Remote Configuration function, you need to login to the target system first. The account you login with should have administrator privileges (on the system you want to access or in your domain).

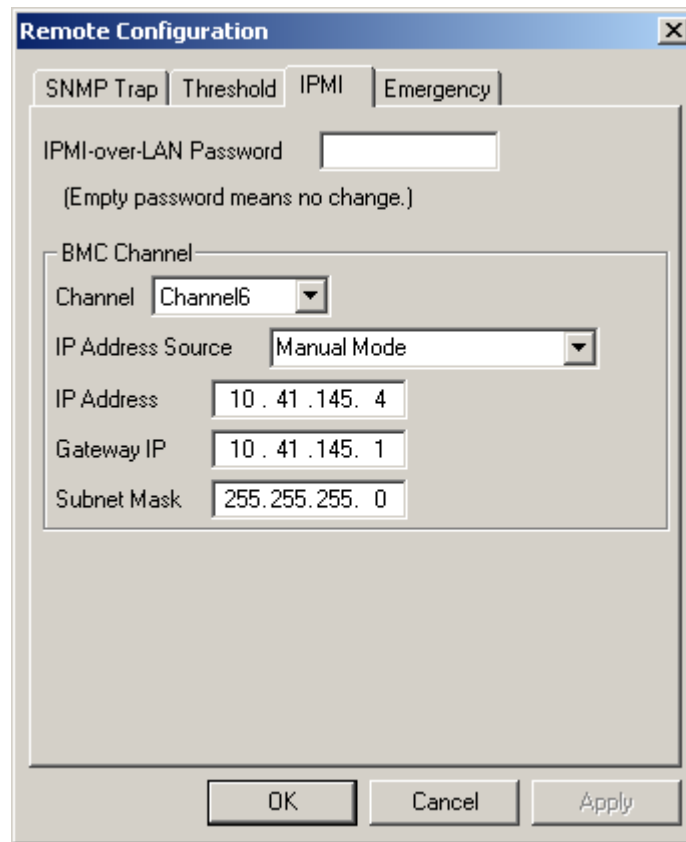


The number of tabbed pages in the Remote Configuration window depends on your specific system. If your system supports SMBIOS, there will be three tabbed pages (SNMP Trap, Threshold, and Emergency). If your system supports SNMP, there will be four tabbed pages (SNMP Trap, Threshold, IPMI and Emergency). If your system supports ASF, there will be three tabbed pages (SNMP Trap, Threshold and ASF). If your system supports neither, there will be two tabbed pages (SNMP Trap and Threshold).

On the SNMP Trap page, you can add an SNMP trap destination by clicking Add and entering the destination.

On the Threshold page, you can change the threshold by clicking Threshold Value and entering a new value.

On the IPMI tabbed page (For system with IPMI available), you can set or change the IPMI-Over-LAN password and change the BMC Channel settings.



IPMI-over-LAN Password: Set the IPMI authentication password here.

Channel:

Channels provide the mechanism for directing the routing of IPMI messages between different media connections to the BMC. A channel number identifies a particular connection. For example, 0 is the channel number for the primary IPMB. Up to nine channels can be supported (the System Interface and primary IPMB, plus seven additional channels with media type assigned by the implementer.) Channels can thus be used to support multiple IPMB, LAN, Serial, etc., connections to BMC.

IP Address Source: Specify the IP address of IPMI.

Unspecified - The IP address is not specified.

Manual Mode - Configure the IP address manually.

DHCP Mode - The IP address is obtained by BMC running DHCP.

Sharing OS IP Mode - The IP address loaded by BIOS or system software.

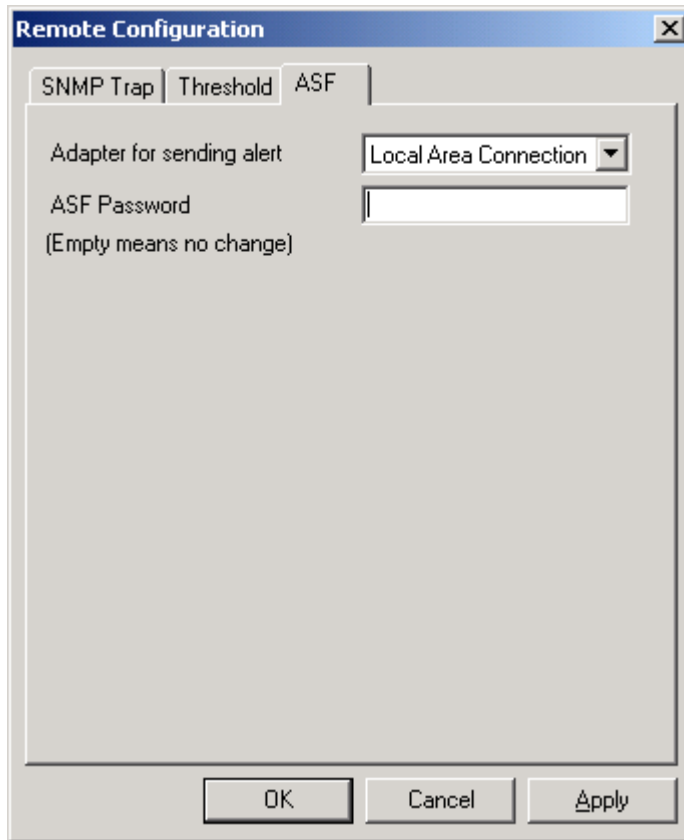
IP Address: Specify the IP address for IPMI. Available when the IP address Source is Manual Mode.

Gateway IP: Specify the Gateway IP address for IPMI. Available when the IP address Source is Manual Mode.

Subnet Mask: Specify the subnet mask for IPMI. Available when the IP address Source is Manual Mode.

4 Using ASM6

On the ASF tabbed page (For system with ASF available), you can set or change the ASF password and change the adapter settings for sending alert .

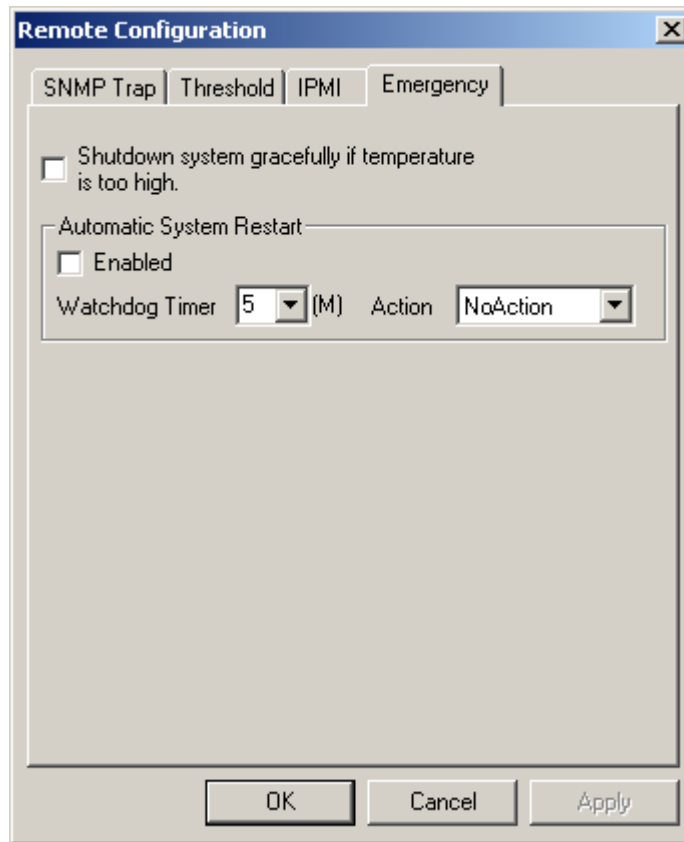


Adapter for sending alert:

Adapters provide the mechanism for directing the routing of ASF messages between different media connections to the BMC.

ASF Password: Set the ASF authentication password here.

On the Emergency page, you can choose to shutdown a managed system if the temperature is too high. For IPMI enabled systems, you can also set the automatic restart function here.



Shutdown system gracefully if temperature is too high.

Automatic System Restart

Watchdog Timer - Specify the time interval for the Watchdog Timer, if the specified period is reached but the Watchdog Timer is not reset by the ASM Agent, the action you select from the Action drop down box will be executed.

Action - Execute the action when the specified period is reached but the Watchdog Timer is not reset by the ASM Agent.

Power Control

ASM6 provides power control functions for you to control the power states of managed systems, including:

- **OS Shutdown** - Shutdown the managed system with WMI / Pegasus available.
- **OS Restart** - Restart the managed system with WMI / Pegasus available.
- **IPMI Power On (For system with IPMI available)** - Power on the managed system with IPMI available.
- **IPMI Power Off (For system with IPMI available)** - Power off the managed system with IPMI available.
- **IPMI Reset (For system with IPMI available)** - Reset the managed system with IPMI available.
- **ASF Power On (For system with ASF 2.0 available)** - Power on the managed system with ASF 2.0 available.
- **ASF Power Off (For system with ASF 2.0 available)** - Power off the managed system with ASF 2.0 available.
- **ASF Reset (For system with ASF 2.0 available)** - Reset the managed system with ASF 2.0 available.
- **Task panel** - Show the tasks on the managed system.

Web Viewer

Web Viewer allows you to add an URL that can be viewed by ASM6.

Surveil

When ASM Console is running, it polls the status of every managed system, if a managed system becomes inaccessible, a red cross will be displayed on the bottom-right of the managed system's icon. No other action will be taken. But if a managed system is under surveillance, ASM Console will generate a "Managed System Unaccessible" event when it becomes unaccessible. Administrators can use "Event Rule Setup" to configure what actions to do after receiving such an event.

By default the managed system is not under surveillance. To put a system under surveillance, administrators can right-click the managed system and choose "Surveil." If a managed system is under surveillance, there will be a green check on the top-left of the managed system's icon. To cancel surveillance on a managed system, administrators can right-click the managed system and choose "Don't Surveil."

Refresh Selected System

Choose this option to refresh the properties of the selected system.

Properties

Please refer to Viewing System Properties on page 32.

Authentication

To manage target systems, ASM6 uses several standards to retrieve information and login to a managed system.

- **SNMP** (Simple Network Management Protocol) - SNMP is a network management standard widely used in TCP/IP networks and, more recently, in Internet Packet Exchange (IPX) networks. SNMP provides a method of managing network hosts such as workstations or servers, routers, bridges, and hubs from a centrally-located computer running network management software. SNMP performs management services by using a distributed architecture of management systems and agents.
- **IPMI** (Intelligent Platform Management Interface) - IPMI is a de facto industry standard, and uses a dedicated BMC as the intelligent management processor for high-end server management. The IPMI / BMC keeps the sensors in check, serves the queries from the ASM Console, logs the events and sends alerts to the ASM Console, through Out-Of-Band communications. Since there is no agent support required, this is sometimes called agentless implementation, and functions even when the server OS is down or when the server is powered down. Advanced BMC can even support complicated management functions such as remote console, remote virtual floppy / CD drives, and web-based management interface.
- **Pegasus** - Pegasus is an open-source implementation of the DMTF CIM and WBEM standards. It is designed to be portable and highly modular. It effectively translates the object concepts of the CIM objects into a programming model but still retains the speed and efficiency of a compiled language. Pegasus is designed to be inherently portable and builds and runs on most versions of UNIXÆ, Linux, and Microsoft Windows.

Global Authentication Options

The Options window allows you to set the global SNMP and authentication options.

To launch the Options window, click **Tools** menu and then choose **Options...**

- **SNMP Option** allows you to set the SNMP options. If you want to use the default options, please click the Default button.

- Windows Authentication allows you to specify a default login user for all managed Windows Systems.
- IPMI Authentication allows you to specify a default login user for IPMI device in all systems.
- Linux Authentication allows you to specify a default login user for Pegasus service in all systems.

Authentication Option for a Selected System

To set authentication option for a selected system:

Right click on the system and choose **Properties** from the drop down menu, the system properties will be displayed in the working area. There are four tabbed pages related to authentication options.

- SNMP Option - shows the SNMP options for the selected system. If Uses default SNMP Options is checked, the default SNMP options are applied to the selected system. You can also uncheck this box and define the SNMP options yourself.
- Windows Authentication - allows you to specify a default login user for the selected Windows System. If Use Global default login user is checked, the login you defined in Tools Options will be used for the selected system. You can also uncheck this box and define a private default login user yourself.
- IPMI Authentication - allows you to specify a default login user for IPMI device in the selected system. If Use Global default login user is checked, the login you defined in Tools Options will be used for the selected system. You can also uncheck this box and define a private default login user yourself.
- Linux Authentication - allows you to specify a default login user for Pegasus service in the selected system. If Use Global default login user is checked, the login you defined in Tools Options will be used for the selected system. You can also uncheck this box and define a private default login user yourself.

Viewing System Properties

The Properties window shows the information of the selected system and the authentication options.

To view the properties of a managed system:

Right click on the system and choose **Properties** from the context menu, the system properties will be displayed in the working area. There are six tabbed pages in the Properties window as follows:

General - shows the basic information of the selected managed system.

Object Properties - shows the detailed information of the selected managed system

The Properties window also shows the authentication options for the selected system, which may be different depending on the authentication method available on that system. For detailed information, please refer to Authentication on page 30.

If required, the system properties can be exported and saved in a .csv file.

To export system properties:

From the **File** menu, click **Export...** to display an Export Managed System window. Enter the file name and select the directory in the **Export** window.

Select the properties you wish to export and then click **Finish**, to save the system properties.

To import system properties:

From the **File** menu, click **Import...** on the file menu to show an **Open** window. In the **Open** window, select the file you want to import from and then click **Open**. The computers will be added to the managed systems list.

If the computer already exists in the Managed System List, ASM6 will show a **Confirm System Insert** window. You can choose to skip the update or continue and create a new computer.

To refresh the properties of a managed system system:

From the Managed System List, select a system and right click on it, and then choose **Refresh Selected System** from the drop down menu to refresh the properties of the selected system.

To refresh the properties of all systems:

Click the **Tools** menu and then select **Refresh All Systems**.

Now you have mastered the handling managed system list and system properties, and you can start to use other ASM6 management functions through the ASM Console to manage and monitor systems, diagnose problems, or use the remote console functions to manage the systems remotely.

Monitoring System Health

The ASM6 System Health function monitors the environmental health status of managed systems with various environmental sensors. Major items that system health monitors and reports include:

- **CPU Temperature**
- **Voltages**
- **Fan and Cooling Device**
- **Power Supply status**
- **System Chassis intrusion**

System administrators can proactively query system health status through the ASM Console. If any faults occur, the System Health monitor will log the event and alert the system administrator .

Underlying Technology

This sub-section explains some technical background information about how ASM6 has been designed and implemented to provide the functionalities. It is for more technical readers who demand deeper understanding of ASM6. If you find it difficult to understand this sub-section, you may prefer to skip it.

Query and Alert

There are two types of basic server management activities:

- **Query** - System administrators use ASM Console to request information from the managed server, and to perform management actions.
- **Alert** - The ASM Agent installed on the managed server monitors and sends alerts automatically to the ASM Console when abnormal conditions occur.

In-Band and Out-Of-Band

There two ways for the ASM Console to query and manage the targeted server:

- Through ASM6 Agents running on managed servers. Since agents run under the OS and make use of the native network and communication mechanisms, this is usually called In-Band communications.
- Through direct communications with the intelligent management processor in the managed server. Since it does not require OS support by the server, and may even use its own network channel, it is usually called Out-of-Band (OOB) communications.

The actual mechanisms used in your server management are largely determined by management technology (hardware and firmware) deployed on your server, as explained below.

SMBIOS, ASF, and IPMI / BMC

To achieve different alert levels, different hardware and firmware technology needs to be used in addition to the hardware sensor technology. Examine your system specifications to find out which technology is supported by your system.

- **SMBIOS (System Management BIOS)** - SMBIOS is an industry standard to keep management information in a well-structured, easy to access area within BIOS. It also contains sensor data and event logs in pre-defined structures. Due to the lack of additional hardware support, the server management of SMBIOS - only platforms totally depends on the agents and In-Band communications, for both query and alert, leaving no support when the OS is down, or when the server is powered down.
- **ASF (Alert Standard Formats)** - ASF is a different industry standard for alerting. The ASF logic usually is built into the NIC hardware and firmware. In ASF enabled systems, the sensor reading query still depends on In-Band communications through agents and / or SMBIOS. But the alert of ASF-defined events, as well as the ASF-defined management functions such as power on / off / reset, can be supported by ASF logic through Out-Of-Band communications. Even when the server has been powered down, those ASF functions are still supported, as ASF logic in the NIC is also supported by secondary power (sometimes called backup power).
- **IPMI (Intelligent Platform Management Interface)** - IPMI is a de facto industry standard, and uses a dedicated BMC as the intelligent management processor for high-end server management. The IPMI / BMC keeps the sensors in check, serves the queries from the ASM Console, logs the events and sends alerts to the ASM Console, through Out-Of-Band communications. Since there is no agent support required, this is sometimes called agentless implementation, and functions even when the server OS is down or when the server is powered down. Advanced BMC can even support complicated management functions such as remote console, remote virtual floppy / CD drives, and web-based management interface.

