Installation and User Guide

for

Acer Server Manager Enterprise (ASMe)

Ver. 5.1

Legal Information

Contents

1. Introduction

Acer Server Manager Enterprise (ASMe) is a server management tool implemented with a client-server architecture. This guide explains how to install ASME and use the software to:

- Remotely set up servers
- Automatically monitor server hardware
- Configure alert notices to be sent based on server activity and hardware sensors
- Receive emergency notification and remotely manage servers
- Work together with third-party server management software

Platform Compatibility

The ASMe features depend on which version of ASMe is running on which platform. Compatibility may be an issue when a current version of the ASMe console manages a network of systems that are running older versions of ASMe. For a list of features available in this release, see the Platform Compatibility table beginning on page 63.

New ASMe Features

This release of ASMe includes the following features that were not in ASMe prior to release 5.1:

Feature	See these pages:
Email Alerts	52

Getting the Latest Information and Support

ASMe components are frequently enhanced and updated to support new features and platforms. For updated information on such changes, see the ASMe release note files README.TXT and ERRATA.TXT. Also, refer to the monthly ASMe Specification Update posted on the Web at: http://support.acer.com/

On the web site, under Acer Server Manager Enterprise software, look for Specifications and Errata, then see the ASMe Specification Update.

For technical details about ASMe, see the Technical Product Specification at the same web site location.

If you have questions or need help using ASMe, contact your service representative.

Overview of the Installation Process

For brand new servers with unpartitioned hard drives and no OS installed, the most straightforward way to install the ASMe software is:

On the Server System

1. Install a Service Partition. **(See page 11)**
2. Boot from the Service Partition and use the System Setup Utility (SSU) to configure low-level management capability, such as modem or LAN configuration, passwords, etc. **(See page 13)**
3. Install the OS and set up whatever connections (modem, LAN, etc.) will be used for management communications.
4. Repeat steps 1-3 for each server to be managed.

On the Console and Server Systems

5. Install any third-party enterprise management software **(see page 9)** that ASMe will integrate with. This step is optional.
6. Install ASMe software. For Windows†-based systems, you can install console software and server instrumentation software locally or remotely, either from a console or server system. For other operating systems you will have to take some manual steps on each server during the installation or install ASMe individually on each server system. **(See page 17)**
7. Do OS-specific configuration after the installation. **(See page 19)**
8. Enable the LAN-Alert Viewer if you will use it on console systems. **(See page 23)**

Connecting Consoles to Servers

There are several methods for connecting to a server for management. You can use any combination of the following connections:

- Local Area Network (LAN)
- Analog telephone modem (serial connection)
- Local direct connection through a serial port
- Intelligent Chassis Management Bus (ICMB)

For typical management activities, a LAN is the preferred connection. In some cases where the network is inoperable or the OS is down, or for other emergency access, a modem or direct serial connection can let you manage a server from a console. An ICMB connection allows you to manage servers that are otherwise not supported by ASMe, such as servers running non-supported operating systems.

System Requirements

ASMe contains two parts:

- ASMe Console Software, which runs on one or more client systems, can be installed on these operating systems:
  - — Windows XP Professional
  - — Windows 2000 Advanced Server, Service Pack 2
  - — Windows 2000 Professional, Service Pack 2
- ASMe Server Instrumentation Software, which is installed on the servers to be managed, can run on these operating systems:
  - — Windows 2000 Server, Service Pack 2

Support for SNMP-Based Third-Party Server Management Software

ASMe can run from its own ASMe Console or can integrate into one of the following SNMP-based third-party management consoles:

- H-P OpenView† Network Node Manager 6.2 for Windows
- Computer Associates (CA) Unicenter The Next Generation† (TNG) 3.0 for Windows

The default ASMe installation incorporates the integration software for these tools. In a custom installation, you can select the appropriate checkbox for integrating H-P OpenView Agent or CA Unicenter Agent.

Simple Network Management Protocol (SNMP) support must be installed to use one of these supported third-party management consoles. For SNMP configuration information, see your Windows documentation.

On the console system(s), when configuring SNMP you must integrate MIB files into the SNMP management consoles (see page 20). SNMP services must also be installed and configured on the console system to enable Platform Event Traps used for ASMe LAN Alerts (see page 23).

The requirements for the console system may be different than those listed below if you use one of these third-party management applications. Please refer to their installation requirements for more information.

Console OS and Minimum Hardware Requirements

ASMe supports these platforms to be used as a console (client) system. Also, any of the supported servers can act as clients.

- Windows 2000 Advanced Server or Professional (Service Pack 2) or Windows XP Professional
- Intel® Pentium® microprocessor, Intel® Celeron® microprocessor, or higher
- At least 64 MB of RAM
- At least 120 MB of available disk space for the entire set of software
- Microsoft Windows-compatible modem must be used if you connect to servers by modem

Managed Server Requirements

ASMe supports several Acer baseboards. For a complete list of supported server baseboards and qualified BIOS revision levels, see the files README.TXT and ERRATA.TXT. You can find these files in the appropriate language directory of the ISM\Docs directory on the installation CD.

For any server you need a login account with root or supervisory privileges. The following requirements must be met for a managed server, depending on the OS.

Windows Server Requirements

- Windows 2000 Advanced Server (Service Pack 2)
- 64 MB of RAM
- 120 MB of available disk space
- Windows SNMP service is required for connectivity with an SNMP-based third-party management console or to enable LAN Alerts (see pages 20 and 23

2. Installation Steps

Step 1. Install the Service Partition on Servers

The service partition is a special hard disk partition that you establish when you initially set up the server system. It contains utilities such as the System Setup Utility (SSU) and other software required for remote management. The service partition is not marked as an active partition and the server will only boot from it by a special request. It is not normally visible to the server user because it has a special non-standard partition type that does not appear as an accessible file system to the operating system. However, low-level disk utilities may see the partition entry as an EISA partition, and recognize its space.

The utilities on the service partition can be run locally or remotely. In either case, the server must first boot from the service partition. Remote execution is available from ASMe using either:

- Direct Platform Control (DPC) Console Manager
- Client System Setup Utility (CSSU), which is a remote or client interface to the SSU

Service Partition Requirements

For a new service partition you must install only as follows:

- On a clean hard drive with no partitions defined
- Before installing any operating system

NOTE

Installing the service partition on a partitioned drive is not recommended because some operating systems may no longer boot if partitions are added or removed after the OS has been installed. You can add a low capacity hard drive for the service partition.

Additional requirements:

- At least 40 MB of unused (not partitioned) hard drive space is required. Hard drives greater than 8 GB must be unpartitioned.
- The service partition can be on any of the first 4 BIOS-supported physical hard drives.
- Service partition hard drives must support BIOS INT13 and INT15.
- The current BIOS must be installed on the baseboard.

Installing the Service Partition

⚠ CAUTION

To prevent data loss, do not attempt to run the installation utility from any device other than the System CD.

Installing the Service Partition

1. Boot the server from the System CD of EasyBUILD v5.1. Assuming the system can boot from a CD, proceed to step 2. If the system won't boot from a CD, do the following:
   a. Insert the CD into the CD drive.
   b. Restart the server.
   c. When the “F2 to enter setup” message appears, quickly press F2 to enter BIOS Setup.
   d. While in BIOS Setup, disable any system features (such as virus protection) that would prevent writing to the hard drive boot sector.
   e. In Setup, select the menu to set Boot devices and configure ATAPI CDROM as the first (highest priority) boot device. Ensure that the boot sequence of your server is configured as
      - Floppy drive A:
      - IDE CD-ROM
      - Hard Disc C:
   f. Press F10.
   g. Select Yes to confirm saving of the current settings and press Enter. The server restarts and boots from the CD.
2. Follow the screen hint, entering installation information . If you select installing Redhat 7.3, you will find “Create Service partition(40 MB)” option in “Partition information” Page; If you select installing Windows 2000, you will find “Create Service partition(40 MB)” option in “Storage” Page. Ensure the check box of “Create Service partition(40 MB)” option is selected. More about SystemCD installation procedure ,please click on Help icon of EasyBUILD or ‘ Help.htm’ in System CD root directory for detail.
3. Before reboot for installing OS, there are two Installation Diskette will be created. The second created diskette is the Service partition Installation Diskette.
4. After finishing creating two diskettes, you should keep the Service partition Instatllation Diskette(disk #2) in floppy drive and remove the System CD from CD-ROM drive while rebooting.
5. Boot from Service partition Installation Diskette(disk #2) and begin to create service partition automatically.
6. When you see the information “Service partition has been created successfully!”, you should replace floppy with OS installation diskette (disk #1) and press enter.
7. You have finished and left installation procedure.

Step 2. Boot the Service Partition, Configure the Server

To run the utilities (such as SSU) that are now installed on the service partition, boot the server from the service partition. You can reboot a server locally to run the SSU directly and configure the server for management. Later, after ASMe software is installed on both console and server systems, you can also boot from the service partition remotely, using the DPC Console Manager or Client SSU. Those ASMe components are described later in this manual.

The configuration process involves these steps, described in the following sections:

1. Boot the server from the Service Partition.
2. Run the System Setup Utility (SSU).
3. If you will access the server over a serial port from the console system (direct connection or modem), configure the Emergency Management Port (EMP) using the SSU (see page 14).
4. If you will access the server over the LAN from the console system, configure the LAN control elements of the Baseboard Management Controller (BMC) using the SSU (see page 15).
5. Configure BIOS event logging using the BIOS Setup, to enable management activities (see page 16).
6. When using third-party management software which requires SNMP (see page 9), install the third-party software and configure SNMP before installing ASMe (page 17).

Locally Booting the Server from the Service Partition

Recent server platforms include a BIOS option to let you directly boot the Service Partition at startup, using the <F4> key. If your platform does not have this feature, you can boot the Service Partition by making a change in BIOS Setup.

1. Restart the server.
2. If you see a message like "press F2 to enter Setup, press F4 to boot the Service Partition", simply press F4. Ignore the following steps. Proceed to the following section to run the SSU.
3. If there is no option to boot the Service Partition directly, when the “F2 to enter Setup” message appears, quickly press F2 to enter Setup.
4. In Setup, use the arrow keys to select the Server menu.
5. Select Service Boot and press Enter.
6. Choose Enabled and press Enter. The Service Boot option resets to Disabled after the next system boot.
7. Press F10.
8. Select Yes to confirm saving of the current settings and press Enter. The server restarts and boots the service partition.

How to Run SSU

There are several ways to run the System Setup Utility (SSU). Choose one of the following:

A. When you boot locally from the service partition you receive a DOS prompt. Enter the commands:
   cd \ssu
   ssu

B. You can remotely run SSU from the client console using the Direct Platform Control (DPC) component of ASMe. (DPC is described later in this manual.) To reboot to the service partition and access SSU from DPC, first connect to the appropriate server, then in the Action menu select Reboot to Service Partition. In the Service Partition menu that subsequently appears, select Run Program. Then either select SSU or enter the command line SSU.

C. You can remotely run the SSU interface from the client console using the Client SSU (CSSU) component of ASMe. (CSSU is described later in this manual.) To reboot to the service partition and run SSU, Select (Re)Connect from the Server menu in CSSU.

Configuring the Server for EMP Access

This step is optional and only needed if you intend to use a direct serial or modem connection to the server. For these serial connections, the Emergency Management Port (EMP) and console redirection settings must be configured using the SSU.

1. Run the SSU using one of the methods described earlier.
2. In the Available Tasks list select Platform Event Manager and click OK.
3. Click the Configure EMP button.
4. Enter the following in the Emergency Management Port (EMP) dialog box:

Option	Entry
Enter New Password:	Enter the EMP password (if required), up to 16 characters.
Verify New Password:	Re-enter the EMP password (if required).
ESC Sequence:	+++ (default)
Hangup String:	ATH (default)
Modem Dial Command:	ATD (default) may need to change depending on requirements of installed modem.
Modem Ring Time:	63 (default) This is the number of 500 ms increments during which the BMC will monitor the Ring Indicator (RI) signal from the serial connector and will claim the serial connection after a ring is detected. The value 0 means the BMC will switch the multiplexor immediately on the first detected transition of RI. The value 63 (the maximum value allowed) means that the BMC will ignore the RI signal. You must set this value to 0 in order to connect using a modem if the EMP Access Mode is set to Preboot. If the Ring Time is not set to 0, the modem will not answer.

Modem Init String:	ATE1Q0V1X4&D0S0=0 (default). May require change based on the installed modem requirements.
System Phone Number:	The phone number to call when using a modem to access the EMP port.
Access Mode:	Always Active (default is Preboot).
Restricted Mode:	Disable (default is Enable).
Connection Mode:	Modem Connect (default) for modem connections to COM2. Direct Connect for serial connections to COM2.

5. Click Save, then Close.
6. Exit from the SSU.
7. Quit the menu.
8. Reboot the server.

Configuring the Server for LAN Access

To take advantage of LAN access and BMC LAN-Alert features, server settings must be configured using the SSU. After the settings are initialized they can be changed remotely with CSSU.

⟹ NOTE

If you enable LAN Alerts, you will need to install SNMP and configure the SNMP community when you install the OS, before installing ASMe.

1. Run the SSU using one of the methods described earlier.
2. In the Available Tasks list select Platform Event Manager and click OK.
3. Click the Configure LAN button.
4. Enter the following settings in the BMC LAN Configuration dialog box:

Option	Entry
Enable LAN Alerts:	Click to enable BMC LAN-alerts (optional).
Enter New Password:	Enter the BMC LAN Configuration password, up to 16 characters (optional). Default is NULL. This will be used for all LAN connections in CSSU, DPC, PIC, and BMC LAN-Alerts.
Verify New Password:	Re-enter the BMC LAN Configuration password (if one is set).
LAN Access Mode:	Always Available, which allows DPC and CSSU access via LAN. (By default, LAN access is Disabled.)
SNMP Community String:	Public (the default) unless there is a predefined SNMP host to receive SNMP traps from BMC LAN-Alerts. Must be from 5 to 16 characters and the string "public" must be all lowercase characters.
IP Configuration:	Static (default) unless you are using DHCP for IP hosting, then select DHCP.
Host IP Address:	Enter the IP address of the server if you are not using DHCP.
Gateway IP Address:	Enter the IP address of the router/gateway if you are not using DHCP.
Subnet Mask:	Enter the subnet mask of the hosts on the subnet if you are not using DHCP.
Alert IP Address:	Enter the IP address of the console that will receive SNMP traps for the community defined with the SNMP Community String. Enter 0.0.0.0 (default) if a community is not defined.

5. From the Configure LAN Alerts pull-down menu, select the LAN Alert items to be monitored. After making the selections, click OK, then Close.
6. Click Save, then Close.
7. Exit from the SSU.
8. Quit the menu.
9. Reboot the server.

Configuring Event Logging on Managed Servers

ASMe uses the event-logging feature of the BIOS for system management status and information. To enable this feature for each server to be managed with ASMe, run the BIOS Setup and set the appropriate System Event Log (SEL) options.

For more information about the SSU interface, see the system Product Guide for your servers.