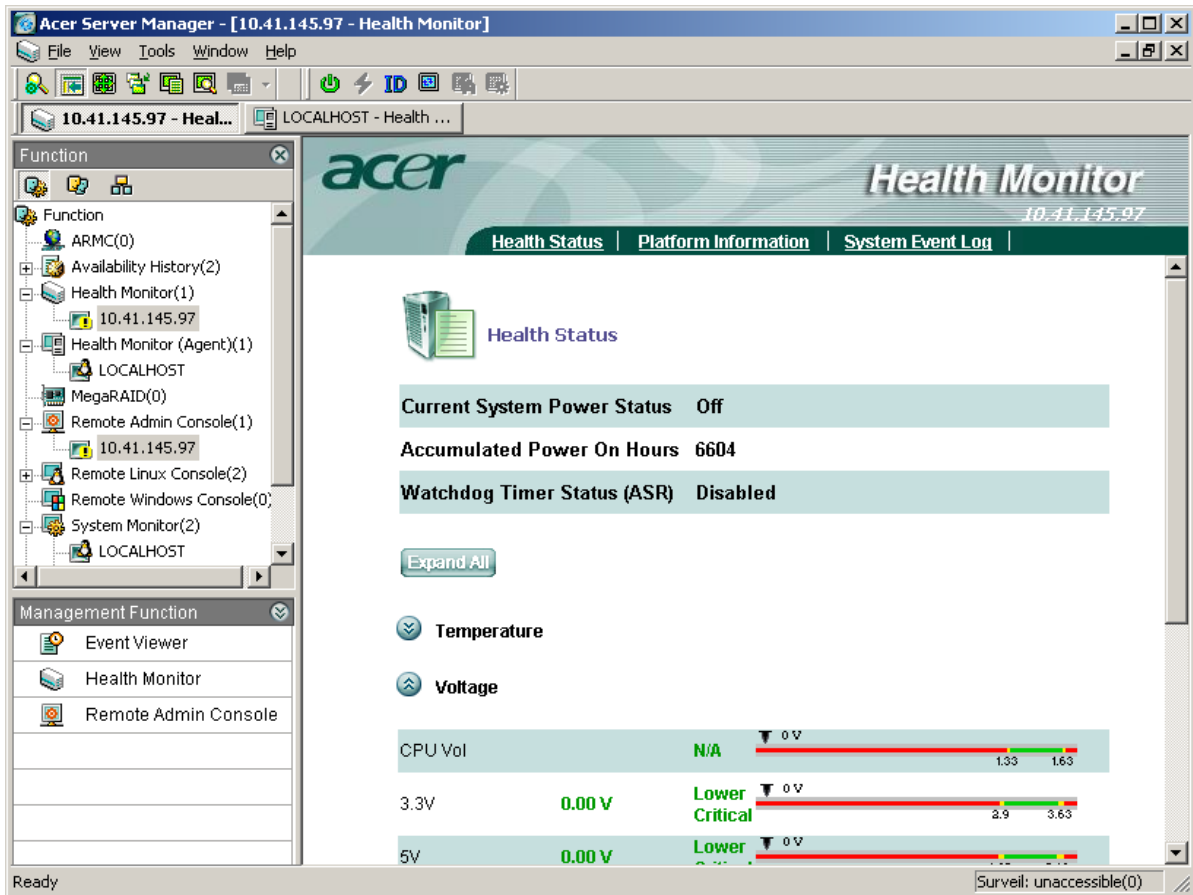
System Health Monitor Interface

If the system is equipped with IPMI/BMC, the Health Monitor will be shown in the management function pane; if the system is equipped with ASM Agent, the Health Monitor (Agent) will be shown in the management function pane.

To launch the System Health Monitor, select a system in the Managed System List, and then click **Health Monitor** in the Management Function List. You can also launch it by right-clicking the system name and selecting Health Monitor from the drop down menu.

Enter your user name and password when prompted.

The System Health Monitor shows the following system health status screen, with Chassis, Temperature, Voltage and Fan information etc. which may be different depending on the health monitoring type.



Health Monitor with IPMI / BMC






Health Monitor toolbar

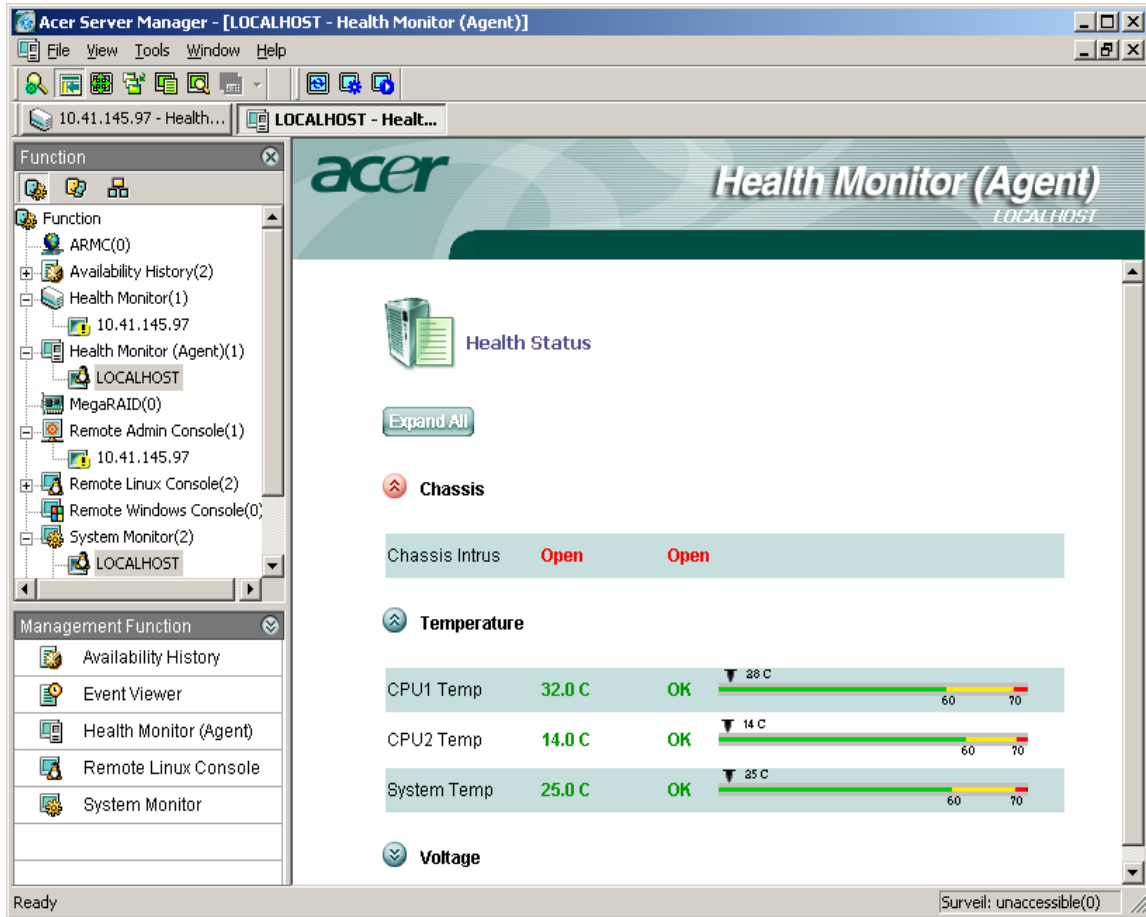
Icon	Description
------	-------------

Power On/Off Powers on or off the managed system.






4 Using ASM6


Icon	Description
Reset 	Resets the managed system.
ID LED On/Off 	Turns the ID LED of the managed system on or off.
Refresh 	Refreshes the managed system's screen.
Auto Refresh On/Off 	Turns the automatic refreshing function on or off.
Refresh Rate 	Sets the refreshing time interval.




Health Monitor with ASM6 Agent


Health Monitor (Agent) toolbar

Icon	Description
	Refreshes the managed system's screen.
	Sets the refreshing time interval.
	Starts the automatic refreshing function.

Icon	Description
	Stops the automatic refreshing function.

Please note that the icons on the system health monitoring screen stand for:

 : The sensors of this device are in healthy states.

 : The sensors of this device are in failing states, or could not be read / detected.

If all the devices of the managed system are in good states, the light indicator in front of the System Summary Status will be green; otherwise it will be Red.

You may click the icon in front of the monitoring device to display the individual sensors and their status.

System Health Monitoring with IPMI / BMC

The System Health Monitoring in ASM6 can automatically detect which health monitoring technology has been deployed in the targeted server, and invoke the right ASM health monitoring module for that technology. If the IPMI/BMC technology has been deployed in the targeted server, then, more health monitoring information will be displayed and handled in five property pages: Platform Information, Health Status, and System Event Log.

Health Status

This page displays several categories of health information from the managed system. The number of actual categories may vary depending on the actual hardware of the managed system.

Current System Power Status: Power status, On or Off.

Accumulated Power On Hours: The amount of time that the system has been on.

Watchdog Timer status (ASR): Status of the Watchdog Timer.

Temperature

CPU Temp: Current CPU temperature in degrees Celsius.

Baseboard Temp: Current temperature of the baseboard.

Inlet Temp: Current temperature at the chassis inlet.

Voltage

CPU Vol: Current CPU core voltage

3.3V, 5V, 12V,5V Standby, 3V CMOS battery: Current voltages respectively.

Fan

Status of the CPU and system fans.

Processor

CPU Status: Summary of CPU status. If any items are abnormal, the status will change to Fail.

Other sensors

Status of other sensors, if any.

Platform Information

This page displays general system information obtained from IPMI / BMC:

Basic Information

Product ID: The product ID of the managed system.

Manufacturer ID: The manufacturer ID of the managed system.

IPMI Version: The firmware version of IPMI.

BMC Firmware Version: The firmware version of BMC.

System GUID: Global unique identifier for each system.

Out of Band IP: The IP address which IPMI / BMC uses to communicate with the ASM console. It could be same or different from operating system's IP address.

Product Information

Manufacturer name: Name of the system manufacturer.

Product name: Product name of the system.

Product part/model number: Part/model number of the system.

Product version: Version of the system.

Product serial number: Serial number of the system.

Base Board Information

Manufacturer name: Name of the base board manufacturer.

Product name: Product name of the base board.

Serial number: Serial number of the base board.

Part number: Part number of the base board.

Chassis Information

Chassis type: Type of the chassis.

Part number: Part number of the chassis.

Serial number: Serial number of the chassis.

System Event Log

This page displays system events logged by IPMI/BMC. The system generates events when there are any abnormal situations, such as low CPU Fan speed, high CPU temperature etc.

System Event Log

Total supported event log number: Total amount that IPMI/BMC can log.

Current Logged event number: Number of events currently in the log.

Last add event log time: Last time an event was logged.

Last erase event log time: Last time events were cleared.

Blue screen log time: The blue screen time logged.

SEL Entries

No: Sequence number of event.

Time: The time the event occurred and was logged.

Description: Description of the event.

Event Direction: Direction of event, it could be **A** for Assertion or **D** for Desertion. For example, if CPU temperature goes too high, it will generate an Assertion event. When it goes back to normal, it will generate a Desertion event.

Clear: Clear all events.

Up: Page up.

Down: Page down

Go to: Go to a selected SEL.

System Health Monitoring with ASM6 Agent

For non IPMI-over-LAN enabled systems, Health Monitoring function requires an ASM Agent. The supported platforms include IPMI 1.0 and SMBIOS models.

The detailed items may vary depending on the specific hardware configuration of the managed system.

Chassis

Chassis Intrusion: Shows the status of the chassis door. It could be OK (door closed) or Fail (door open).

Temperature

CPU Temperature: Current CPU temperature.

SystemTemperature: Current System board temperature.

Voltage

VCORE: Current CPU core voltage.

+3.3V, +5V, +12V, +5VSB, VBAT: Current voltages under respective states.

Fan

CPU Fan: CPU fan revolutions per minute.

System Fan: System fan revolutions per minute.

BPL Fan: BPL fan revolutions per minute.

Move the mouse cursor to any of these items and detailed information will be shown in the left column of the window.

Monitoring System Configuration

System configuration in the ASM6 System Monitor provides administrators with an easy-to-use interface to re-

4 Using ASM6

view system configuration, including information on System, Processors, Memory, BIOS, HDD / IDE / SCSI HDD, Device drivers, Bus type / slots, Ports, Network, Video, operating system, Software, RAID, as well as health status.

System performance in the ASM6 System Monitor provides system availability information with an easy-to-use graphic user interface for monitoring the system status. The information includes CPU utilization, Memory use, HDD activity, and Network information with TCP/IP monitoring, Service and Process monitoring and handling, and System availability report

Disk and storage monitor in ASM6 System Monitor allows administrators to monitor SMART IDE / SCSI / SATA HDDs to predict HDD faults and monitor disk space, issuing an alert if the used space exceeds the threshold setting.

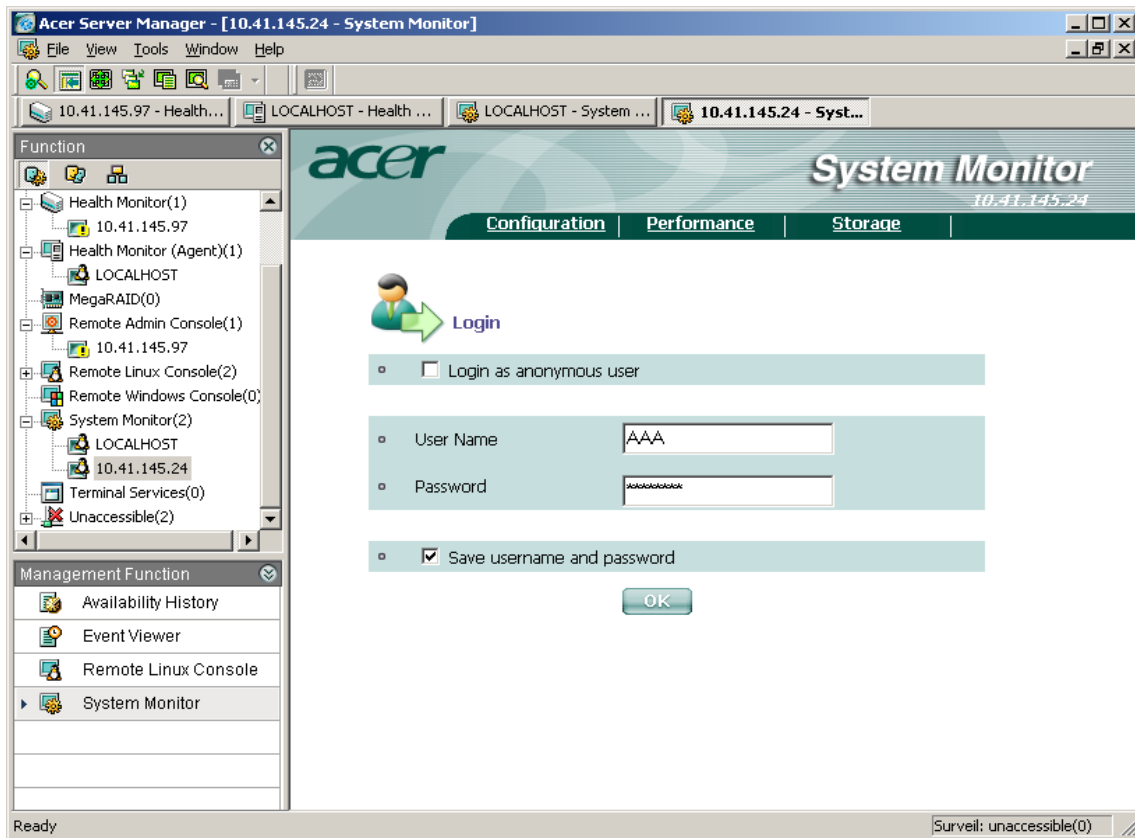
Note: The following description is highly technical. ASM6 System Monitor uses different methods to retrieve management information from System Monitor Agents running on various operating system platforms. If the managed system is running Windows (NT, 2000 or 2003 server), ASM6 System Monitor will retrieve information through Windows Management Instrumentation (WMI) interface. If the managed system is running on Linux, it will use a different set (Pegasus) of CIM interface to retrieve information from Linux Agent. If both of these two methods fail, then, it will try to use SNMP to retrieve information. System Monitor will choose the proper methods automatically; therefore it is completely transparent to users.

Launching System Monitor

To launch ASM6 System Monitor, select a target system from the Managed System List and then click System Monitor in the Management Function List. You can also right-click the system name and then select System Monitor from the drop down menu.

You will be required to enter a user name and password to login before connecting to a managed system. The only exception that user name and password will not be required to login is that if SNMP is being used for the communications between the ASM Console and the managed system.

Note: Because of security limitation, users with empty password may not be used to access Windows XP.



System Monitor Interface

Once the System Monitor is launched, you can view the managed system information in the Working Area. The system information is categorized into three property pages: Configuration, Performance, and Storage.

Configuration

System Monitor allows you to view configuration information for all monitored systems, including: System Summary, System Port, System Slot, System Drive, System Service, and Installed Software.

System Summary - Shows basic system information.

System Port - Shows system port information.

System Slot - Shows system slot information.

System Drive (Windows platforms only) - Shows system drive information.

System Service (Windows platforms only) - Shows the services that are running.

Installed Software - Shows software installed on the system.

Performance

ASM6 Performance Monitoring analyzes potential bottlenecks and the hardware and system capability planning. ASM6 Performance Monitoring translates performance indexes into the operational status against a set of thresholds and criteria to quickly identify problems.