Step 3. Prepare for ASMe Installation

On a new server, after SSU configuration is complete, perform these steps before installing ASMe:

1. Install the OS of your choice (see the list of supported server operating systems on page 10).
2. Complete any OS configuration of the links between the client console and the server systems, such as modems, LAN connections, etc. To use a serial link, you will need a null-modem cable. For a modem or serial link, you must configure a serial connection on both the managed server and the client workstation. For emergency communications with an unpowered server, the server's modem must remain powered on.
3. If you will use LAN Alerts (see page 23) or a third-party management software package, install and configure SNMP. For SNMP installation information, see the documentation specific to your OS.
   For Windows 2000 systems, install SNMP as follows:
   a. Open the Control panel and select the Add/Remove Programs applet.
   b. Click on the Add/Remove Windows Components icon.
   c. Click the Management and Monitoring Tools checkbox and then the Next button.
   On the managed servers, specify these items when configuring SNMP:
   d. Community string names for SNMP Get and Set operations.
   e. Community string names for sending traps.
   f. The trap destination (IP address or name) of the client system that will run the third-party management console, as the recipient of the traps.
4. Install and configure any third-party management software package you will use (this item is optional, see page 9).
5. Follow the preparation steps in the following sections for your specific operating systems.

Windows

Before upgrading to this version of ASMe, the system BIOS must be upgraded to the latest version.

Simple File Sharing on Windows XP Consoles

By default, Windows XP systems enable Simple File Sharing. If you attempt to remotely install ASMe to a Windows XP system, the installation will fail if both the following conditions are true:

- Simple File Sharing is enabled and
- The remote system is not part of a DOMAIN

To avoid an installation failure, you can install ASMe locally instead of remotely, disable the Simple File Sharing capability on the remote system, or make sure the remote system is part of a DOMAIN.

Linux, NetWare, OpenUnix

ASMe for Linux, NetWare, and OpenUnix are not supported on version 5.1 release.

Step 4. Install ASMe

The ASMe package contains both console and server instrumentation software. The default installation always attempts to install both console and server parts of the software if it detects that the system is a valid server (it contains a baseboard management controller chip, or BMC, etc.). If the system is not determined to be a server, only the console parts of the software are installed. When installing from a Windows-based system, you can specify automatic remote installation over the network to other systems that run supported Windows.

Installation for Windows Consoles and Windows Servers

Before starting, verify that H-P OpenView is not running.

Use the instructions below to install remotely to Windows servers.

1. On a Windows console system, run the ASMe file SETUP.EXE, either from the ASMe CD or as downloaded and unzipped from the web. On the CD, the Setup file is located in the \ISM\Software directory. To automatically run the Setup file from the CD:
   a. Insert the CD in the drive and it automatically runs, opening a browser window.
   b. Click on Install Acer Server Manager Enterprise.
   c. Complete the registration form and click on Submit. The ASMe installation package runs automatically.

Dialogs and Prompts During the Installation

- If prompted whether to run the program from its current location or download to disk, select running from its current location (the CD) and click OK.
- If you receive a Security Warning asking whether you want to install and run SETUP.EXE from the CD, click Yes.
- You receive a prompt to select Local Install, Multiple System Install, or Custom Install. Select one and click Next, then read and accept the License Agreement.
  — Local Install will automatically select your local system and install all ASMe components.
  — Multiple System Install will prompt for systems on the network which you can add to the installation, including the local system. It will install all ASMe components on all systems that you add to the list. As you specify each server, a dialog prompts you for a login. Connect as a user with supervisor rights for each Windows server. Otherwise the ASMe installation will fail on that server. Select all the servers to be installed and follow the instruction on the screen to continue.
  — Custom Install allows you to choose the parts of ASMe to install (for an overview of the ASMe components, see page 22). On this screen you can also select the support software that integrates ASMe with H-P OpenView and/or CA Unicenter TNG. After selecting the software components, select multiple systems on which to install as described above.
- The installation automatically reboots the local system and reboots remote Windows servers twice.

When installation is complete, view the file logfile.log in the installation directory of each system to verify that ASMe installed correctly. The default installation directory for Windows is Program Files\Acer\ASMe. You might have specified a different directory during installation.

Step 5. Configure Servers After the Installation

SNMP Installation

For the DMI-SNMP Translator to work correctly (see page 19) the SNMP agent on the managed server OS must be configured correctly. For example, the SNMP agents need some configuration to enable the server to send SNMP traps to specific SNMP management consoles. To configure the SNMP agent on each server, see the documentation supplied by the OS vendor.

On the managed servers, specify these items when configuring SNMP:

- Community string names for SNMP Get and Set operations.
- Community string names for sending traps.
- The trap destination (IP address or name) of the client system that will run the third-party management console, as the recipient of the traps.

Customizing Windows Servers After Setup

The set action of some SNMP attributes causes the server to shutdown/power off. To globally disallow all set requests:

1. Change the `ReadOnly` entry in the *%ISCPATH%\bin\sdlink.cfg* file to `True`.
2. Reboot the server.

Step 6. Configure Console Systems After the Installation

Configure SNMP for LanAlert Viewer

If you will use the LanAlert Viewer to receive alerts on a Windows console, you will need to enable SNMP services on that console system (see page 23 for information about LAN Alerts). Verify that "SNMP Service" and "SNMP Trap Service" are running on the console system. If they are not, install these services using the Windows installation CD. This lets you receive special SNMP traps as generated by the server firmware that will report on changes in server health or condition.

For information about the format of SNMP traps used by LanAlert, see the ASMe Technical Product Specification.

Load MIB Files for SNMP Integration

ASMe includes MIB files as listed below for support of server software and hardware, including onboard third-party controllers. The third-party MIB files are specific to onboard controllers and may not apply to add-in cards.

- BASEBRD4.MIB
- CIO400I.MIB: (Adaptec† SCSI)
- FTDMISVCI.MIBL (Promise† IDE)
- ICMBFEAT.MIB
- NI_NICI.MIB: (Intel® LAN Adapter)
- LRA.MIB
- RMTCHAS.MIB
- SHA.MIB
- SYMBIOS4.MIB: (LSI Logic)

You must load the MIB files into your third-party management tool (H-P OpenView or CA Unicenter TNG). Each tool provides a menu or other way to load MIB files. For more information about loading MIB files, see the documentation supplied with your management software.

MIB files are installed during the PIC installation on the console and server. The files are copied to the %PIC_PATH%\SNMPMIBS directory during installation. PIC_PATH is the installation directory chosen during installation.

Incorporating the MIB files on the client system enables the management console to receive traps generated by the ASMe DMI-SNMP Translator, which operates on server systems. MIB files also allow the management software to access the DMI database on the server. DMI events (indications generated by the component instrumentation when a threshold is crossed or a sensor changes state) are translated into enterprise-specific SNMP traps.

Uninstalling ASMe

Windows Systems

To uninstall ASMe itself or components of ASMe, run the setup.exe file as described on page 18. One of the dialogs presents you with the choice of installing or uninstalling the software. Select the uninstall option. You can uninstall ASMe from Windows servers either locally (one at a time) or remotely from a Windows console system.

3. Acer Server Manager Enterprise (ASMe) Concepts

ASMe Components

ASMe includes the following server management tools:

Acer Server Manager Enterprise Console: The ASMe Console provides basic server management functions. It lets you discover servers that have ASMe installed, and allows you to run Platform Instrumentation Control (PIC), Direct Platform Control (DPC), DMI Explorer, and Client System Setup Utility (CSSU).

See page 24 for more information on the ASMe Console.

Platform Instrumentation Control (PIC): PIC is the main administrative access for configuring alerts and monitoring the state of servers when the server operating system is running and the server is on the network. It monitors platform sensors and manages alerts based on events that you can configure. PIC communicates over the LAN to the Platform Instrumentation (PI) software on the server, using standard DMI/RPC protocols.

For detailed information on using the PIC, see Chapter 4 or click the Help button in the PIC Console.

Direct Platform Control (DPC): DPC gives you emergency access to restart and reconfigure a server. It provides access to a remote server when it is on or off the network, when the operating system is hung, or when it's powered off. When you receive notice that a server has malfunctioned (the alert might come from a numeric page or LAN broadcast, for example), you can use DPC to investigate the cause of the alert, to initiate corrective action, and to restart the server into normal operation. You can also run other utilities on the service partition.

DPC communicates either with the serial Emergency Management Port (EMP), which is a serial port for modem or direct link, or over the LAN using the onboard NIC(s) on the server.

For more information on using DPC, see Chapter 5 or click the Help button in the DPC console.

Client System Setup Utility (CSSU): CSSU is a remote interface to the SSU (described on page 14). Use CSSU for low-level configuration and updates. It communicates over a channel opened by DPC.

For more information on using CSSU, see Chapter 6 or click the Help button in the Client SSU program.

DMI Explorer: DMI Explorer is an interface in the ASMe Console that lets you discover servers on the network. It is automatically installed with the ASMe Console. In addition to discovering servers, it shows attribute values for each DMI-compliant component, and you can use it to manage third-party DMI-compliant components.

LAN-Alert Viewer: The LAN-Alert Viewer receives alerts over a LAN connection, as opposed to numeric pages which are sent over a serial connection. The LAN-Alert Viewer runs on the client system to monitor alerts.

Setting Up and Using Alerts

As system administrator, there are several ways you can be notified of a server event requiring your attention:

- LAN Alerts provide a means of notification over the network to the console system.
- Platform Event Paging is a service that notifies a numeric pager.
- Email Alerting sends a notice to specified email IDs.

LAN Alerts

The LAN Alert software can alert you of system failures and state changes regardless of the state of the server's operating system or the server's management software. LAN Alert works with the Baseboard Management Controller (BMC) to create SNMP traps and send them out over the LAN using a UDP/IP protocol. On the client system, LanAlert Viewer senses and decodes these traps and displays the results.

The LanAlert Viewer displays information about the Server IP address and sensor and event data related to the alert. You can use the LanAlert Viewer to:

- Configure different notification and viewer options
- View detailed information about an alert
- Respond to an alert by acknowledging or deleting it from the list
- View the platform GUID

You can configure LanAlert to detect:

- Temperature or voltage sensors out of range
- Fan failures
- Chassis intrusion (security violation)
- Power supply faults
- Uncorrectable ECC memory errors
- POST error codes or boot failures
- Watchdog Timer reset, power down, or power cycle
- System reboot

On the server you use SSU to configure:

- The trap destination as a specific IP address or an address of a specific IP subnet
- The Host IP configuration data such as the IP address, default gateway, and subnet mask
- Filters for alert events

For more information about using LAN Alerts, see the LanAlert Viewer Help system.

Platform Event Paging (PEP)

Platform Event Paging lets the managed server send an alert for notification of critical system failures and state changes, independent of the state of the operating system or server management software. Platform Event Paging uses an external modem to send a message to a numeric paging service. When notified by a page, you can use ASMe tools to remotely view server health and status, system logs, etc., or to configure or reset the server.

Platform Event Paging can generate pages during pre-boot and post-boot states—the only requirements are that the server is using a modem on the COM2 serial port and the Baseboard Management Controller (BMC) is functional.

To configure the paging string and event filters, use PIC or CSSU on the console, or use SSU on the managed server. The paging string includes all the information to connect to the pager as well as the message to send. Paging is one of the alert actions you can configure in the PIC.

Paging alerts can be configured for the same events as supported by LanAlert (page 23).

Email Alerts

You can use the PIC to configure an email address to receive alerts for any of the same events as supported by LAN-Alert and Platform Event Paging. Unlike the other two alert methods, you cannot configure email alerting with the CSSU or SSU. (For more information see page 52.)

Launching ASMe Tools

ASMe tools can be launched from the ASMe standalone console or can be used to manage servers from a third-party management console. Supported management consoles provide automatic discovery of servers, server security, and LAN-based and/or phone-page alerts. They may also include performance monitoring, load balancing, optimization, report generation and traffic analysis.

Supported third-party management software includes:

- H-P OpenView Network Node Manager
- Computer Associates (CA) Unicenter TNG

After launching ASMe tools from one of these management consoles, the management console application can terminate, and ASMe will continue to operate normally.

ASMe Console

Use the ASMe Console to manage ASMe-enabled servers without installing a third-party system management application. To launch the ASMe Console:

1. Click Start, and select Programs.
2. Select Acer Server Manager Enterprise, and then click on ASMe Console.

H-P OpenView Network Node Manager

The H-P OpenView Network Node Manager Console automatically detects servers running ASMe server instrumentation software, including interfaces for PIC, DPC, DMI Explorer and CSSU. ASMe-enabled servers display as nodes on the network map. To launch ASMe, select an ASMe-enabled server on the H-P Console network map, click the right mouse button, and select “Acer Server Manager Enterprise” from the popup menu.

To launch a particular ASMe tool, for example, PIC, after selecting an ASMe-enabled server, you can select the "Platform Instrumentation Control Applet" option from the Tools Menu. Alternatively, you can launch PIC by selecting an ASMe-enabled server on network map, clicking the right mouse button, selecting “Launch ASMe” and then selecting the "Acer, Platform Instrumentation Control" option from the popup menu.

CA Unicenter TNG

The CA Unicenter TNG Console automatically detects servers running ASMe server instrumentation software, including interfaces for PIC, DPC, DMI Explorer and CSSU, if the ASMe to CA discovery service is enabled. It should automatically be enabled after ASMe installation. To enable discovery manually, start the “Acer Tng-ASMe AutoDiscovery” service from the TNG Unicenter “Auto Discovery” dialog.

The discovery service creates a new “Acer Server Manager Enterprise” object for each server with ASMe-instrumentation software installed. The ASMe objects display under “ASMe World View.” When you double-click the ASMe World View icon, a pane opens that displays the ASMe Server icons. To launch an ASMe tool like PIC, right-click on an “Acer Server Manager Enterprise” icon, and select the “Launch ASMe” option from the popup menu. On the following popup menu, select “Acer Platform Instrumentation Control” to launch the PIC application.

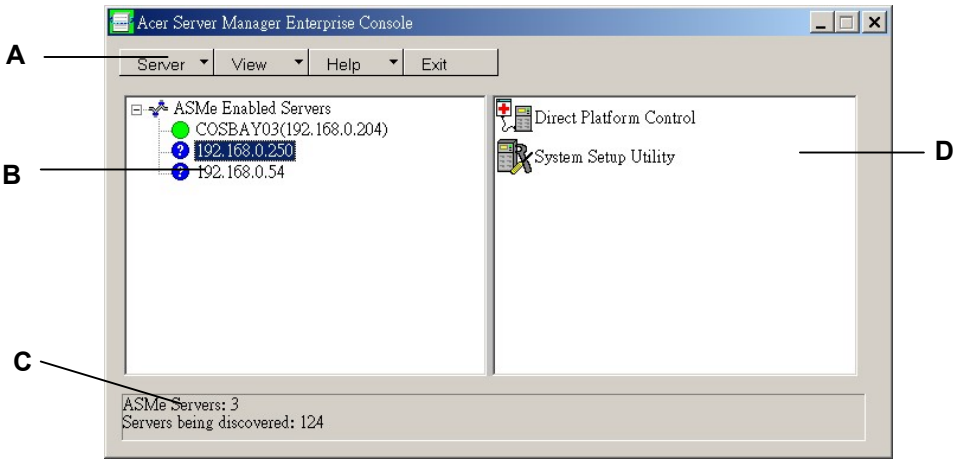
Using the ASMe Console

The ASMe Console provides basic server management functions. From it you can run PIC, DPC, DMI Explorer, and CSSU. The ASMe Console lets you:

- Discover ASMe servers
- Discover which ASMe management tools are available on discovered servers
- Launch the management tools on the managed servers

ASMe Console Main Screen

The following figure shows the main screen of the ASMe Console.