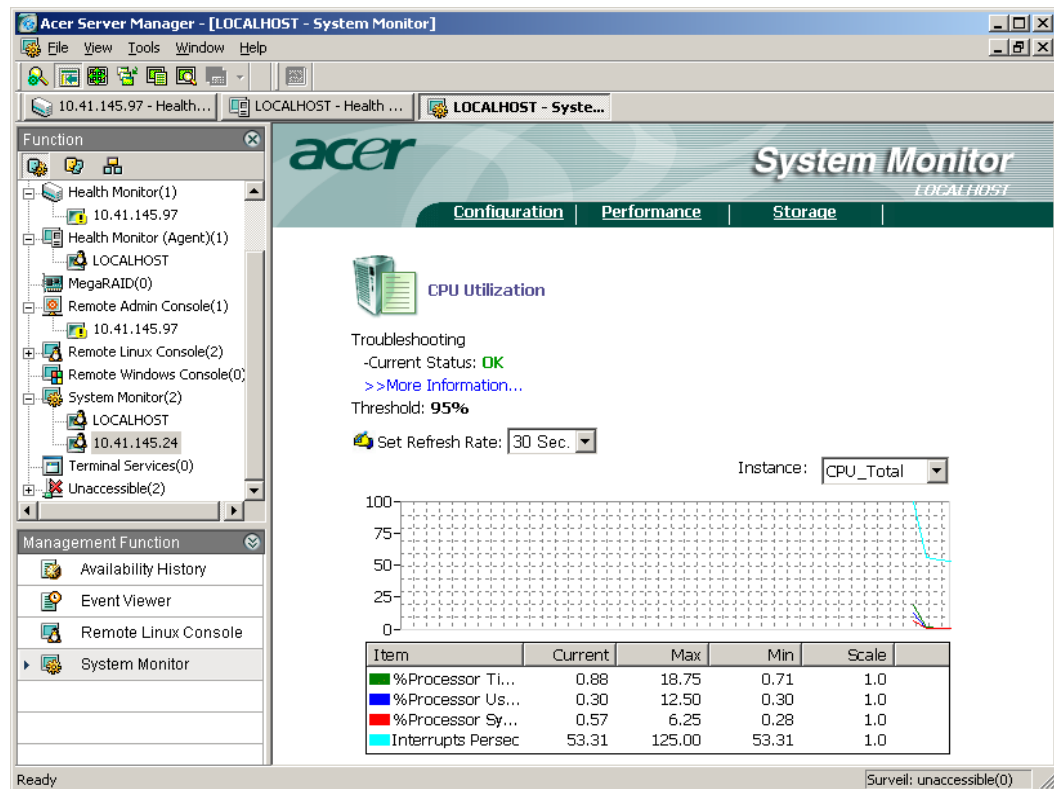
Administrators can set a scale for graphic reports. Right-click in the graphic area and select **Set Scale**. A Set Scale window will be displayed and you can select a new scale.

Note: Threshold values indicate that an undesired limit has been reached. When a threshold value has been reached, an event trap is sent to the ASM Console to alert the administrator.

CPU Utilization

Performance Monitoring displays a dynamic line graph of CPU loading status, to indicate how much CPU power is currently being used. When CPU utilization is too high continuously, it may indicate that the load on your server is approaching capacity. You may need to find the reason(s) and solution(s) to the loading condition, or you may need to upgrade the CPU(s).

The managed system may have more than one CPU. Click the down arrow next to **Instance** to view the working status of each CPU.



Memory Utilization

Performance Monitoring dynamically reports the current memory usage. Continuously high memory utilization may indicate a system over and/or memory resource shortage. Administrator action(s) may be required, such as terminating top memory intensive processes.

Memory Utilization list items


Available KBytes: Shows the amount of free memory.

Page Faults Per sec: The average number of pages faults that have occurred.

Page Input Per sec: The average number of pages read into physical memory from disk when the operating system performs memory swapping.

Page Out per sec: The average number of pages written into the disk from physical memory when the operating system performs memory swapping.

NIC Status

ASM6 Performance Monitoring dynamically displays the NIC (Network Interface Controller) usage status. The NIC Status measures network activity, tracks network card usage, and generates a series of statistics. The information could be especially helpful in studying the server behavior during the heavy loading periods. Detailed information and statistics reported by NIC Status are listed below. If the system contains more than one network card, you can click the arrow  next to the current network card name to view the working status of each network card.

NIC Status list items

Bytes/Sec. In: Bytes received per second.

Bytes/Sec. Out: Bytes sent per second.

Packets/Sec. In: Packets received per second.


Packets/Sec. Out: Packets sent per second.

Errors/Sec. In: Errors received per second.

Errors/Sec. Out: Errors sent per second.

HDD Performance

HDD Performance graphically displays HDD usage in graphics. The HDD activity is another important performance index to track. Depending on the major applications running on the server, excessive HDD inputs, outputs, and delays will cause lags in the run-time environment, which in turn cause more CPU and memory loading greatly reducing system performance. Information and statistics provided by HDD Performance are listed below.

If the system contains more than one hard disk, then, you can click the arrow  next to the current hard disk name to view the working status of each hard disk.

HDD Performance list items

% Disk Time: The percentage of time that the selected disk drive spends reading or writing requests.

Average Disk R/W time: The average time (in seconds) to read or write data to the disk.

Disk Transfer Number: The rate of read and write operations on the disk.

Disk Transfer Bytes: The bytes transferred to and from the disk.

Running Processes

Running Processes displays all applications that are currently running on the system.

Setting scale for the graphic reports

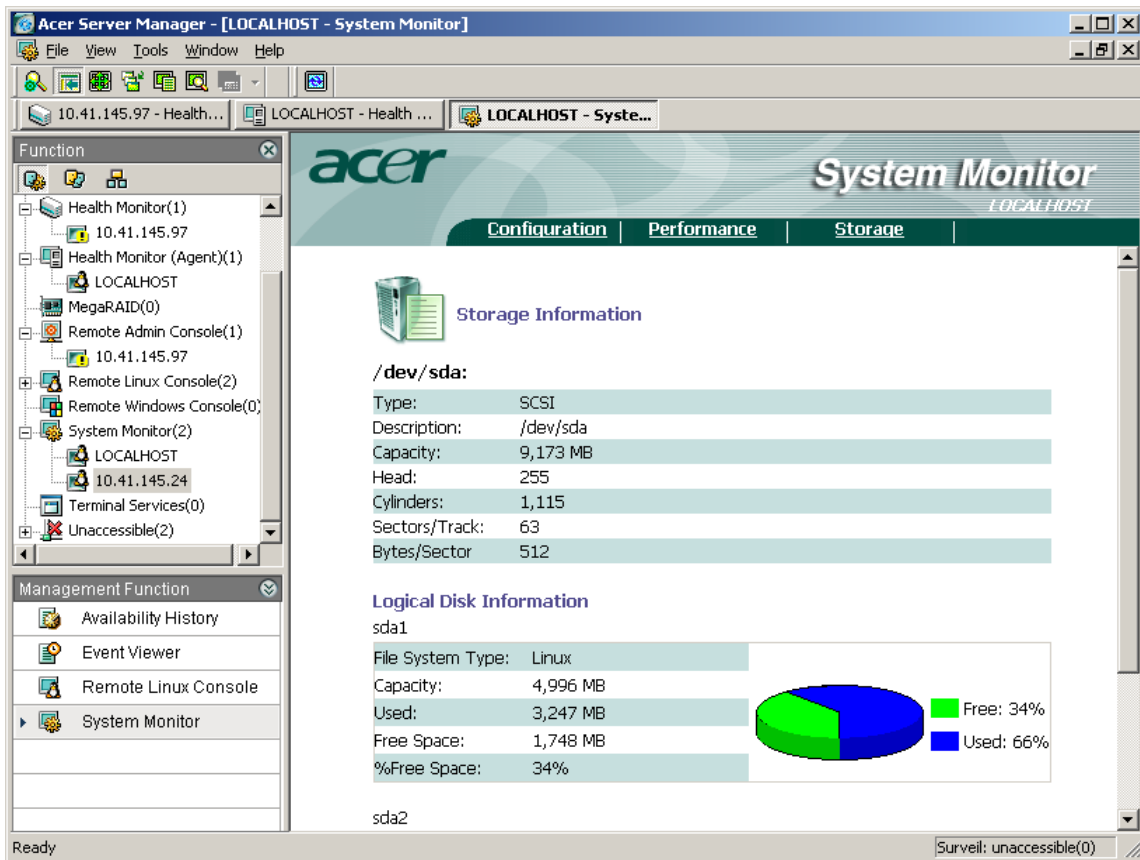
On the CPU Utilization, Memory Utilization, NIC Status and HDD Performance pages, you can set a desired scale for the graphic reports.

Right-click in the graphic area and select Set Scale. A Set Scale window will be displayed and you can select a new scale.

Storage

Storage Monitoring provides HDD information. You can check the physical disk specifications, the logical defini-

tion and usage, and the S.M.A.R.T. status of HDDs. Click the icon before each item to view its details.



Click the name of a physical disk and its information will be displayed, including Type, Description, Capacity, Heads, Cylinders, Sectors per Track, Sector Size, Bad Blocks / Sectors.

The information of the Logical disk(s) is displayed next, which includes File System Type, Capacity, Used space, Free space, %Free Space. The percentage of free space on the logical disk(s) are illustrated in a pie chart at the right.

S.M.A.R.T in System Monitor

S.M.A.R.T. stands for Self-Monitoring Analysis and Reporting Technology. Based on the statistics and failures of the current HDD Read / Write operation, it can predict and report impending failures so that preventive actions can be taken in time. The S.M.A.R.T. alert indicates that HDD operation has reached a pre-defined threshold. Preventive measures are strongly recommended.

S.M.A.R.T. support can be enabled in the system BIOS.

System Monitor Agent

System Monitor Agent enables S.M.A.R.T. support on IDE and SCSI HDDs. It collects S.M.A.R.T. data periodically and analyses the information. When measurements exceed the threshold levels, the S.M.A.R.T. mechanism sends an event trap to the ASM Console.

System Monitor Console

The System Monitor console shows information and the health status of IDE and SCSI HDDs provided by the System Monitor agent. When an event trap is received by the console indicating a S.M.A.R.T. error, you will be notified by the ASM alerting mechanism via e-Mail, Pop-up message, Audio Alarm, or other pre-assigned application.

Managing Through Web Access

The ASM6 Web Viewer function allows you to manage your networked systems with built-in web server support. One good example is to use ASM6 Web Viewer to manage the system with an Acer Remote Management Card (ARMC) installed. The ARMC provides built-in web-based system management capabilities. From Web Viewer, you can easily connect to the ARMC main page, and monitor targeted systems through comprehensive Web pages.

Launching Web Viewer

To launch Web Viewer:

Select the target system in the Managed System List and then click Web Viewer in the Management Function List. The pre-linked web (main) page will appear in the working area.

Adding a URL

To add a URL that can be managed by Web Viewer:

Right click in the Managed System area, choose Web Viewer, and then Edit. In the Config URL window, click Add, enter the URL and click OK.

Using External Tools

ASM6 has flexibility and extendability built-in. You can make use of the Tool Configuration capability of ASM6 to select and configure external tools to be used in ASM6.

Adding a New Tool

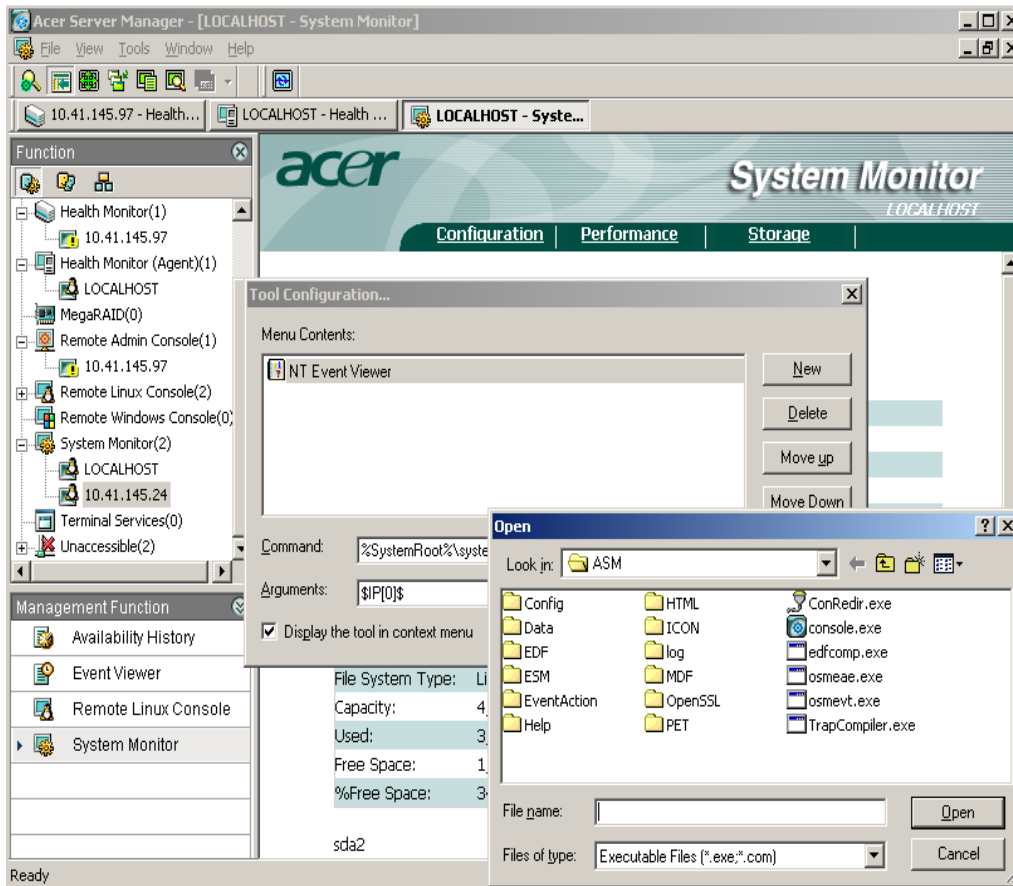
The addition of new tools allows you to select and configure external tools using ASM6 for extended manageability. You can invoke these tools interactively from ASM6 console when needed; or you can associate specific tools with the specific event occurrences to achieve automatic server management.

To add a new tool:

- 1 Click on the **Tools** menu and then choose **Tool Configuration...** from the drop-down list. A Tool Configuration dialog box will appear.
- 2 Click the **New** icon.
- 3 Enter the name for the new tool to be added.
 - If you want to reposition the tool in the list, select the tool and then click the Move Up / Move Down button.
 - If you want to change the display icon for the tool, please click the **Change Icon** button, and then choose the desired icon.

4 Using ASM6

- 4 Click the **Browse** button on the right of the Command field to choose the desired tool.



- 5 Click **Open** and the path for this tool will be displayed in the Command field.
- 6 Choose **Arguments** for this tool.
- 7 If advanced configuration options are needed, click the **Advanced** button. The dialog box will expand with advanced options to be configured.
 - Display the tool when selected system(s) comply with the following rule - This option allows you to set several rules. Once set, the tool will be displayed only when all of these rules are met.
- 8 Click the **Close** button in the dialog box to complete the new tool addition.

Deleting a Tool

To delete a tool.

In the **Tool Configuration** dialog box, select the tool you want to delete and then click the **Delete** button.

Note: The tool will be deleted directly from the tool list, there is no confirmation prompt.

Monitoring MegaRAID

MegaRAID is a kind of RAID controller.

4 Using ASM6

MegaRAID function in ASM6 allows you to monitor your networked systems with MegaRAID installed. You can use ASM6 to view MegaRAID related information, such as adapters, channels, physical disks, logical disks, etc. In order to do so, please make sure you have correctly installed MegaRAID.

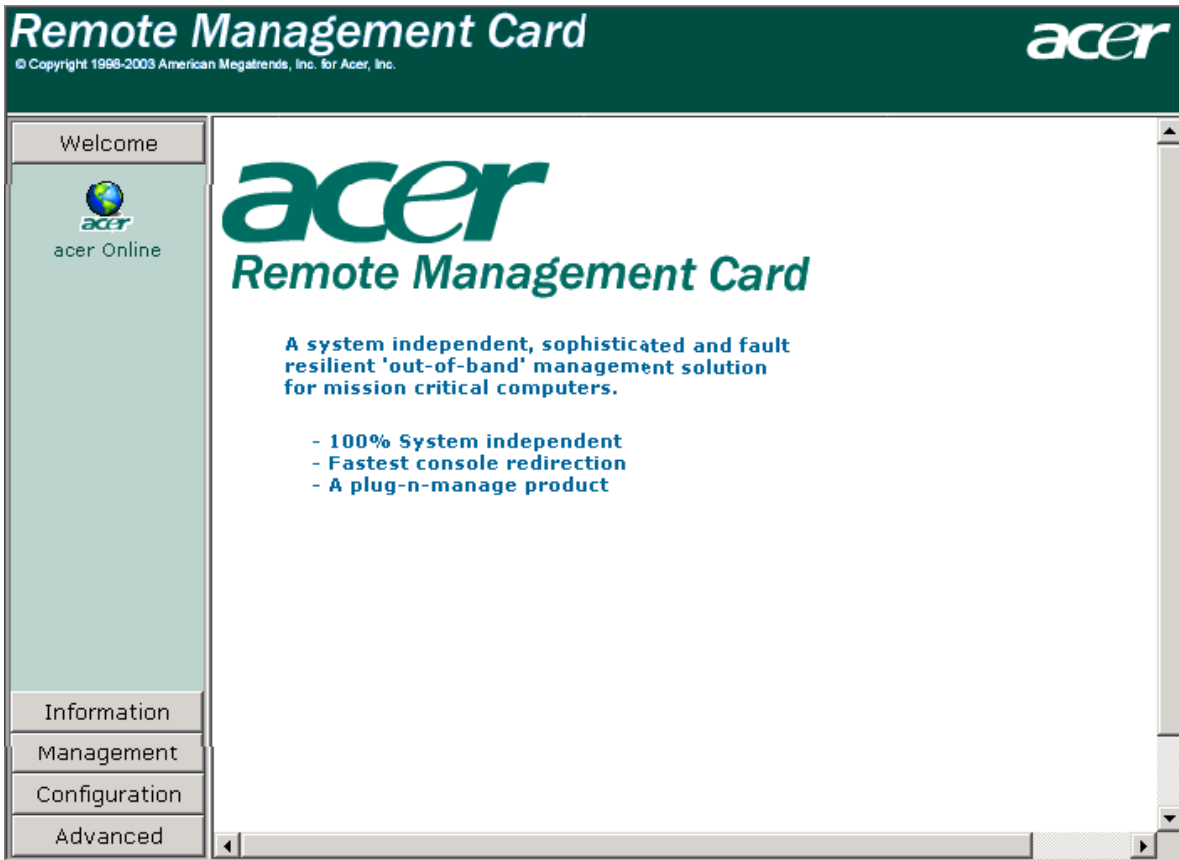
MegaRAID hardware and software are from its vendor. When you install MegaRAID software, please read all license agreements.