A Button bar
B Navigation Pane
C Status Bar
D Tool Pane

ASMe Console Button Bar

The Button Bar includes the following options:

Item	Options
Server Menu	**Discover:** Start server discovery **Add:** Manually add a server to the tree **Delete:** Delete the selected server from the tree **Delete All:** Delete all servers from the tree **Stop Discovery:** Stops server discovery
View Menu	**List View:** View the tool list as a list **Icon View:** View the tool list as icons
Help Menu	**Contents:** Accesses ASMe Console help topics **About ASMe Console:** Displays ASMe Console version information
Exit	Exit ASMe Console

The ASMe Console includes a navigation pane (tree view) on the left and a tool pane (list or icon view of tools) on the right. Servers that are discovered are added to the tree view. When you select a server from the tree, the tool pane shows a list of supported "tools" running on that server. Launch the supported tool by double-clicking on the icon in the tool pane.

Server Menu Options

Discover

You can discover multiple servers in a single step and add them to the server tree. To discover a range of servers with IP addresses, do the following:

1. On the Button Bar, click the Server->Discover menu selection.
2. Enter the starting address and ending address to be discovered. The starting address defaults to the network subnet of the console machine starting at address 0. The ending range defaults to the value 255, indicating that ASMe will search the entire network subnet. If you change the default address value, enter the full IP address. Wild card characters are not allowed. For all IP addresses, the range of values allowed for any IP address segment is between 0 and 255.
3. Click <OK>.

The ASMe Console investigates and tests each server for all ASMe-registered tools. If one or more of the tools is found, the server is added to the server tree. Depending on the size and complexity of your network, the discovery process can take several minutes.

During the discovery process, the status bar indicates the number of servers still to be investigated. When the number of servers being discovered is displayed as zero, discovery is complete.

Information on servers discovered by ASMe is maintained across machine boots. When the ASMe Console is run, servers discovered during previous sessions are displayed. You do not have to run discovery every time the ASMe Console is launched.

If any of the tools supported by the ASMe Console are installed or removed from a managed server, you should rediscover the server using Server->Add or Server->Discover to update the tool list for that server.

Add

You can manually add a server to the ASMe Console server tree by entering its IP address:

1. On the Button Bar, click the Server > Add menu selection.
2. Enter the full address of the desired server. Wild card characters are not allowed. The range of values allowed for any IP address segment is between 0 and 255.
3. Click OK.

The ASMe Console tests the specified server for all ASMe-registered tools. If one or more of the tools is found, then the server is added to the server tree.

Delete/Delete All

You can manually delete a server from the ASMe Console server tree.

To delete a server, do the following:

1. Select a server or multiple servers in the navigation pane.
2. On the Button Bar, click the Server->Delete or Server->Delete All menu.
3. A confirmation dialog is displayed. Click <OK>.

ASMe deletes the server(s) from the server tree. To restore information about that server, you must rediscover the server using Server->Add or Server->Discover.

Stop Discovery

Stops the discovery process. This is only valid during a discovery. You may choose to stop discovery of all servers on the network and simply add the server IP addresses that you want to manage.

View Menu Options

Icon View/List View

Changes the format of the icons in the Tool Pane.

The Navigation Pane

The Navigation pane shows a tree view of servers with management tools that have been discovered. The tree view has expansion icons ("+" or "-") appearing to the left. The tree can be expanded to list managed servers or collapsed to hide managed servers.

The Tool Pane

When you select a server in the navigation pane, the tool pane displays a set of icons representing the management tools supported on that server. You can start the management tool for the managed server by double-clicking the tool icon in the tool pane.

The PIC application icon does not appear in the tool list for servers discovered by the ASMe console application unless the ASMe Platform Instrumentation (PI) software is running on the server during discovery. To launch PIC from within the ASMe Console, double-click the PIC icon.

The Status Bar

The status bar displays information about ASMe Console operations, such as the number of ASMe servers discovered and the number of servers still to be processed.

4. Platform Instrumentation Control (PIC) Details

Platform Instrumentation Control (PIC) communicates with servers running supported operating systems, and provides real-time monitoring and alerting for server hardware sensors. PIC communicates over the LAN to the Platform Instrumentation (PI) software on the server, using Desktop Management Interface (DMI) 2.0 protocols.

Platform Instrumentation (PI) is server-resident software installed by ASMe to monitor and control the server when the operating system is online. PI retrieves data from the OS, the hardware, firmware and BIOS.

PI can also provide instrumentation data for servers connected through the Intelligent Chassis Management Bus (ICMB). PIC interacts directly with only servers running PI and a supported OS. Through that managed server, with the ICMB interface, Acer servers that are not running PI or are running non-supported OSs can also be managed with PIC. You need a functioning LAN connection from the client system to the server running PI. (For more information about configuring ICMB, see page 46.)

On the client system, the PIC interface integrates into the ASMe Console or one of the supported third-party management tools. PIC relies on the management console to discover servers over the LAN, and forwards changes in the server state to the management console for appropriate alert handling. You can use PIC to:

- View server health information and monitor server hardware sensors, such as
  - Temperature
  - Voltage
  - Cooling fan status
  - Chassis intrusion
  - ECC memory
  - Processor status
  - Power supply status
- Configure sensor thresholds and the actions to take if a threshold is crossed
- Configure, receive, and act upon alert events in the system event log (SEL)
- Specify audio or visual notifications in response to an event
- Automatically shut down, reboot, or power-off the system in response to an event
- View the system event log, the hardware inventory, and information on the BIOS and system slots. If the server has a SCSI controller or LAN adapter you can view their status

With PIC you can track system status and manage hardware conditions. Some conditions have a threshold or range of acceptable values. Default values are configured during system manufacturing. You can use PIC to configure and monitor these values, along with the current readings, error status, and timer settings. An event occurs when a parameter crosses a defined threshold. When an event occurs, PIC initiates the action you have configured, including:

- Resetting or powering off the server
- Generating an NMI
- Beeping the system speaker
- Logging information to disk
- Broadcasting a message on the network
- Displaying a message on the system console
- Paging the administrator
- Sending an email alert

For example, if the temperature reaches a level outside of the user-defined threshold, an event has occurred. You can configure PIC to respond to this event in multiple ways, as listed above.

You can use PIC to view system hardware, BIOS, and slot information. You can also use PIC to configure alert actions for events generated by any of the following hardware components if they are on your server platform:

- Onboard Adaptec SCSI controller
- Onboard LSI Logic SCSI controller
- Onboard QLogic† SCSI controller
- Onboard Promise IDE controller
- Onboard Intel LAN adapter

Using PIC

When you start PIC, the main window displays a tree view. You can expand the view to show the sensor types supported on the managed server and further expand it to display detailed information. A presentation area on the right half of the PIC window displays current readings, threshold configurations, inventory, and other related information for whatever item you have selected in the tree view.