The screenshot displays the Acer Server Manager interface for the MegaRAID M25D-1 controller. The left sidebar shows a tree view of system components, with MegaRAID selected. The main pane shows a tree view of the MegaRAID configuration, including Adapters, Channels, and Logical Drivers. The right pane displays detailed information for a physical drive.

Physical Drive -- IBM DNES-309170W SA30	
Adapter Number	1
Physical Channel	1
Target ID	0
State	Online
Array Position	A1-1
Size(MB)	8715
Device Type	Disk
Inquiry String	IBM DNES-309170W SA30
SCSI Level	SCSI3
Maximum Queue Depth	32
Rebuild Progress	Not In Prog
Medium Errors	0
Physical Slot Status	0
Physical Slot Number	0
Other Errors	0
Physical Termination	Wide
Physical Speed	Maximum
SCSI LUN ID	0

Monitoring ARMC

Acer Remote Management Card (ARMC) provides more management features for your servers. After you have installed and configured the plug-in card in your server, ASM6 enables you to easily browse the Web-based management pages built in ARMC.



5 ASM6 Event Manager

In server management, event notification is one of the most important and critical features to support anywhere, anytime server manageability. When a hardware or system error has occurred or a particular threshold setting has been exceeded, the ASM agent detects this condition and sends an event trap to the Event Manager within the ASM Console. Use the Event Viewer to interact with the ASM Event Manager.

ASM6 Event Viewer

When ASM Agent detects error conditions or pending problems, an event trap is sent to the ASM Event Manager. The event will then be displayed in the Event Viewer. The Event Viewer can be used to get a better understanding of the event nature, to prepare responding actions to resolve the problems.

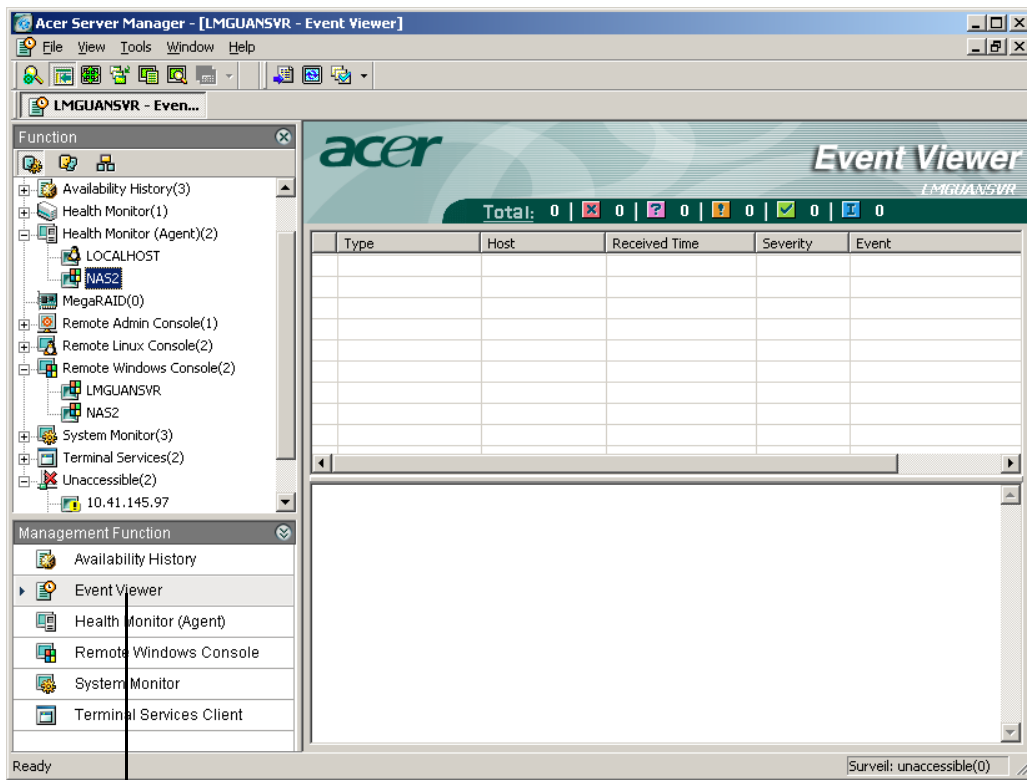
Launching Event Viewer

There are two ways to launch the Event Viewer -- an independent Event Viewer application, and a snap-in Event Viewer integrated with the ASM Console.

The independent Event Viewer application is automatically launched as your operating system is being started, and an Event Viewer icon will be shown in the system tray. Double-click the Event Viewer icon to bring up the Event Viewer window. Once finished, right-click the Event Viewer icon and select Exit to close Event Viewer.

5 ASM6 Event Manager

For the snap-in Event Viewer, launch it from the Management Function List.



Event Viewer

Event Viewer User Interface

When ASM Event Manager receives an event trap, the event is logged in the real time log and displayed in the Event Viewer, with the following information:

Type: The event type

Host: The name of the system where the error or warning event occurred.

Received Time: The time when the Event Manager received the error or warning event.

Severity: The severity of the error or warning event. Severity is classed as Information, Recoverable, Warning, Critical, or Non-Recoverable.

Event: a brief description of the error or warning.


Click an event and its information will be shown in the lower window.


Viewing Events


Once the Event Manager is launched, an add-on toolbar with three icons on it appears.

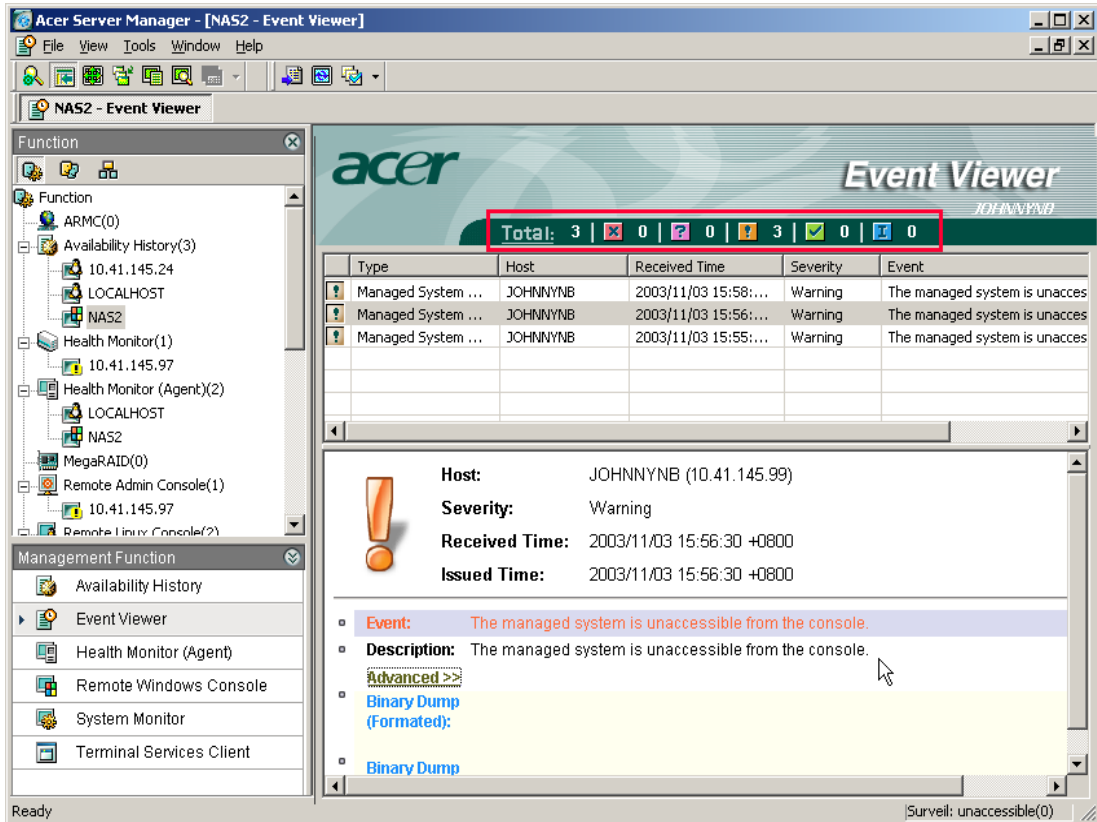


The three icons on the add-on toolbar are:

 **All Systems:** Click this icon to show events for all the systems that are being monitored.

 **Refresh:** Click this icon to refresh the events shown in the Event Viewer window.

 **Filtered by Severity:** Use this icon to filter events by severity level. Click the down arrow next to this icon to open a drop down list showing all the severity levels for you to choose from. Choose a severity level to display all events with the selected severity level. You can also filter the events by clicking the corresponding severity level icon above the event list.



Event Rules


Event Rule Setup in ASM Event Manager allows you to specify target systems and events you are interested in. Select specific conditions you want to distinguish from (critical temperature, high bus utilization, etc.), the alert methods you prefer to receive, and the responding actions you would like to take upon receipt of the event.


To set up event rules, click the Tool menu, then, click Event Rule Setup... to launch the Event Rule Setup window

Using Wizard to Create Event Rule

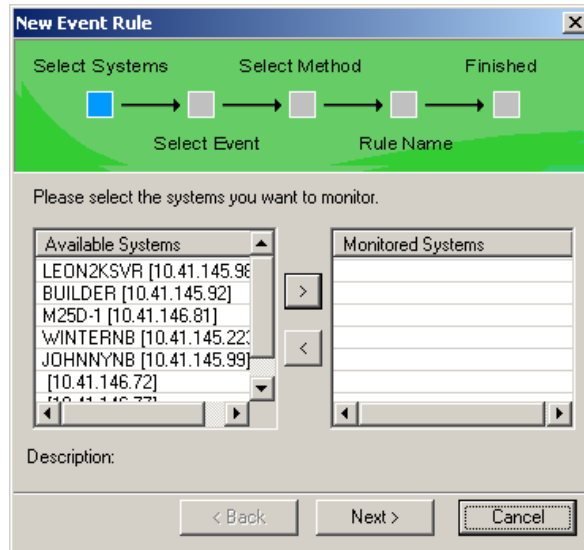
ASM Event Manager provides an easy way for you to create event rules using a wizard. From the **Event Rule Setup** window, click the arrow next to the **New** button then select **By Wizard...**, and follow the wizard prompts step by step to create an event rule.

5 ASM6 Event Manager

- 1 Select the system you want to monitor in the Available Systems list field, and then click the  button to add it to the Monitored System list.

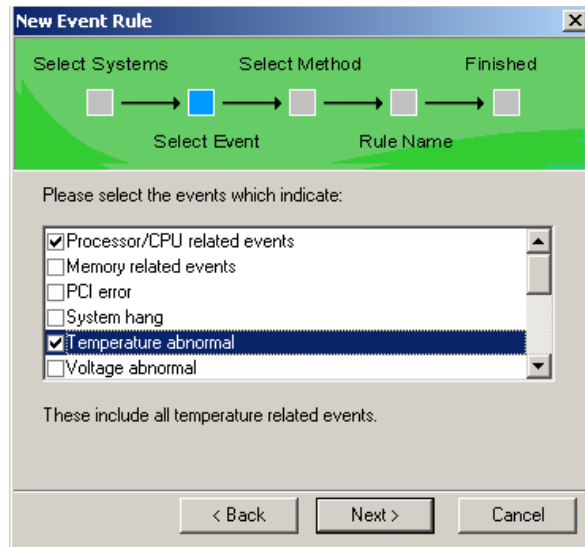
If you want to remove a system from the Monitored System list, select it and then click the  button.

Click **Next** to continue.



- 2 Select events.

Select the event types from the list.



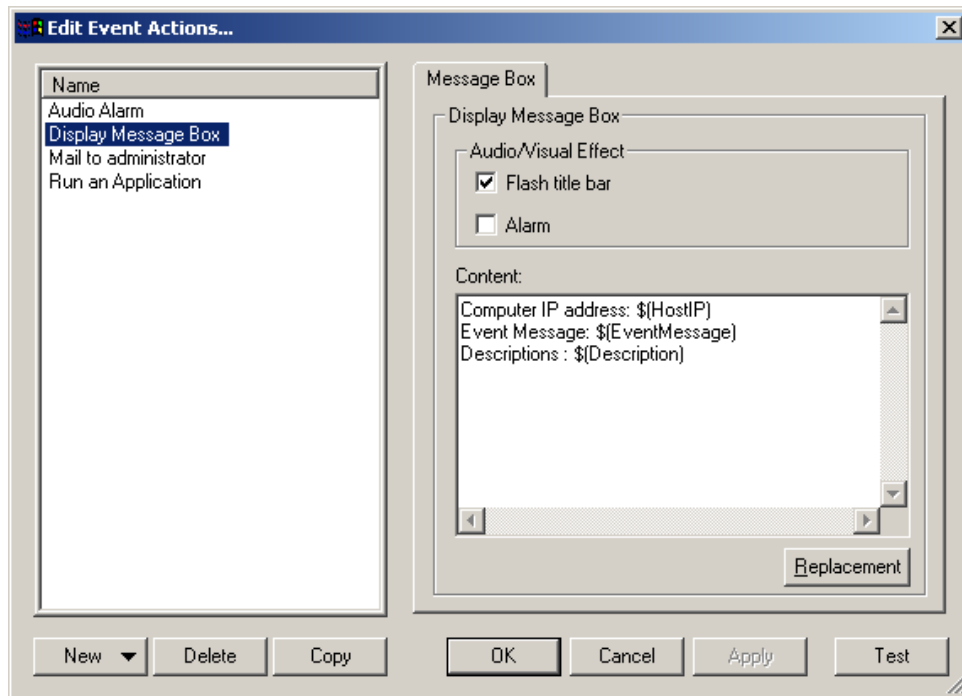
Click **Next** to continue.

- 3 Specify actions to be taken.

Select the action type first and then click the **Details...** button to edit the detailed action.

- **Display Message Box**

If all conditions are met, a message box will be displayed on the ASM Console.



If **Flash title bar** is checked, the title bar of the message box will be flashing when the message box pops up.

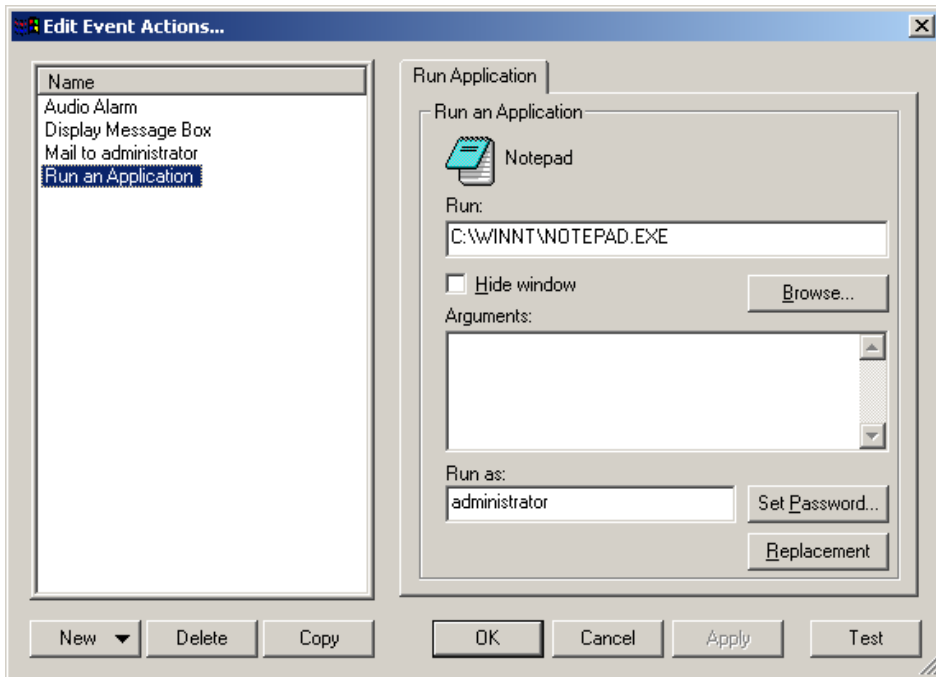
If **Alarm** is checked, the system will beep when the message box pops up.

If **Replacement** is clicked, a list of computer information options will be shown, for you to select and to replace with the message box content. When an option is selected, the option will be added to the Content field of the message box. When the message box is displayed, the message box items will be replaced with the selected computer information.

Once finished, you can click **Test** to preview the message box content.

- **Run an Application**

If all the conditions are met, ASM6 will run an application in response to the event.



Click Browse to select an application to be launched when event conditions are met.

Hide window

If you check Hide window, the application's window will not be displayed when it starts.

Replacement

Click Replacement. A list of computer information options will be displayed for your selection, including: Host Name, Host IP Address, Event Type, Event Message, Received Time, Issued Time, Event Description and Event Severity. When you select an option, it will be added to the Arguments field of the command line. The application will use these arguments to handle the event when triggered.

Run as

Enter a user name to run this application. Click **Set Password** to set the password for this user.

Test

To run the application as a test.

- **Mail to Administrator**

If all conditions are met, an email will be sent to alert the system administrator. Before this function can be used, you should prepare a profile first.