Most of the PIC sensors have associated thresholds that trigger alert actions when the thresholds are crossed. You can:

- Specify which alert actions you want to occur
- Modify the default thresholds
- Configure the default actions and notifications for each threshold

Main Menu Bar

The Main Menu Bar includes the following options:

Item	Options
File Menu	**Exit:** Exits the application
View Menu	**Toolbar:** Toggles the toolbar on or off. **Status Bar:** Toggles the status bar on or off. **Large Icons:** Displays list using large icons. **Small Icons:** Displays list using small icons. **List:** Displays items in list format. **Details:** Displays items in detail format. **Arrange Icons:** Arranges icons by name or status. **Refresh:** Triggers an immediate screen and data refresh. **Options:** Displays the view options dialog so you can configure viewing preferences, such as temperature format and display refresh rate.
Configure Menu	**Enable Front Panel Power & Reset:** Toggles the front panel power and reset option. **Immediate Power Off Server:** Powers off the server and you must manually restart power or use another interface like DPC to restore power. The PIC window will disappear. **Immediate Hardware Reset Server:** Resets the server. The PIC window will disappear. **Enable Watchdog Timer:** Toggles the watchdog timer option. **Watchdog Timeout Value:** Set the watchdog timeout value, which will take effect if the timer is enabled. **Paging Configuration:** Lets you configure Paging Alerts (see page 48). **Email Alert Configuration:** Lets you configure Email Alerts (see page 52). **Restore Factory Defaults:** Restores default values for threshold sensors and the Watchdog Timer.
ICMB Menu	**View Managing Server:** Views the managed server to which PIC is directly connected (the one managing the downstream ICMB servers). **View Managed Server(s):** Views the ICMB-managed servers to which PIC is indirectly connected through the primary managed server. **Reclaim Inactive Resources:** Reclaims inactive ICMB resources on the managing server.
Help Menu	**Help Topics:** Accesses PIC help topics. **About PIC:** Displays PIC version information.

Toolbar

The toolbar gives quick access to some menu items. To hide the icon toolbar, click the right mouse button over the toolbar, and then click the Hide item that appears.

Navigation Pane

The Navigation Pane shows a tree view of server components that can be monitored. Many branches of the tree represent group components that have further branches, which you can expand or collapse with the "+" or "-" icons.

Status Bar

The Status Bar displays status messages. To hide the status bar, click the right mouse button over the status bar, and then click on the "Hide" popup menu that appears.

Presentation Pane

The presentation pane displays details about the item selected in the navigation pane. You can arrange these items by name (sorted alphabetically) or by status (sorted by current status: critical, noncritical, and OK). To change the presentation pane, click the right mouse button over the pane, and then select from the popup menu that appears. This popup menu has two items:

- **View**—Changes between large icons, small icons, list, or detail view
- **Arrange Icons**—Arranges the list view icons by name or status

When you select a sensor item in the navigation pane, the presentation pane displays a set of tabs representing the detailed sensor information. Depending on the item selected in the navigation pane, one or more of the following tabs is displayed:

- **Sensor Settings**—Displays the sensor's current status and current value, threshold values and error counts.

  Use this screen to configure new threshold values (such as Upper Critical Threshold, Upper Noncritical Threshold).

  The sensor status is also represented as a colored "Health" icon: Red is critical, Yellow is noncritical, Green is OK, and Blue is unknown status.
- **Alert Actions**—Displays the currently configured alert actions for each threshold type (such as Voltage-Status Changed to Upper Critical, Voltage-Status Changed to Lower Critical).

  Use this screen to change the alert actions for each supported threshold. The factory default alert actions are Log the Event to Disk and Display a Dialog Box.
- **Sensor Information**—Displays individual sensor information (such as Sensor Tolerance, Maximum Reading, Minimum Reading).
- **Inventory Information**—Displays inventory information for the sensor (such as Description, Manufacturer). The information varies based on the sensor type.

Display Details

For all the following items, PIC displays the item only if appropriate sensors are available on the baseboard. For example, there is a "Chassis" display only if the baseboard has chassis open/closed switches.

Health

Information about all unhealthy sensors is copied under the Health branch. Select the Health branch of the server tree in the navigation pane to get a quick and simple view of the current server health. If, for example, a 12 V voltage sensor indicates that the current status is not OK, then data about that 12 V sensor is added to the Health branch of the tree. You can select the 12 V entry in either the Health or Voltage branch of the tree to display information about the sensor.

All sensors in either a critical or noncritical condition appear in the Health branch of the tree in addition to their normal location in other areas of the navigation tree. In this way, you can get a quick summary of problem areas on your server and begin corrective actions.

Colored icons in the Health branch of the server tree indicate individual sensor status and overall server status:

- **Green:** healthy server
- **Yellow:** noncritical conditions
- **Red:** critical failures
- **Blue Question Mark:** unknown status

The color of the overall server health icon displays the state of the most severe sensor status. If any sensor is in a critical condition (even if all other sensors are noncritical), the server health status is shown as critical (red). If there are only noncritical sensors, the server health status is shown as noncritical (yellow). If all sensors report normal conditions, the server health status is shown as OK (green).

Chassis

PIC monitors chassis door open/closed switches for managed servers that support this feature. The number of sensors monitored depends on the server chassis. If a server supports chassis sensors, the chassis intrusion sensor screen displays the current security status.

When a chassis door that includes an open/close switch is opened, the vulnerable state is indicated as a critical condition in the health branch of the PIC Console, and the requested event actions are carried out. When all chassis sensor switches are closed, PIC indicates the chassis is secure by updating the health indicator.

Fan Sensors

The fan sensor screen displays actual fan RPM for systems that support this feature. The threshold appears in terms of the RPM value. If the current fan RPM value falls below the specified threshold value, then the sensor status changes and an event is generated. For the systems that do not support fan RPM threshold, the threshold setting is 0 and read-only. If the fan stops, the sensor status changes and an event is generated.

PIC monitors two types of fans:

- Rotation-sensing fans—PIC can detect whether a fan has stopped but is not able to indicate which fan has failed. These fans, together, are treated as a single fan unit. Therefore, event actions must be configured for all fans together, rather than separately.
- RPM-sensing fans—PIC can detect whether an individual fan has either slowed or stopped and it displays the actual fan RPM value for systems that support this feature. Each RPM-sensing fan is independently configurable with its own threshold and event actions.

If a rotation-sensing fan fails or an RPM-sensing fan crosses a threshold, PIC displays the event as a critical condition via the health branch of the software, and the requested event actions are carried out.

ICMB

This item displays devices connected through the Intelligent Chassis Management Bus (ICMB). For more information about ICMB, see page 46.

Memory Displays

Memory and memory error correction are represented by the following items:

- Memory Devices
- Memory Arrays

For systems that support Error Correction Code (ECC) memory, PIC reports memory status information for memory arrays and individual memory devices. When you highlight a device or array in the navigation pane, the presentation pane displays a variety of information about the selected device(s). The Sensor Status tab lists details about memory errors. The Sensor Information tab lists details about the memory type and error handling. When you select a memory array, you can configure alert actions to be taken on the Alert Actions tab. There is also a System Inventory tab for memory arrays that lists hardware details.

ECC memory subsystems can detect and report both single-bit errors and multiple-bit errors, as described in the following sections.

Single-Bit Error (SBE) Handling

If a single bit error occurs, the system generates a System Management Interrupt (SMI) that allows the BIOS to log information about the error in the System Event Log (SEL). This information identifies the exact memory device in which the error occurred. Because this condition is recoverable, BIOS returns the system to normal operation after logging the error.

This error is indicated in the health branch of PIC as a noncritical condition, the requested event actions are carried out, and PIC:

- Increments the noncritical error count on the Sensor Settings tab
- Sets the Memory Device Error Type to SBE on the Sensor Information tab for the Memory Device
- Sets the Last Error Update value to "During PIC Runtime," indicating the update occurred while the system was operational

The BIOS stops logging noncritical single-bit errors when the SBE error count reaches nine. This prevents the errors from filling the SEL. Upon system reboot, the OS uses the SEL records, along with the results from its own memory test, to map out bad memory by reducing the usable size of a memory bank to avoid using the bad memory element(s). This elimination of hard errors is a precaution that prevents single-bit errors from becoming multiple-bit errors after the system has booted, and also to prevent single-bit errors from being detected and logged each time the failed locations are accessed. Upon reboot, the single-bit error count is set to zero in the SEL.