Enter the name of the new profile, as prompted.

Enter your email address in the following screen, as prompted.

In the next screen, enter the name of the SMTP server. If Event Manager fails to send an email to the address you specified in the Edit Event Actions dialog box, it will return the email to the sender whose address is specified in "Your mail address" with the cause of the error.

Now, enter the requested server information.

New profile 3/4

You have to specify SMTP server name or its IP address, and its port number, the default port number is 25, other port number is not recommended.

Outgoing mail (SMTP):
server1

Port number:
25 Use Default

< Back Next > Cancel

And then, enter the authentication information if necessary.

New Profile 4/4

Some SMTP server requires authentication, if your SMTP server requires authentication as well, you have to supply one.

My server requires authentication

Account: aaaa

Password: xxxx

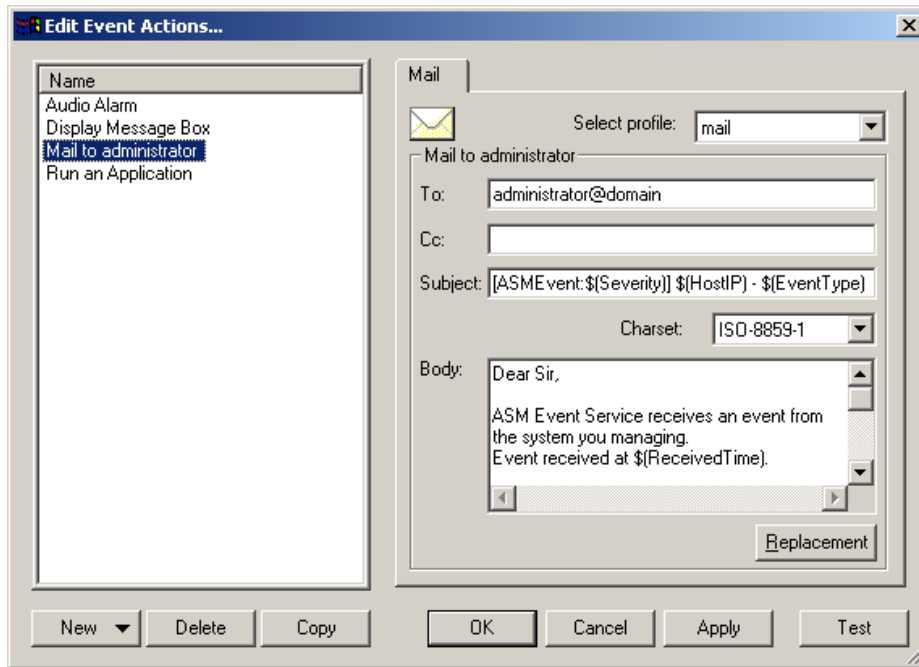
< Back Finish Cancel

After the profile is created, compose the mail in the **Edit Event Action** window.

You may click **Replacement** to get a list of computer information options such as: Host Name, Host IP Address, Event Type, Event Message, Received Time, Issued Time, Event Description and Event Severity. You can select an option to be added to the insertion point within your e-mail. When the e-mail is being sent, those items selected will be replaced.

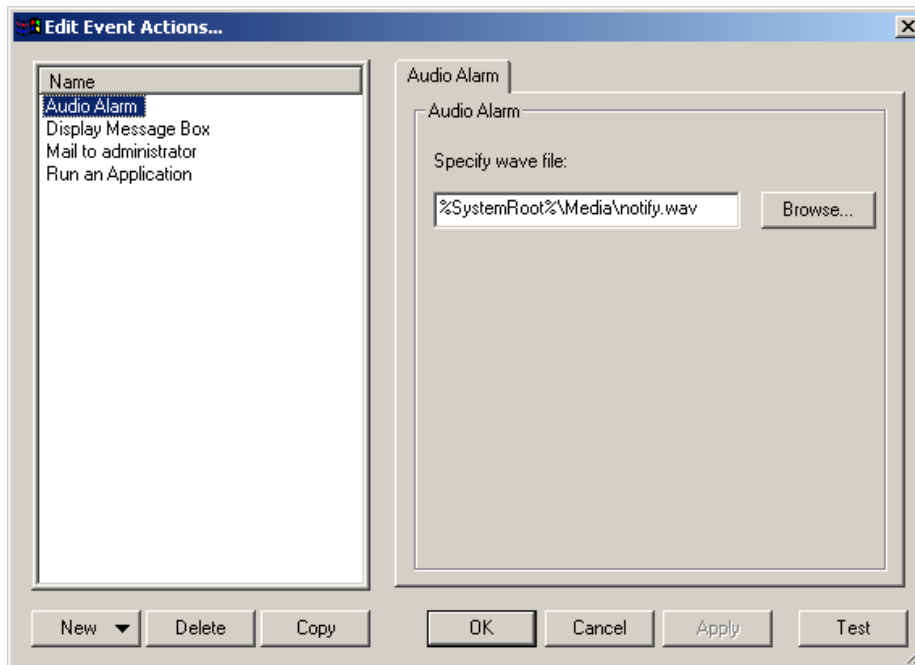
5 ASM6 Event Manager

Click Test to send a test email.



- **Audio Alarm**

If all the conditions are met, an audio (.wav file) alert will be played.



- 4 Click **Next** to continue.
- 5 Enter the name for this rule and then click **Next**.
- 6 Click **Finish** to complete the operation.

Creating Event Rule in Advanced Mode

You can also create event rules in advanced mode. From the **Event Rule Setup** window, click the arrow next to the **New** button then select **New...**, or click the **New** button directly to bring out the **New Event Rule** window.

Choose the conditions to be applied for this rule in the top list and then select the actions in the second list. If details need to be set, click the **Edit Action** button. Specify the conditions in the third list.

New Event Rule

Select conditions and actions first, then click on an underlined value to edit it

1. Select conditions for the rule:

<input type="checkbox"/> System name contains:	<input type="checkbox"/> Event severity is less than:
<input type="checkbox"/> System name is:	<input type="checkbox"/> Event severity is more than:
<input type="checkbox"/> System's IP is:	<input type="checkbox"/> Time and count restriction is:
<input type="checkbox"/> System belongs to subnet:	<input type="checkbox"/> For any event
<input type="checkbox"/> Event type is a kind of:	
<input type="checkbox"/> Event message contains:	
<input type="checkbox"/> Event severity is:	

2. Select Action for the rule: Edit Action

<input type="checkbox"/> Display Message Box
<input type="checkbox"/> Run an Application
<input type="checkbox"/> Audio Alarm
<input type="checkbox"/> Mail to administrator

3. Rule description (an underlined value to be defined):

Apply this rule after the event arrives.
No condition(s) defined.
No action(s) defined.

4. Rule name:

OK Cancel

- **System name contains:**

Specify the characters or substrings contained in the system name.

Specify Words In System Name

Word in Name: Add

Name	
A	


Remove Option...

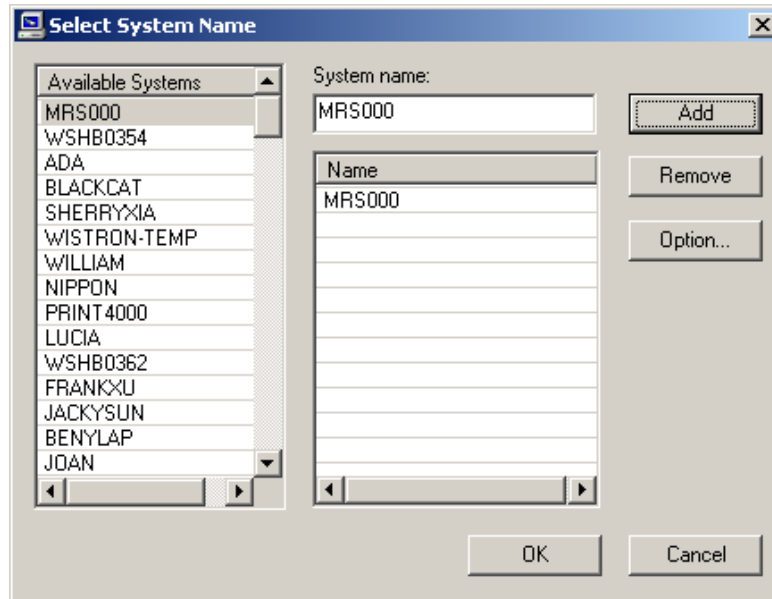
OK Cancel

- **System name is:**

5 ASM6 Event Manager

From the New Rule window, you can check this option to specify the name of the system.

Click the  icon next to "System name is" and the **Select System Name** dialog box will open.



You can choose system name from the Available Systems list or enter the system name manually in the System name field. Then click the **Add** button to add it into the Name list. You can specify multiple system names in one rule. Click OK to finish.


Click the **Option** button to open the Rule Option dialog box. You can choose:

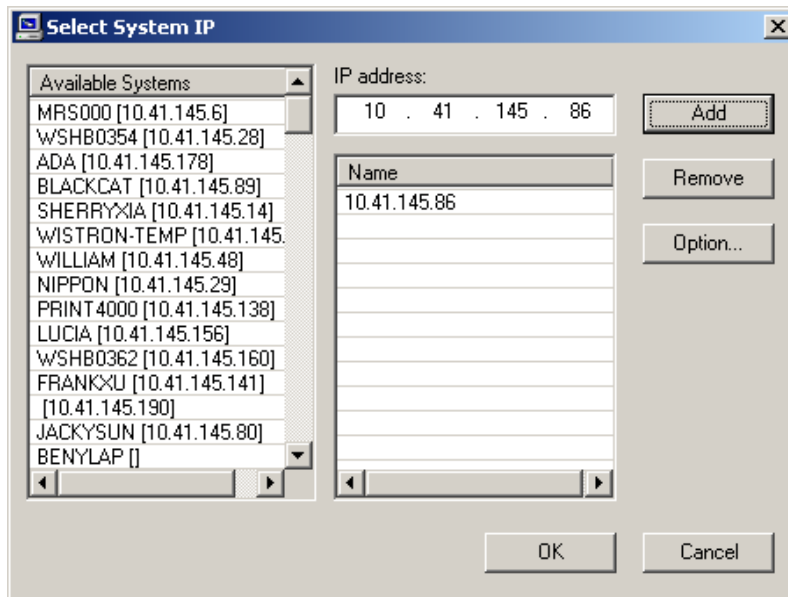


contains - Only the system(s) with the specified name(s) can trigger the actions.

not contains - All systems except those specified can trigger the actions.

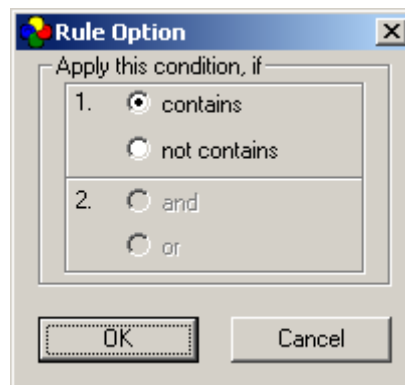
- **System's IP is:**

From the New Rule window, you can check this option to specify the IP address of the target system. Click the  icon next to "System's IP is" to open the **Select System IP** dialog box.



You can choose from the list of Available Systems, or enter a different IP address, then click the **Add** button to add it to the list. You can add several systems to the Name list in one operation. Once the addition of IP addresses is completed, click **OK** to finish.

From the Select System IP window, you can click the Option button to open the Rule Option dialog box, which allows you to choose the rule option.

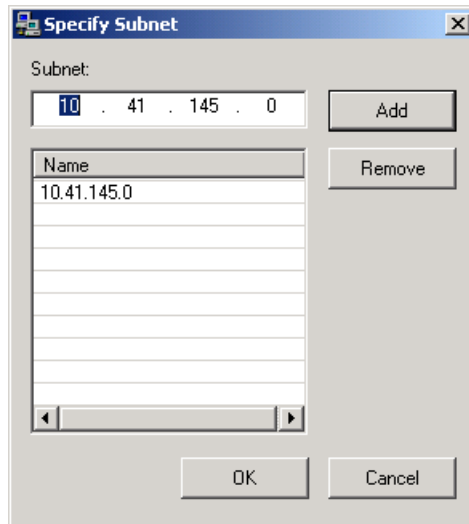


contains - Only the system with the specified IP address can trigger the actions.

not contains - All systems except those specified can trigger the actions.


- **System belongs to subnet:**

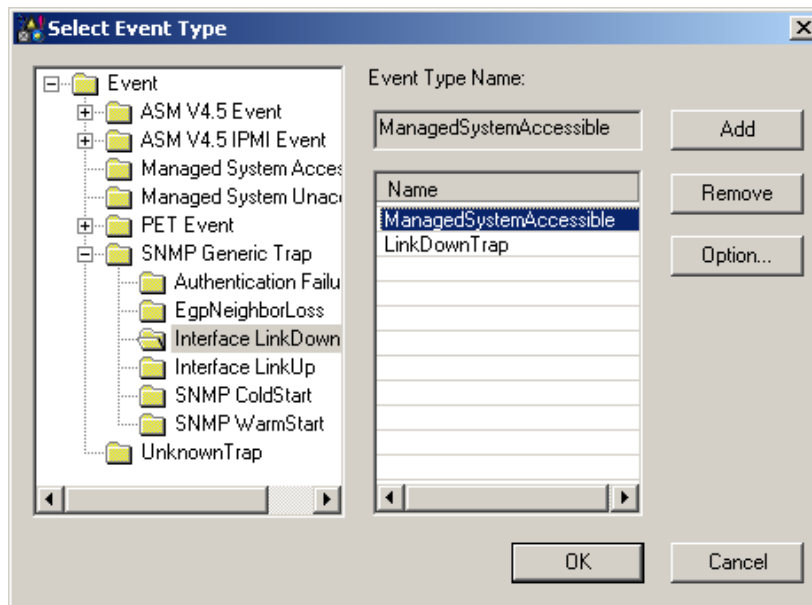
Select the subnet to which the targeted system belongs.



- **Event type is a kind of:**

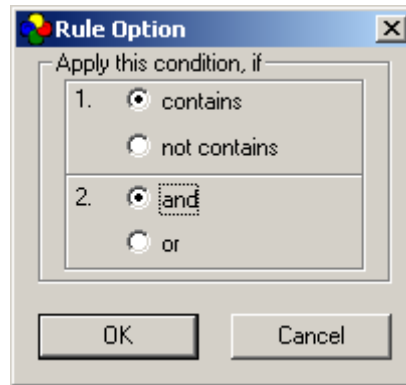
From the New Rule window, you can select the Event type is a kind of to specify the event type of interest.

Click the  icon next to "Event Type is a kind of" to open the Select Event Type dialog box.



You can choose from the Event list on the left and then click the Add button to add it into the Event Name list on the right. You can specify several event types at the same time and add them to the Event Name list. Once completed, click **OK** to finish.

Click the **Option** button to open the Rule Option dialog box, which allows you to choose the rule option.



contains - Only the specified types of conditions can trigger the actions.

not contains - All types of conditions except those specified can trigger the actions.

and - The actions will not be triggered until all types of conditions you specified are met.

or - The actions will be triggered if any condition you specified is met.

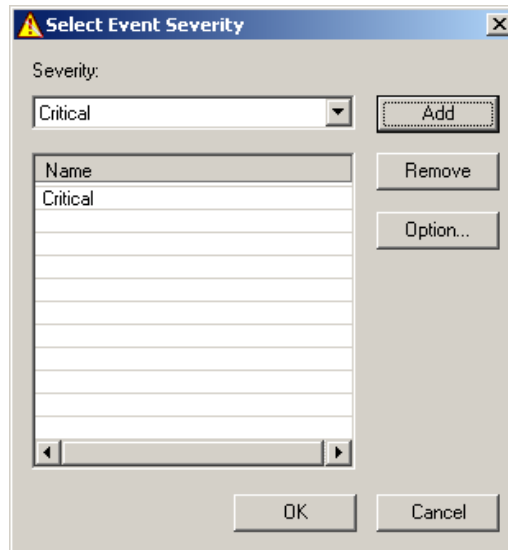
- **Event message contains:**

This option allows you to select key words to be searched in event messages. A Specify Event Message window will pop up to allow you to specify words or phrases you want to find in an event message.



- **Event severity is:**

Select the severity level so that actions will be triggered if the occurring event is at the specified severity level.



- **Event severity is less than:**

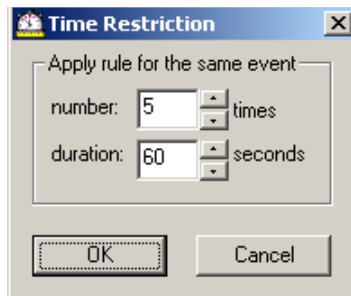
Select the severity level so that actions will be triggered if the severity of the occurring event is less than the specified level.

- **Event severity is more than:**

Select the severity level so that actions will be triggered if the severity of the occurring event is higher than the specified level.

- **Time and count restriction is:**

Select this item to specify the limits on the number and duration of the repetitive recurring events.



- **For any event** - Any event will trigger the actions.

Once completed, enter the name for the rule in the Rule Name field.