Multiple-Bit Error (MBE) Handling

If a multiple-bit error occurs, the system generates a System Management Interrupt (SMI) that allows the BIOS to log information about the error in the SEL, identifying the memory bank in which the error occurred. However, on some systems, it is not possible to determine the exact memory device that caused a multiple-bit error.

Because a multiple-bit error is a critical condition, upon logging the error the BIOS generates an NMI that halts the system. Upon rebooting the server, this error is indicated as a critical condition on the Memory Array and Memory Device in the health branch of PIC. The requested event actions are carried out, and PIC:

- Increments the critical error count on the Sensor Settings tab
- Sets the Memory Device Error Type to MBE on the Sensor Information tab for the Memory Device
- Sets the Last Error Update value to Previous Boot, indicating the last update occurred during the last system boot

Comparison of Single-bit Errors to Multiple-bit Errors

The following table compares the steps taken with single-bit and multiple-bit errors

SBE and MBE Comparison

Memory Error Handling	SBE	MBE
Generate SMI	Yes	Yes
Log information includes	Exact SIMM or DIMM	Memory bank only
Action after SEL logging	Continue operation	Stop the system
Indicated by PIC screen changes	Immediately	After the system reboots
Bad memory is mapped out at next reboot	Yes	Yes (immediately after the failure)

PCI HotPlug Device

This sensor screen displays information about each PCI Hot Plug device installed in a PHP slot.

Power Supply and Power Unit

The Power Supply sensor screen shows information about each power supply.

The Power Unit represents power supply redundancy. For systems that support it, PIC monitors the status of the power supplies in the managed server. The power unit sensor screen displays information and status about each power unit.

If a power supply reports a predictive failure condition, PIC reports the status as a non-critical condition in the health branch and carries out the requested event actions.

If a power supply fails, PIC reports the failure as a critical condition in the health branch and carries out the requested event actions. PIC also reports the system power as nonredundant and as a noncritical condition in the health branch, and carries out any requested event actions.

If a power supply fails or if the surplus power on the system is less than the amount provided by one power supply, PIC reports that the system power is nonredundant. It reports this condition as a noncritical status in the health branch and carries out the requested event actions.

For systems that do not support power supply sensors, PIC does not display the Power Unit or Power Supply items.

Processor

The processor sensor screen displays information and status about each processor. From this screen, you can find out the type and speed of the processor. Click the Sensor Information tab to display sensor-specific information (not all servers support this function).

For baseboards that support it, PIC monitors processor failures during runtime and system boot operations on the managed server. If a supported baseboard includes multiple processors, each processor can be configured and monitored separately through PIC. If a processor failure is detected, the failure is reported as a critical condition in the health branch of PIC, and the requested event actions are carried out.

System Slots

ASMe gathers sensor information and slot status on all slots in the managed server. The slots are categorized into two groups:

- PCI Hot Plug (PHP) slots, if the server hardware supports PCI HotPlug
- All other non-PHP system slots

Slot names containing "PCI 64bit" identify PHP slots. For PHP slots, there are three tabs available in the presentation pane: Sensor Information, Sensor Status, and Alert Actions.

For non-PHP slots, PIC displays only the Sensor Information details.

System Information

PIC gathers information on field replaceable unit (FRU) components installed in your managed server. This information includes a component description, manufacturer, model, part number, component number, serial number, and revision level. PIC also gathers information on other system resources including Operating System, BIOS, and the System Event Log.

The inventory screen displays components in the system, with a description, manufacturer, model number, part number, serial number, and revision level of components on the baseboard. The inventory list includes information on the baseboard, processor board, chassis, power share board, hot-swap backplane, and memory devices.

Temperature

The temperature item displays information about all temperature sensors. You can see individual sensor information in the presentation pane by selecting the corresponding sensor in the navigation tree. The Sensor Settings tab lets you monitor current temperature readings, current status, and sensor error counts, and lets you set sensor thresholds. If a threshold is not supported, it is grayed out. The Alert Actions tab lets you set what kinds of actions to take if a sensor crosses the boundaries you have set. The Sensor Information tab displays information like minimum and maximum readings, nominal readings (the expected normal reading for this sensor), and the tolerance of this sensor.

Third-Party Components

You can configure event actions for DMI indications generated by third-party Server Instrumentation installed with PI. You can also monitor third-party instrumentation via the DMI Explorer Interface. See page 44 for details about event configuration for third party instrumentation.

Voltage

In a managed server, PIC monitors many types of voltage sensors; the number and type depend on the server hardware configuration. Each monitored voltage sensor has independently configurable thresholds and event actions. Example voltage sensors are:

- 12 V, 5 V, 3.5 V, 3.3 V, -5 V, -12 V
- Processors 1.5 V and 2.5 V
- SCSI A Termination 1, 2, and 3

The voltage item in the navigation pane lists all supported voltage sensors. You can see individual sensor information in the presentation pane by selecting the corresponding sensor in the navigation tree. The Sensor Settings tab lets you monitor current readings, current status, and sensor error counts, and lets you set sensor thresholds. If a threshold is not supported it is grayed out. The Alert Actions tab lets you set what kinds of actions to take if a sensor crosses the boundaries you have set. The Sensor Information tab displays information like minimum and maximum readings, nominal readings (the expected normal reading for this sensor), and the tolerance of this sensor.

Managing Servers with PIC

Besides monitoring server health, the most important actions you take with PIC are configuring the sensor thresholds at which you want to be notified, and configuring the actions to be taken when a threshold is crossed.

Viewing and Configuring Sensor Information

To view or configure a sensor, do the following:

1. On the PIC main window, expand a sensor item (such as voltage or temperature) in the navigation pane to see the list of available sensors.
2. Select an entry from the list.
3. Switch between the available tabs (Sensor Settings, Alert Actions, Sensor Information or Inventory Information) to view or update the information.
4. Click <Apply> for any changes made to the sensor configuration.

At any time you can change views to another sensor by selecting another component in the navigation pane.

If you try to change your view and you have not saved any configuration changes using the Apply button in the presentation pane, PIC prompts you to save or discard the changes before switching to a new view.

Viewing System Information

To view system information (such as FRU, Operating System, BIOS, and SEL) on the managed server or a managed ICMB device, do the following:

1. On the PIC main window, click beside the System Information name in the PIC navigation pane to see the list of options.
2. Select an entry from the list.
3. View the information in the corresponding tab in the presentation pane.

At any time you can change views to another sensor by selecting another component in the navigation pane.

If a component supports FRU data, this information is also displayed on the Inventory Information tab for that component.

System Event Log

PIC displays the System Event Log (SEL) maintained by the managed server's platform hardware. The SEL is a collection of log entries stored in nonvolatile flash memory.

The server software (Platform Instrumentation) automatically extracts event information from the SEL and triggers any user-configured actions associated with that event. Platform Instrumentation clears the SEL when it is near an out-of-space condition. PIC displays the SEL logging status (whether the SEL is Active or Inactive).

The display of SEL records includes timestamp information. Platform Instrumentation sets the timestamp of SEL records written prior to a system boot record using the timestamp from the boot record.

Configuring Thresholds

There are two basic types of thresholds:

- **Range-based thresholds** for which a variety of values can be set; for example, temperatures, voltages, and RPM-sensing fans.
- **State-based thresholds** that have fixed values like OK or Critical; for example, rotation-sensing fans, chassis doors, and memory arrays.