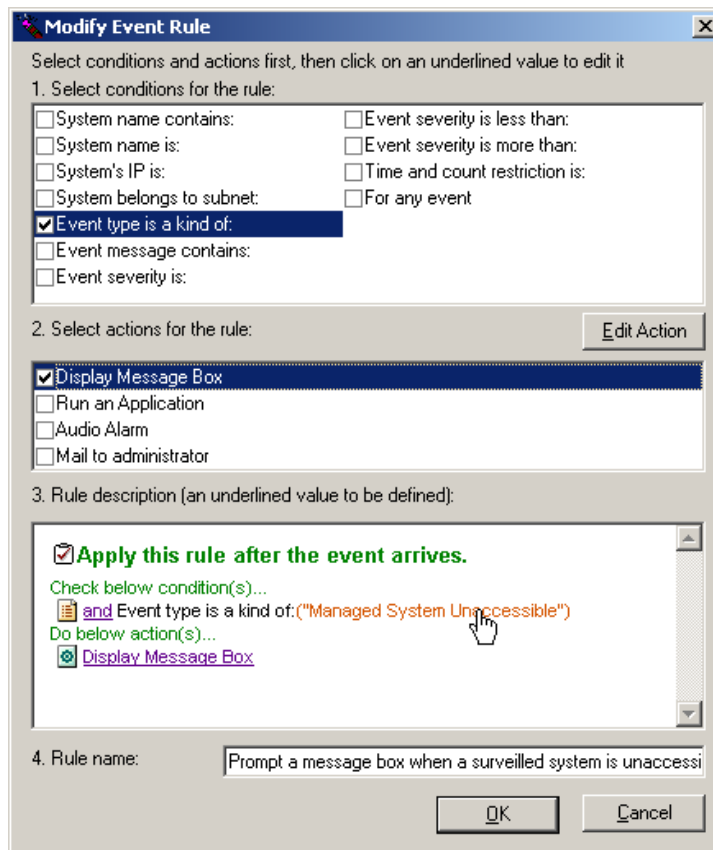
Click **OK** to complete the new event rule setup.

Modifying Event Rule

You can also modify an existing event rule.

5 ASM6 Event Manager

In the main dialog box choose the event rule you want to modify and then click the **Modify...** button, the Modify Event Rule dialog box will appear.



Modify an event rule in a similar way as creating a new one. Please refer to Creating Event Rule in Advanced Mode on page 59.

6 Remote Management

ASM6 provides features such as remote consoles which allow you to manage monitored systems remotely. This chapter is dedicated to describing ASM6 remote management features. The first section discusses the needs and the rationale of having remote consoles of different kinds. The following sections explain different kinds of ASM remote console features and services. The last section explains how to use Microsoft Windows Terminal Services Console from the ASM Console.

Remote Console Overview

ASM6 Remote Console features are provided for you to remotely manage servers. ASM6 Remote Console is a powerful tool which redirects BIOS, OS information and operation of managed servers to the ASM Remote Console no matter what state the managed system is currently in.

ASM6 Remote Console includes:

Remote Admin Console

When your system is powered on, BIOS takes control with fundamental functional support. If the system suffers a key hardware component failure, going through the Power-On System Test (POST) and BIOS Setup could be the only way to detect the problem, sometimes to partially / temporarily limit the problem and keep the system running. In order to support remote manageability at this stage, two technological supports need to be there: BIOS sends and receives console I/O through the serial I/O port in parallel, and a management processor communicates the Serial Over LAN (SOL) with the remote console, since the system functional support is at the minimum level. The management processor is the BMC, implementing the IPMI standards. IPMI / BMC provides additional functionalities such as Sensor Data Record (SDR), System Event Logging (SEL), Field Replaceable Unit (FRU), remote power control. Due to the additional costs of BMC hardware, firmware, and software, this solution is only available on high-end server product lines.

Remote Admin console is a powerful function which redirects BIOS, OS information, and operation on the system side to the remote console.

Remote Windows Console

With Windows running on the managed server, more services and resources are available, and more advanced remote features are supported. To provide OS Console services, OS RCA, implemented as an application service in the corresponding OS environment at the managed system side, redirects the Graphics or text mode console inputs and outputs to the OS Console within ASM Console. It allows you to remotely perform OS-based operational and maintenance tasks as if you were sitting in front of the managed systems.

Remote Windows console redirects graphical or text mode console inputs and outputs from the managed system running Windows (with Remote Console Agent installed) to the ASM Console.


Remote Linux Console


Remote Linux console redirects graphical or text mode console inputs and outputs from the managed system running RedHat Linux (with Remote Console Agent installed) to the ASM Console.

Terminal Services Console

Terminal Services Console allows you to access a Windows server running Windows Terminal Services and take over via remote operation.

ASM6 Remote Admin Console

ASM6 will launch a different Remote Admin Console depending on different managed servers equipped with IPMI /BMC. Pressing  **Remote Admin Console** in the management function pane will launch the Remote Admin Console (DPC Console) for R701, and G90x systems, while pressing

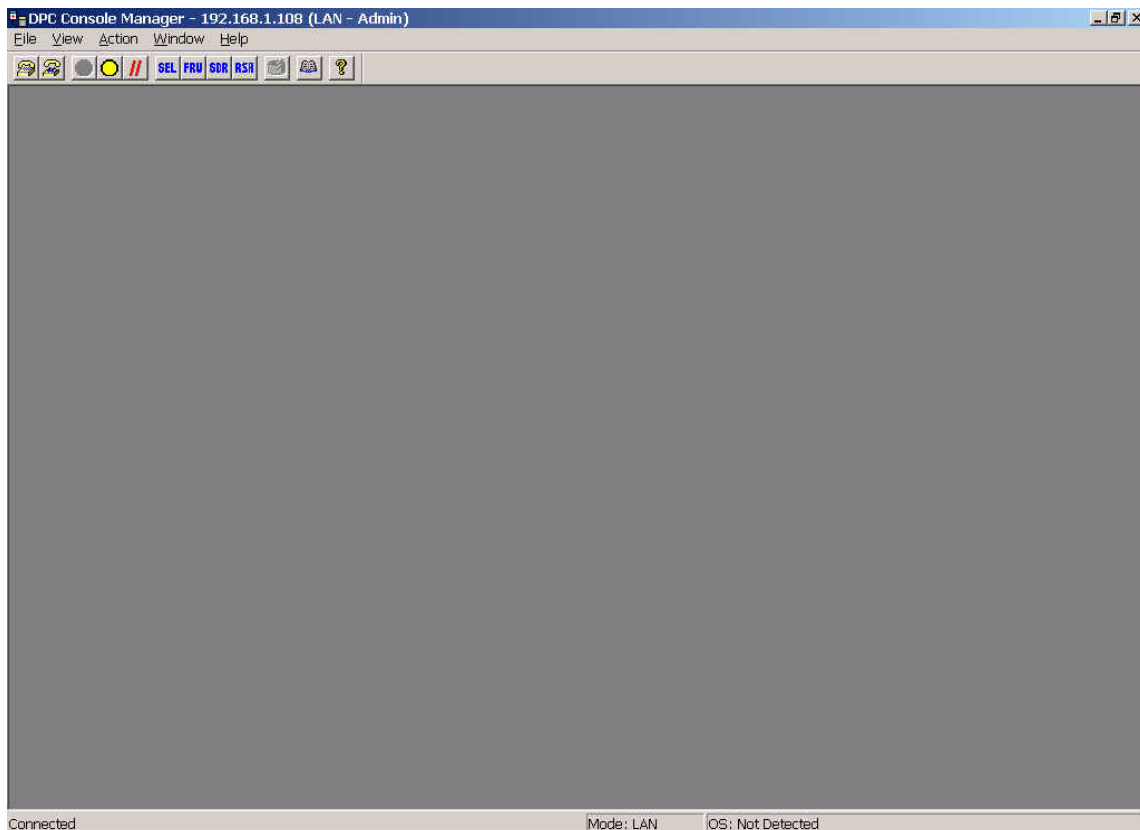
 **Remote Admin Console** will launch the Remote Admin Console for G70x systems.

Remote Admin Console for R701, and G90x systems:

To make the Remote Admin Console for R701 and G90x systems work normally, you should install the DPC Console in ASMe package to the system with ASM Console. The ASMe software is packaged on the same CD with ASM 6.

Launch the Remote Admin Console:

When you select a managed system with Remote Admin Console, and click the Remote Admin Console in management function pane, the DPC Console will be launched as shown below.

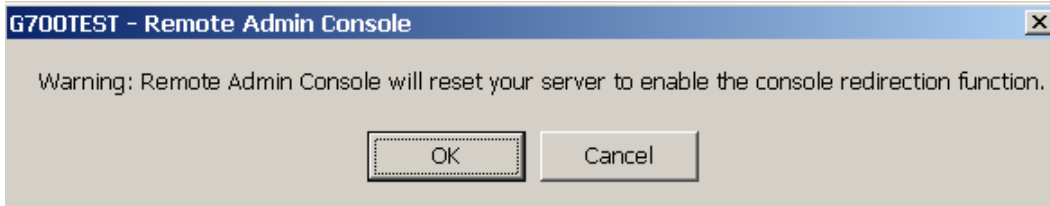


You can operate the DPC Console for a specific function. For the detailed operations of DPC Console, please refer to the ASMe User's Guide.

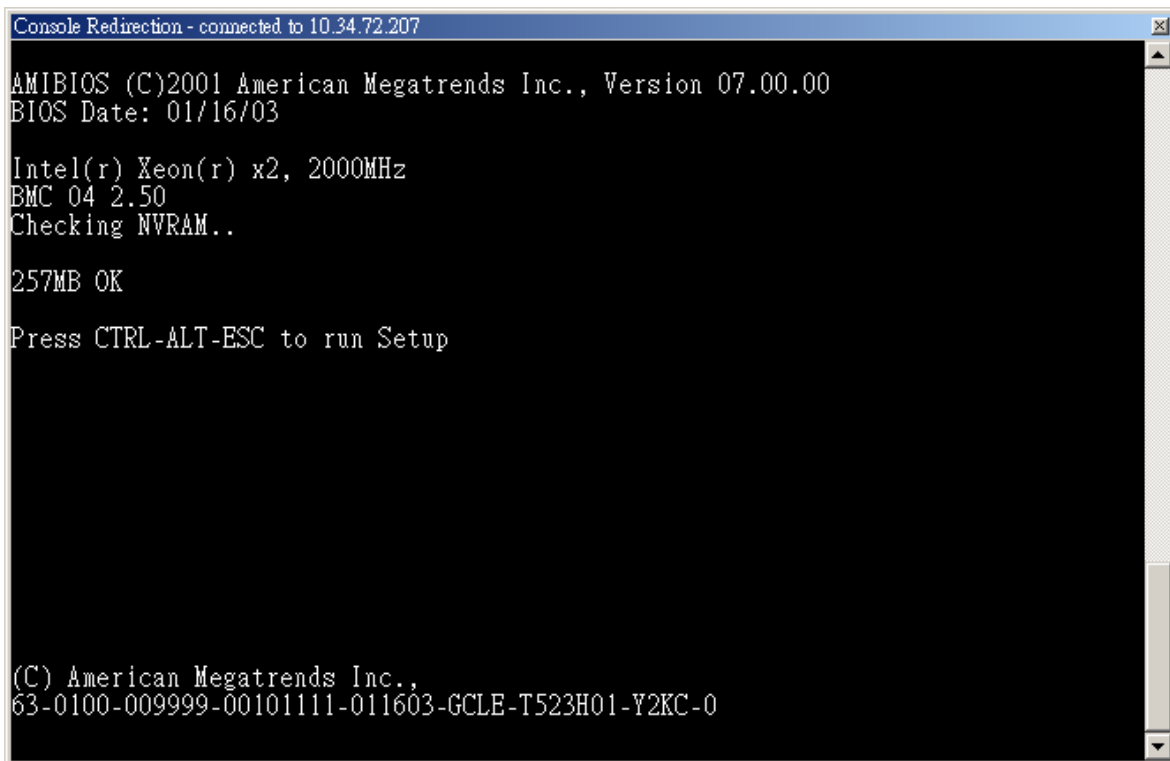
Remote Admin Console for G70x systems:

Launch the Remote Admin Console:

When you select a managed system with Remote Admin Console, and click the Remote Admin Console, the following dialog box will appear. The Remote Admin Console will ask you whether to accept the following operation.



Warning: Remote Admin Console will reset your server to enable console redirection. If you select Cancel, the Remote Admin Console will do nothing. If you select OK, it will reset the system. The system will run BIOS POST and BIOS POST information will redirect to the Remote Admin Console. You can then view the BIOS POST information or enter BIOS setup utility remotely.



ASM6 Remote Windows Console

ASM6 provides the remote windows console function that controls the Windows 2000, Windows Server 2003 systems remotely.

The ASM6 Remote Windows Console Agents running under Windows 2000, and 2003 Server provide the graphic mode console redirection to the ASM Console, using TCP/IP protocols for data transfer. To provide the remote Windows console services, the agents, implemented as an application service in the corresponding Windows environment at the managed server side, redirects the Graphics mode console inputs and outputs to the Remote Windows Console within ASM Console. It allows you to remotely perform operating system based operations and maintenance as if you were sitting in front of the managed system.

To launch ASM6 Remote Windows Console:

Select a system in the Managed System list.

Click **Remote Windows Console** in the Management Function list.

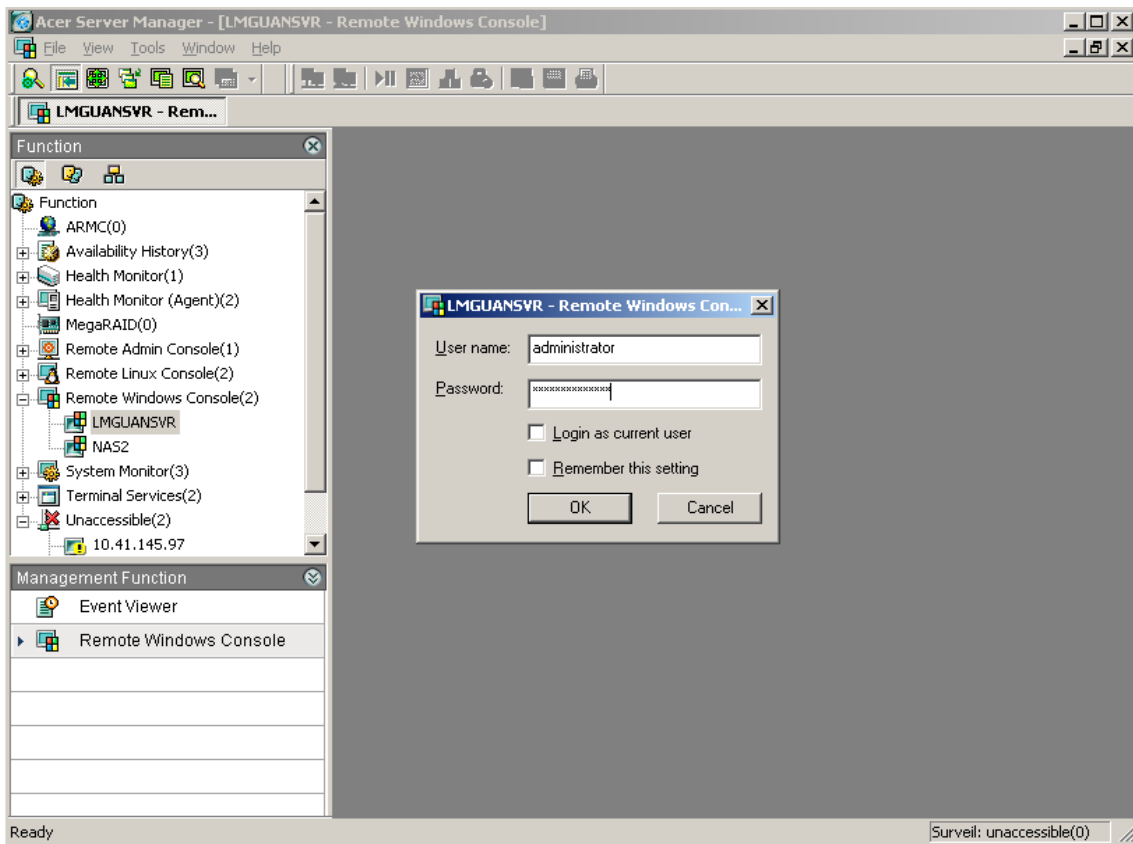
Enter user name and password, as prompted.

- or -

Right-click system name in the Managed System list and then select Remote Windows Console.

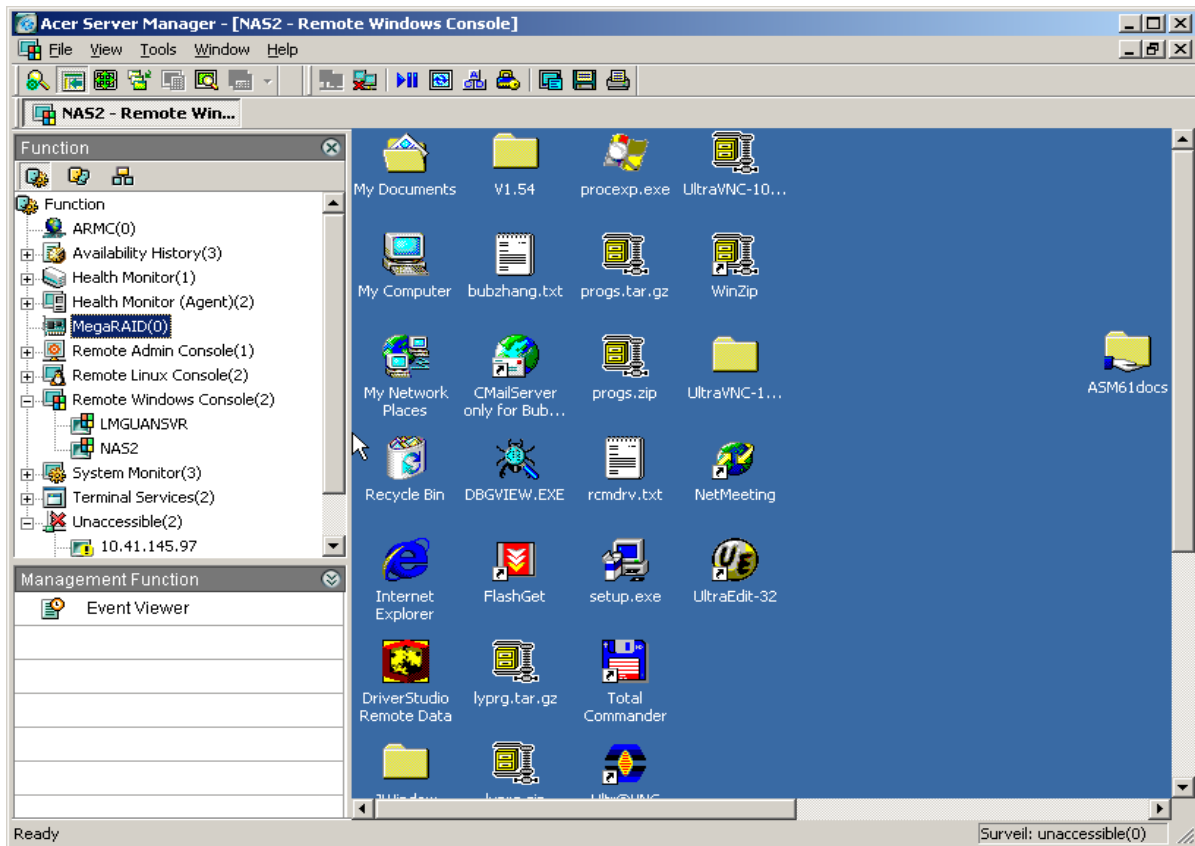
Enter a user name and password. The login account should have administrator privileges (in the system you want to log into or across the domain).

Note: Because of security limitation, users with empty password may not be used to access Windows XP.








6 Remote Management





After you login, the interface is shown as below.



Remote Windows Console toolbar

The Remote Windows Console toolbar will be shown after you log in.

Icon	Description
	Connects to a managed system using the last password. Login as current user: Connects to a managed system agent using the account you used to login to the current operating system.
	Disconnects the selected system agent.
	Pauses/continues the data transmission between the console and the managed system.
	Refreshes the managed system's screen.
	Sends "Ctrl+Alt+Del" to the managed system.

Icon	Description
	Locks/unlocks the managed system's mouse and keyboard.
	Copies the system agent's screen to the clipboard.
	Saves the managed system's screen to a destination folder.
	Prints the managed system's screen.

ASM6 Remote Linux Console

ASM6 also provides Remote Linux Console features to manage Linux servers remotely. The ASM Remote Linux Console Agent provides text mode redirection service to the ASM Console.

To Launch Remote Linux Console:

Select a system in the Managed System list.

Click **Remote Linux Console** in the Management Function list.

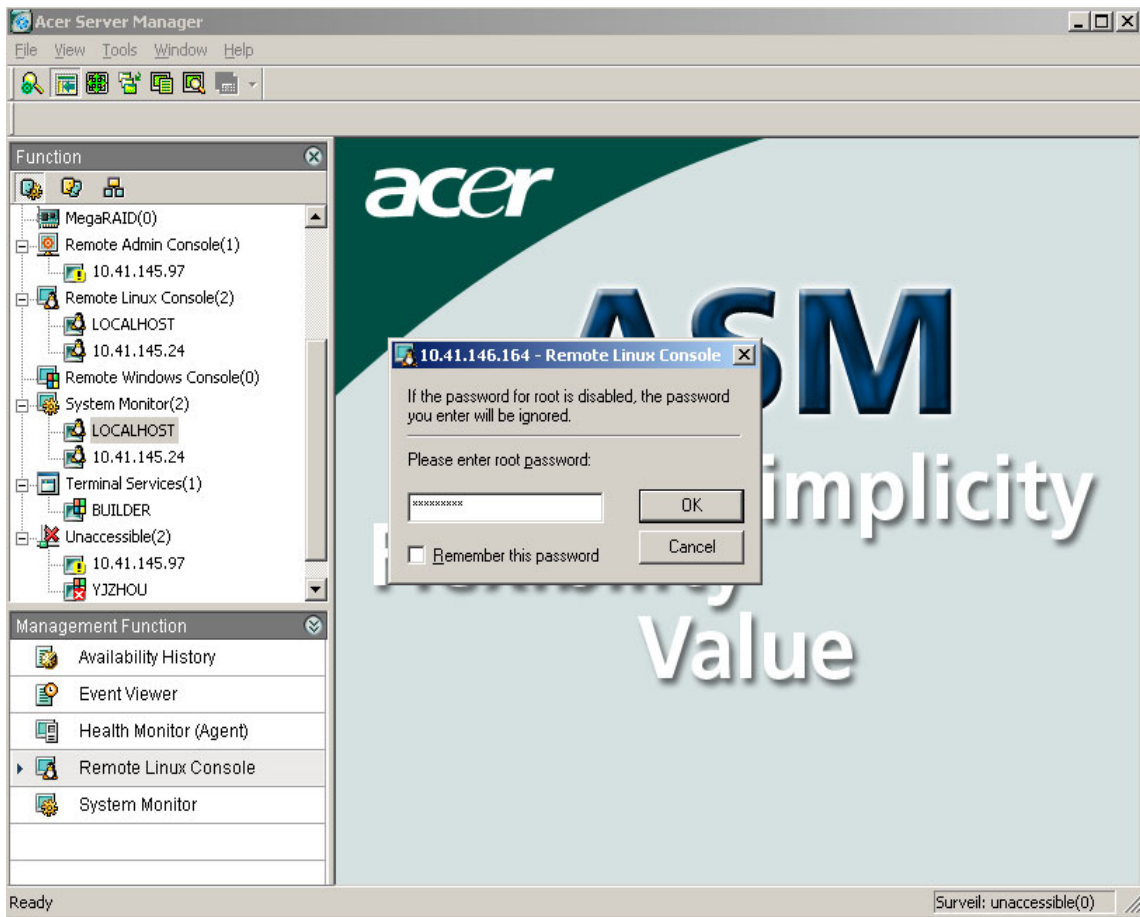
Enter the root password, as prompted.

- or -

Right-click system name in the Managed System list and then select Remote Linux Console, then enter the root

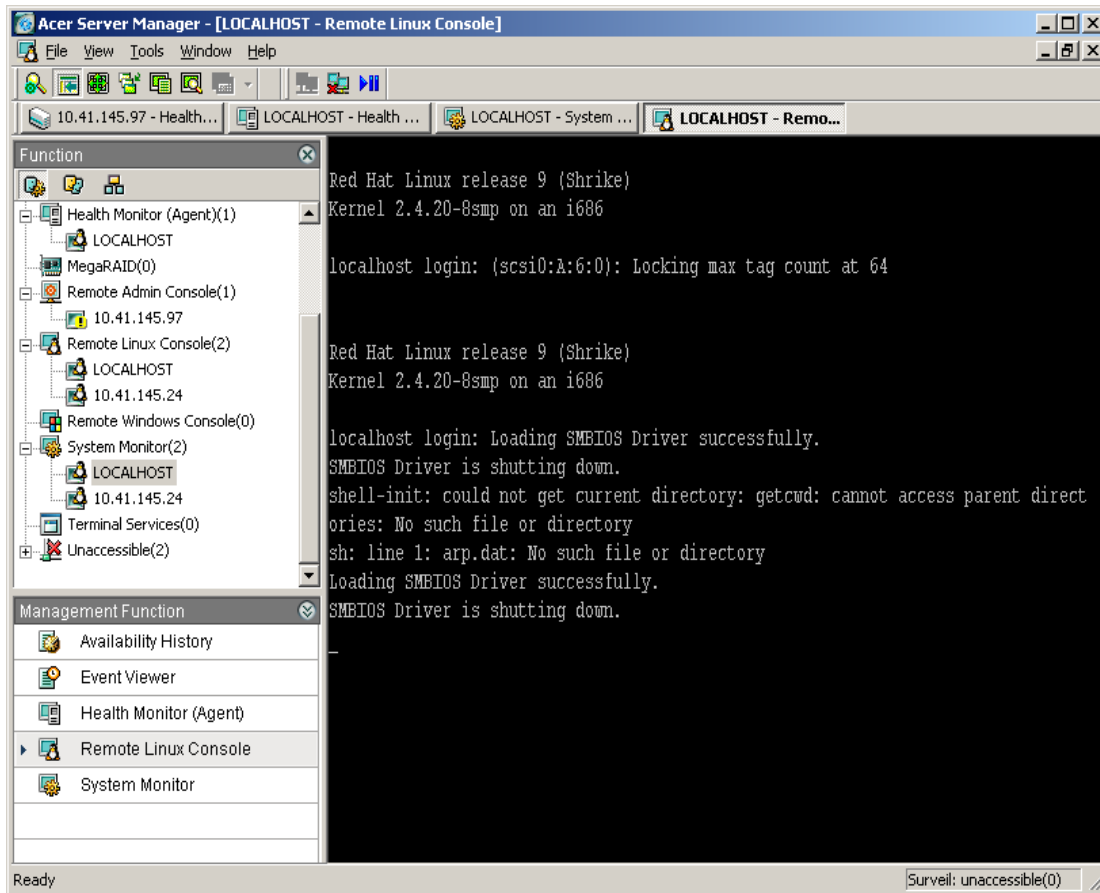
6 Remote Management

password.






6 Remote Management

After you login, the interface is shown as below.



Remote Linux Console toolbar

The Remote Linux Console toolbar will be shown after you log in.

Icon	Description
	Connects to a managed system
	Disconnects the selected system agent
	Pauses/continues the data transmission between the console and the managed system

Using Terminal Services Console

With ASM6 Terminal Services Console you can access a Windows server running Windows Terminal Services and do any of the following:

- **Connect to Remote Terminal Services.**
- **Check the Terminal Services Console number.**
- **Use short-cut keys**
- **Cut and paste from the Remote Terminal Services Client window into an application running locally on the ASM6 Console.**
- **Print to your local printer from applications running on the remote Terminal server.**
- **Disconnect without terminating a session.**
- **Disconnect and terminate a session.**

Connecting to terminal services

To connect to terminal services:

Select a system in the Managed System list.

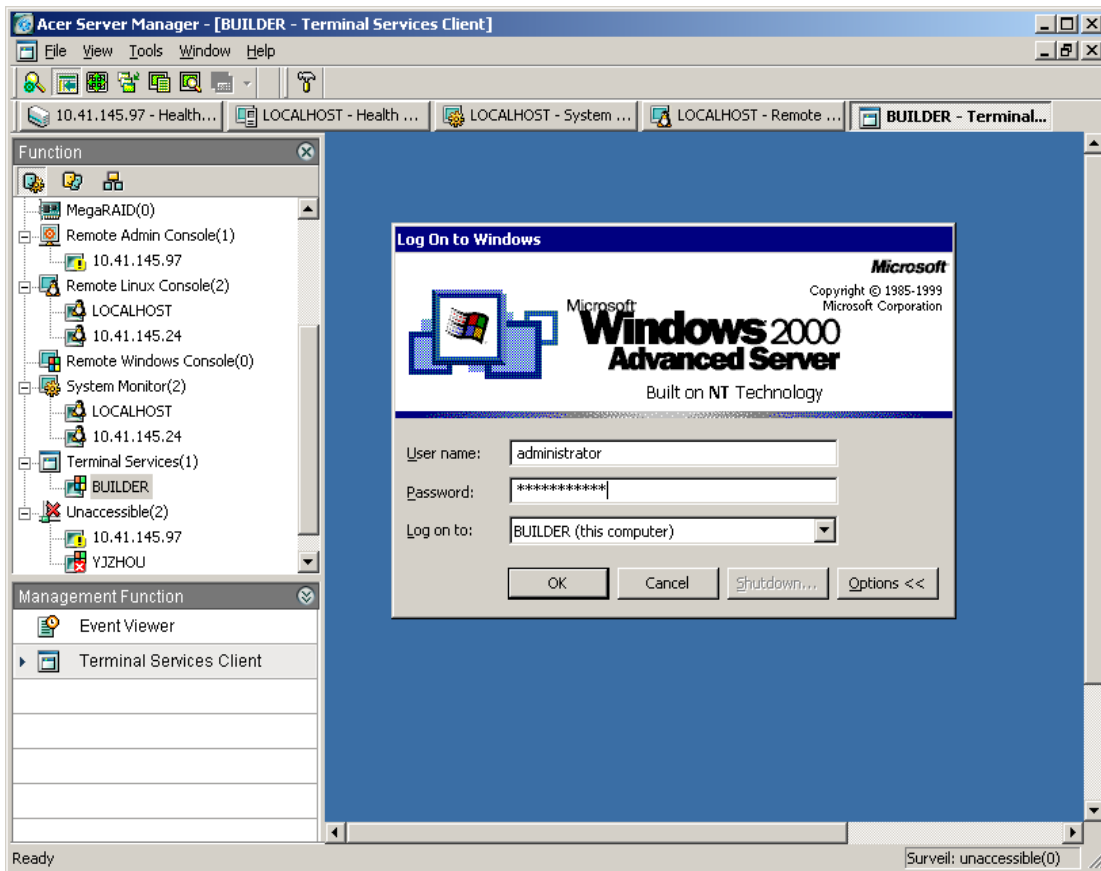
Click **Terminal Services** in the Management Function list.

Enter a user name and password as prompted.

- or -

6 Remote Management

Right-click system name in the Managed System list and then select Terminal Services. Then enter a user name and password, as prompted.

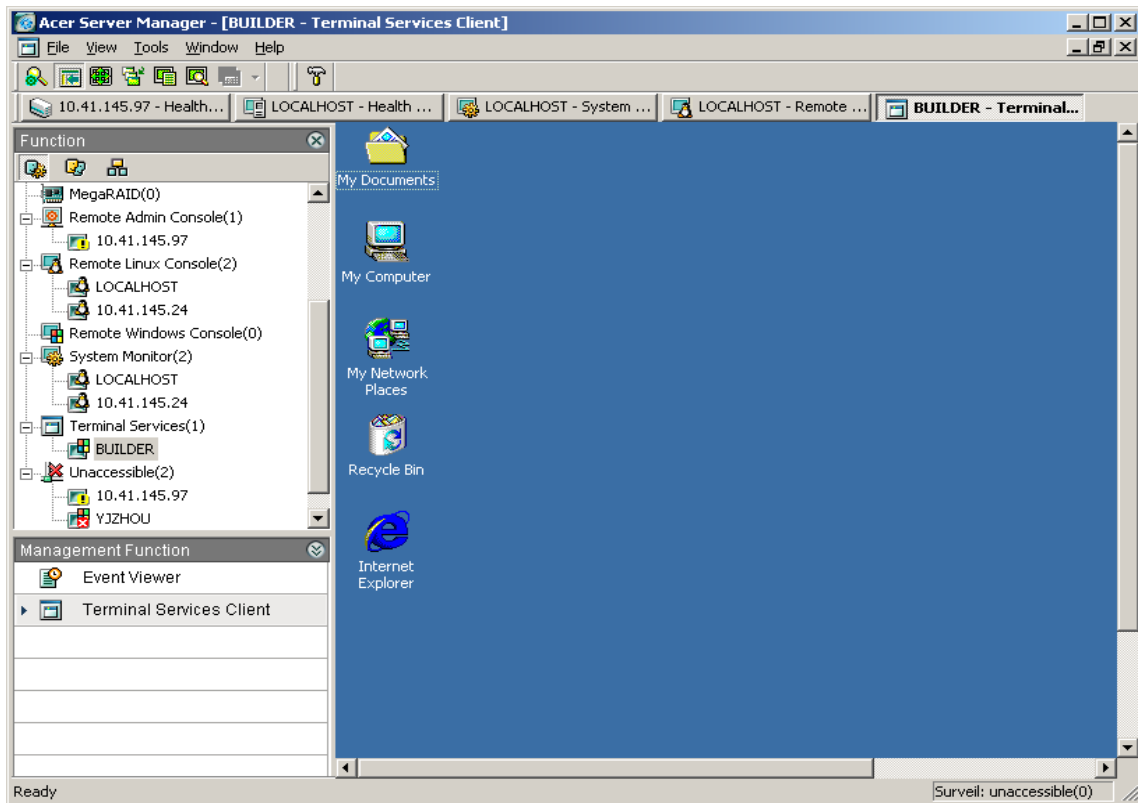


Note: The user name should have administrator privileges.


If you have previously disconnected from a Terminal server without terminating the session, the ASM6 Terminal Services Console reconnects to that session (if the remote server is configured to reconnect disconnected sessions).

6 Remote Management

After you login, the interface is shown as below.



Terminal Services Console toolbar

The  icon will be shown on the toolbar after you log in. Clicking the icon will open a dialog box.

- **Screen Area:** You can change the size of the display area here.

Click **Advance** to expand the dialog box.

- **Start Program:** You can enter the path of a specific program here. The next time you login, the specified program will be launched and shown in the Working Area. Once you close the program, the connection will also be closed.
- **Working Directory:** You can set the working directory for the specified program here.

Using shortcut keys

The following shortcut keys are available from the ASM Terminal Services Console:

CTRL+ALT+END opens the Windows Security dialog box.

ALT+PAGE UP switches between programs from left to right.

ALT+PAGE DOWN switches between programs from right to left.

ALT+INSERT cycles through the programs in the order they were started.

ALT+HOME displays the Start menu.

ALT+DELETE displays the window's pop-up menu.

CTRL+ALT+Minus (“-” symbol on the numeric keypad) places a snapshot of the active window, within the Console, on the Terminal server clipboard (provides the same functionality as **ALT+PrintScrn** on a local computer).

CTRL+ALT+Plus (“+” symbol on the numeric keypad) places a snapshot of the entire Console window area on the Terminal server clipboard (provides the same functionality as **PrintScrn** on a local computer).

Remote Copy, Local Paste

Windows Terminal Services provide seamless clipboard sharing, making clipboard contents available to the local applications on the ASM Console. The contents of the shared clipboard are synchronized with the local clipboard and can be viewed using the Windows Clipbook Viewer (clipbrd.exe). With this capability, you can copy text or graphics from a document or application within the Remote Console window, and paste it into a document on your local computer. The contents of clipboard remain until the Clipboard is cleared or replaced with other information. The content can also be pasted multiple times. You cannot, however, copy or paste files and folders.

Remote Application, Local Printing

Terminal Services also provides printer redirection which routes printing jobs from the remote Terminal server to a printer attached to your local ASM Console. There are two ways to provide access to local printers: automatic and manual printer redirections. Use manual redirection when your local printer (on ASM Console) requires a driver that is not available on the remote Windows 2000 Terminal server.

Automatic printer redirection

Printer redirection is supported in automatic mode when the local printer driver on ASM Console is installed on the remote Windows 2000 Terminal server. When you log on to a remote terminal session on the remote server, any local printers attached to LPT, COM and USB ports of the ASM Console are automatically detected and an equivalent queue is then created on the remote server, and the printer settings and properties are passed over and used on the remote server.

When the ASM Console disconnects or terminates a session, the printer queue on remote server is deleted, and any incomplete or pending print jobs are lost. Information about the local printer and settings are saved on the ASM Console computer only. On subsequent logons, the printer queue is created on the remote server using the information stored in the ASM Console.

If that specific printer driver is not found on the remote server, an event is logged and the ASM Console printer queue is not created on the remote server. To make the printer available, the driver must be manually installed on the remote server.

Manual printer redirection

Printers attached to local LPT and COM ports on the ASM Console can take manually redirected print jobs from remote Terminal service sessions, although this service cannot be supported on USB-connected printers.

To manually redirect a remote print job to an ASM Console printer, connect the ASM6 Console to the remote Terminal server first, and then follow the Windows Terminal server manual printer redirection procedures. After initial manual redirection, local printers on the ASM Console will be automatically redirected during subsequent logons.

Note: When you disconnect or log off from a Terminal session, the printer queue is deleted from the remote server and incomplete and pending print jobs are lost.

Closing Terminal Services Console

You have the option of disconnecting with or without terminating the Terminal session.

Disconnecting without terminating the session allows you to reconnect to this session the next time you reconnect to that remote Terminal server, if the connection is configured to reconnect disconnected sessions. Logging off will terminate the Terminal session, and the next time when you log on, a new Terminal session will be initiated.

7 Frequently Asked Questions

Problems during installation.

In order to install ASM6 smoothly, you need have system administrator or equivalent privileges. In addition, SNMP Service needs to be installed and running when you install ASM6 Agents. To add SNMP Service component into your system, please refer to:

Control Panel | Add/Remove programs | Add/Remove Windows Components | Management and Monitoring Tools | Simple Network Management Protocol

Launching ASM6 console with administrator privilege.

You must be a system administrator or have equivalent privilege to launch ASM6. Only one instance of ASM6 Console can be launched at the same time.

How does ASM6 retrieve server management information?

ASM6 retrieves server management information in three alternative approaches, including ASM6 Agent, Linux / Pegasus instrumentation, and Windows WMI, in this preference and availability order.

What is surveillance?

When ASM Console is running, it polls the status of every managed system, if a managed system becomes inaccessible, a red cross will put over the bottom-right of the managed system's icon. No more action is taken. But if a managed system is under surveillance, ASM Console will generate a "Managed System Unaccessible" event for the managed system when it becomes inaccessible. Administrators can use "Event Rule Setup" to configure which actions to take after receiving such an event.

By default managed systems are not under surveillance. To put a system under surveillance, administrators can right-click the managed system and choose "Surveil." If a managed system is under surveillance, there will be a green check over the top-left of the managed system's icon. To cancel surveillance on a managed system, right-click the managed system and choose "Don't Surveil."

What is an event?

An event is an indication received from a network or a change detected by an ASM Agent. For example, if the disk of a managed system is out of space, it sends out a trap. After ASM receives the trap, it translates the trap to an event and sends the event to registered event consumers, which may cause an application to run, a mail to be sent, etc. Use Event Rule Setup to configure which actions to take when an event is received.

What is MQL in Folder of Function view?

In the ASM Console Managed Object represents a managed system. Managed Objects have lots of properties to attribute the managed systems. For example, the IP property stores the IP address of the managed system; the WMIAvailable property indicates if the WMI service is available on the managed system. MQL is a subset of SQL, which only supports SELECT statement. We can use MQL to define a filter to select a set of managed systems according to a specific criteria. For example,

```
SELECT * FROM IPDevice WHERE WMIAvailable = TRUE;
```

7 Frequently Asked Questions

This statement will select all managed systems which have WMI Service installed and available.

What is a threshold in the System and Health Monitor?

A threshold is a pair of critical points which define a range in which a system behaves well or is in a critical state. When a threshold is passed, it indicates that the monitored system has reached a new (undesirable) state, and alert events will be issued to notify administrators of the change of the state.

Why did the Health Monitor fail to load information from a managed system?

An ASM6 Health Monitor failure may occur as a result of one of the following conditions:

1. The managed system is down without intelligent management processor (BMC) support.
2. Sensor is absent or in error.
3. Health Monitor agent is not installed or is not running correctly.
4. Not enough privilege (i.e. Administrator logon) to log into the managed system.

Why did the System Monitor fail to load information from a managed system?

An ASM6 System Monitor failure may occur as a result of one of the following possible conditions:

1. The managed system is down.
2. System Monitor agent is not installed or not running correctly.
3. Pegasus instrumentation infrastructure is absent.
4. WMI infrastructure is absent.
5. User name / Password is incorrect.

Why did the threshold value in System Monitor fail to load?

You must install System Monitor agent in managed system first.

Why did the System or Health Monitor failed to set the thresholds?

The reasons for a failure to set thresholds include:

1. System / Health Monitor agent is not installed or not running correctly.
2. The value is out of reasonable range.
3. Lack of write privilege on managed system.

Why did the ASM console fail to connect to a remote server?

Correct user name and password (even optional domain) are required for the administrator or root or equivalent privileges.

Why can't the Refresh rate be saved in System / Health Monitor?

The range of refresh rate is (0, 3600). The value out of range can't be saved. Set a value in this range to avoid overloading a managed system

What is ARMC and How do I make it work?

ARMC stands for Acer Remote Management Card. It provides more management features for your server.

In order to make the ARMC manageable from ASM Console, you have to correctly install and configure the plug-in card in your server, and then install ASM Agent. ASM Console will communicate with ASM Agent to detect

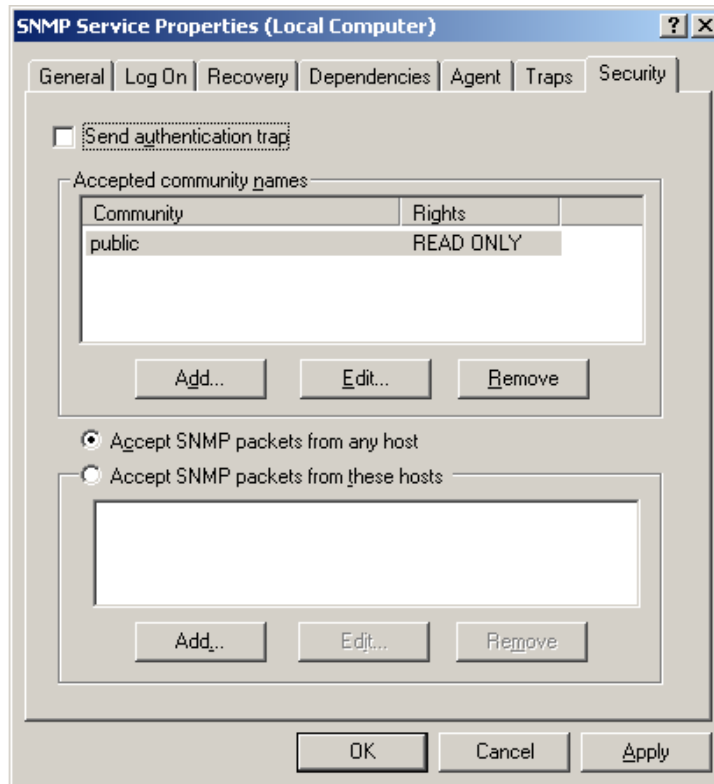
the availability of ARMC and its IP address.

What is MegaRAID and How do I make it work?

MegaRAID is a RAID solution provided by LSI LOGIC Corporation. In order to make the RAID Card manageable from ASM Console, a MegaRAID card should be plugged into the server. The MegaRAID SNMP Agent should be installed too. The MegaRAID SNMP Agent can be installed from Power Console which is included in the "U320 Driver Suite" CD that shipped with the card.

Some management functions, such as System Monitor and Health Monitor (Agent) functions do not show in Function Pane when I select a system running Windows Server 2003.

First, make sure that you have installed ASM Agent in the Windows Server 2003. Second, make sure that the SNMP Service of the server is started and you have properly configured the security settings. By default, Windows Server 2003 rejects any request. To configure the security setting of the SNMP Service, you open the Computer Management, select Services and double click the SNMP Service and choose the Security page:



ASM Console uses "public" community to manage the server by default. So you should create a "public" community with READ ONLY rights for the SNMP Service.

If you choose "Accept SNMP packets from these hosts" option, you should add the computer running ASM Console to the list. Or for simplicity, you can choose "Accept SNMP packets from any host." For security reasons, it is recommended that you specify an ASM console computer.

Some management functions, such as System Monitor, Health Monitor (Agent) and Power Control functions cannot manage a machine running Windows XP Professional.

Power Control function uses WMI to reboot/shutdown a Windows machine. In order to execute the reboot/shutdown method successfully, WMI requires an account with administrative rights in the machine.

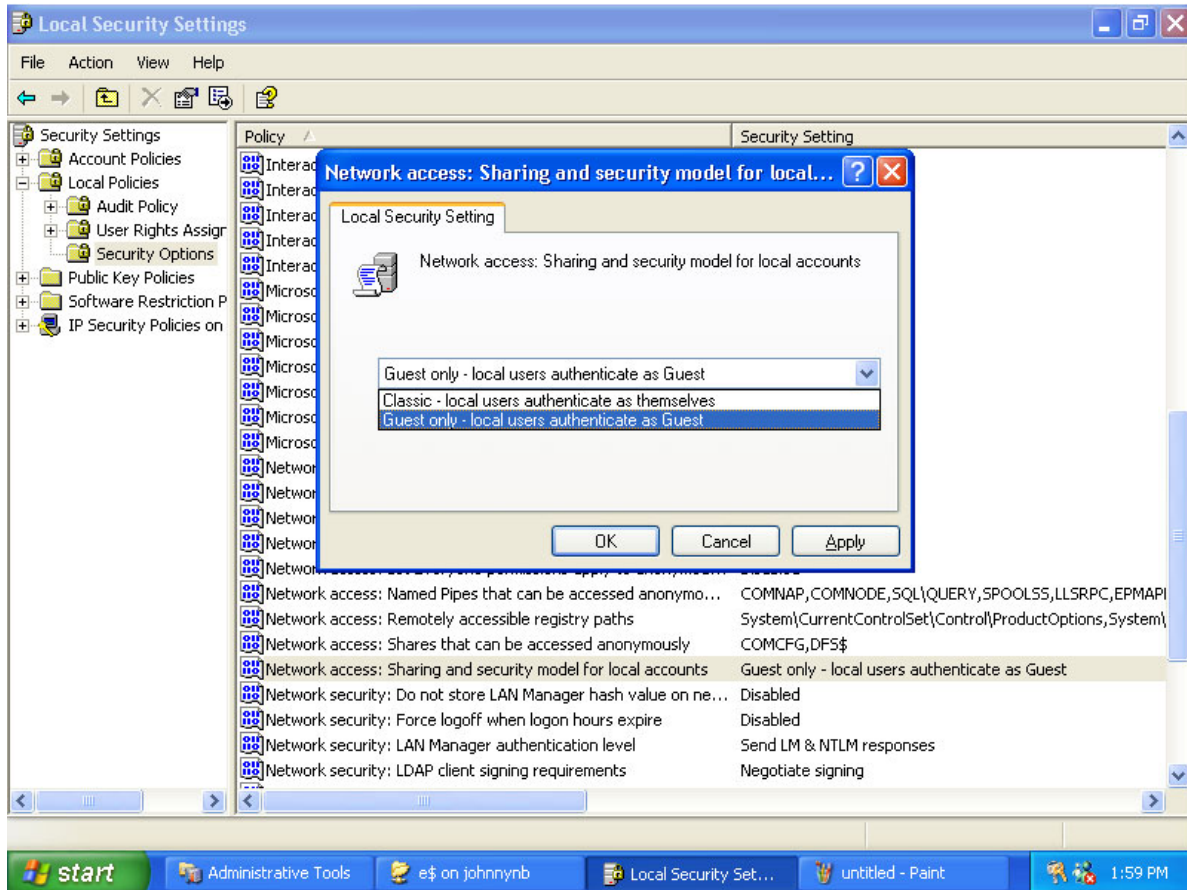
So first make sure that you have provided an administrative account before you reboot/shutdown the machine.

Second, by default the Windows XP Professional's ForceGuest option is enabled, which means any account logged in remotely is considered as the Guest account. While Guest account has no right to reboot/shutdown a machine,

7 Frequently Asked Questions

so whatever account you provide you cannot reboot/shutdown the machine.

When a machine with Windows XP Professional is added to a domain. The system disables the ForceGuest option automatically. To disable the ForceGuest option manually, you can open the Control Panel, Administrative Tools, Local Security Setting, and then choose Local Policies, Security Options:

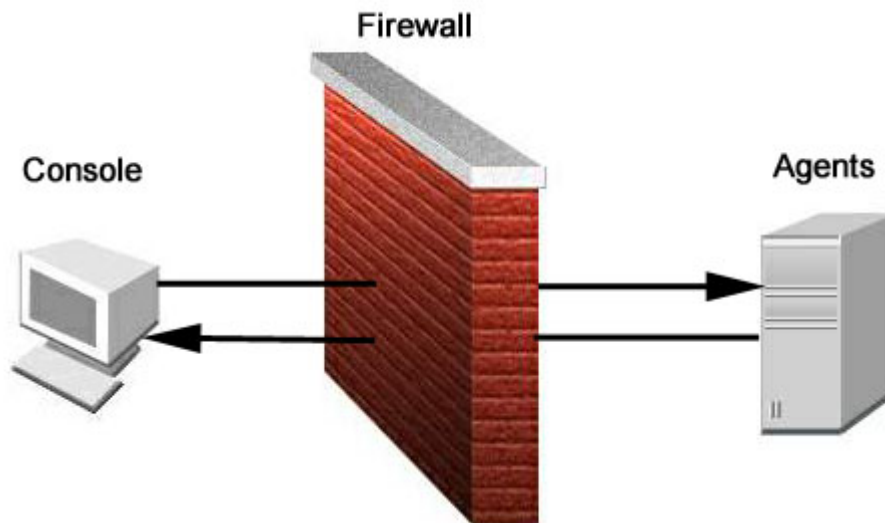


Select the policy: Network Access: Sharing and security model for local accounts. Set it to Classic - local users authenticate as themselves. For more information about ForceGuest Option, please refer to the MSDN article Simple Sharing and ForceGuest at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxp/pro/reskit/prde_ffs_y puh.asp

8 Appendix

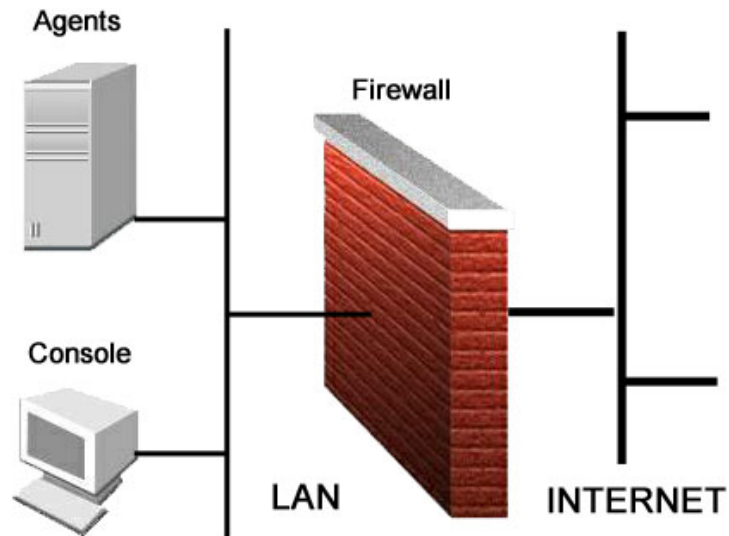
Port List

The ASM Console and Agents use dedicated ports to communicate with each other. If the ASM Console and Agents are not on the same side of the firewall, the correct ports need to be left open for communication. Please refer to the Port List, for the actual ports needed for ASM6.



8 Appendix

It is recommended that the ASM Console and Agents be on the same side of the firewall for more secure server management.



Port Number List:

Item	Port
Remote Window Console	TCP/6100 UDP/6100
Remote Linux Console	TCP/4400 UDP/5500
Pegasus CIM Server	TCP/5988 TCP/5989
RMCP	UDP/623 UDP/664
SNMP	UDP/161
SNMP Trap	UDP/162(Console side)
Terminal Services	TCP/3389

Broadcom's ASF Configuration Utility

Please ensure that you selected Broadcom ASF Management Applications for G510 during Acer Server Manager software installation.

On Windows 2000 OS environment, launch Broadcom's ASF Configuration utility by clicking,

Start | Programs | Broadcom ASF Configuration. In this utility, you can detail ASF configuration and set management console IP etc.