To Configure a Range-Based Threshold

Most voltage sensors, temperature sensors, and RPM-sensing fans have one, two, or four configurable thresholds, depending on your server. Example thresholds are:

- Upper Critical
- Upper Noncritical
- Lower Noncritical
- Lower Critical

Some special sensors do not have configurable thresholds and are displayed for monitoring purposes only.

You can customize the threshold value to suit your working environment.

You can specify what action should occur when the sensor detects that one of the threshold values has been crossed (i.e., the sensor state changes).

- Status Changed to OK
- Status Changed to Upper Critical
- Status Changed from OK to Upper Noncritical
- Status Changed from Critical to Upper Noncritical

These thresholds and sensor state changes let you configure progressive responses in PIC to increasingly serious hardware conditions. For example, noncritical thresholds might be configured to emit a beep from the speaker and send a broadcast message, while critical thresholds might require more serious actions, like a server shutdown.

To configure a range-based threshold:

1. On the PIC main window, expand the item in the navigation pane to see the list of available sensors.
2. Select an entry from the list.
3. Change the threshold values as needed on the Sensor Settings tab.
4. Click <Apply> for any changes made to the threshold value configurations.
5. If you want to change the event actions associated with threshold state change conditions, make the changes on the Alert Actions tab.
6. Click <Apply> for any changes made to the alert action configuration.

NOTE

After applying new threshold values that may cause an event indication, the sensor status icon displayed on the Sensor Settings tab may not change. The console refreshes the display before the new threshold value takes effect on the server, making it appear as though the sensor icon does not accurately reflect the current state of the sensor. Use the menu option, View->Refresh, or the F5 keyboard shortcut, to update the Sensor Settings tab.

To Configure a State-Based Threshold

The state-based thresholds for processor, power supply, rotation-sensing fans, chassis door, and memory arrays have a fixed set of values, not a range. Example state change conditions:

- Single Bit Memory Error
- Processor Thermal Trip
- Power Supply Failed

NOTE

For systems that support rotation-sensing fans, the fan RPM threshold setting displays a "0" and is read-only in PIC.

PIC generates an event whenever the state of these items changes. You can specify which actions should occur in response to changes. To configure a state-based threshold:

1. On the PIC main window, click beside a sensor name in the navigation pane to see a list of available sensors.
2. Select an entry from the list.
3. Select the Alert Actions tab. Change the event actions associated with a state change condition.
4. Click <Apply> to save your changes.

Cautions in Setting Thresholds

Rounding of Threshold Values

Hardware rounding can cause thresholds to be set to a different value than the exact value you enter in ASMe. Redisplay the Sensor Settings tab to find the actual value set by the software.

Avoiding a Power On/Off Loop

Improperly setting event actions can cause the server to enter a state that prevents the server from booting correctly. For example:

1. An event occurs, such exceeding a high-temperature threshold.
2. While the condition causing the event still exists, you set a Shutdown/Power Control Action, like Immediate Power Off, to respond to this event.
3. Because the threshold has already been exceeded, no event is triggered to cause the Immediate Power Off action to occur.
4. If you reboot the system and the event condition has not been corrected (for example, the temperature is still over its threshold), the system detects the temperature condition, triggers the event, and the corresponding action is taken. The system is automatically and immediately powered off because of the Immediate Power Off action you set.

When the system is powered up, an infinite loop of power-up and power-down begins. To break this cycle, choose one of the following methods:

- Clear the event condition (for example, cool the system to clear the temperature condition).

OR

- Create a file named C:\LRA.NOT (or insert a diskette with file \LRA.NOT in A: drive) before the OS boots. The existence of this file disables the software component that responds to the event. The contents of the file are not important. You must then delete this file after the problem is fixed to allow the software to operate normally.

Avoiding a Reboot-Fail Retry Loop

User-defined threshold values and other user-defined configuration attributes are written to disk (persistent storage) so they are available when the server reboots. These "remembered" values replace the PIC default values when PIC initializes.

When you change a threshold value or alert action in PIC, you can create an environment in which an event is immediately generated, such as setting the Upper Noncritical Threshold value below the current sensor reading. If the configured event actions on this threshold included a Shutdown or Power Control action as described earlier, the server would trigger the Shutdown or Power Control action and could enter a reboot-fail-reboot-fail cycle using the new threshold value.

To help avoid this situation, PIC updates the server in two steps:

1. Any change you make is valid immediately in the active instrumentation, but PIC waits five minutes before writing user changes to disk. Thus, if the change causes the server to reboot, the previous value is restored from disk when the server reboots.
2. PIC then uses and displays the previous value, thus avoiding the immediate reboot-fail-reboot-fail cycle.

Any change you make is successfully written to disk as long as the server instrumentation continues running for five minutes after the change is saved.

Configuring Threshold Event Actions

On the Alert Actions tab, you can select actions to take place when a sensor exceeds a threshold or changes state. Options include:

- Audio/visual notifications (you can select more than one)
- Shutdown/power control actions (you can select only one)

NOTE

If you select a power control option for a non-critical event (such as a voltage surge) so that the OS is disabled by the non-critical event, critical actions will not be carried out because the OS has been shut down. It is best to use warnings (such as a speaker beep, a broadcast, etc.) for non-critical conditions.

The following tables list the threshold event actions you can set in PIC. You can specify multiple notifications per event but only one power control action.

Notification Action	Description
Emit a beep from the managed server's speaker	Speaker beeps.
Display an alert message on the managed server	Default action for noncritical and critical indications. The message box stays up until acknowledged.
Log the event to disk	Default action for all indications. This option records the event in the standard system error log. On Windows 2000, PIC records the event in the Windows System Event Log, which you can view with the Windows Event Viewer under Control Panel > Administrative Tools.
Broadcast a message	Default action for critical indications. On Windows 2000, the message goes to all the users currently logged into the managed server, including systems which have a drive mapped to the server.
Page an administrator	A page is sent to a specified pager, with a message that can include the phone number of the server, an ID number, or other numerical information.
Email	An Email with appropriate alert messages is sent to the specified users.

Power Control Action	Description
No shutdown	Default action for all indications. Select this option if you do not want to shut down or reset the server when an event occurs.
Shutdown the OS	Select this option if you want to shut down the OS gracefully (controlled, closing files and applications). On Windows 2000, the server is set to a state ready for manual power-off or reset.
Shutdown the OS and power off	Select this option if you want to shutdown the OS gracefully and turn off the system power.
Shutdown the OS and hardware reset	Select this option if you want to shutdown the OS gracefully and reset the server via hardware.
Immediate power off	Select this option if you want to immediately power down the server. This action is an immediate power-off without a shutdown of the OS; it might corrupt files.
Immediate hardware reset	Select this option if you want to immediately reset the server via hardware. This action is an immediate hard reset without a shutdown of the OS; it might corrupt files.
Immediate NMI	Select this option if you want to cause a hardware Non-Maskable Interrupt (NMI). If this feature is not supported on the managed server, this option is grayed out.

Overriding Power Off or Shutdown Actions

You can globally override power off or shutdown actions while allowing other event actions (e.g., paging, broadcast message, etc.) to take place. There are two ways:

- To override power off or shutdown actions during installation of the ASMe software, select a custom installation and check "Event notification only" under the "Platform Instrumentation" feature in the feature selection dialog. By default, the installation enables power off or shutdown actions.
- If ASMe has already been installed, use the following configuration instructions depending on the server operating system:

  Windows 2000

  Set the `NotificationOnly` parameter in the *%ISCPATH%\bin\lra.cfg* file to `TRUE` and reboot the server.

To re-activate the power off or shutdown action, set the `NotificationOnly` parameter in the corresponding file under each operating system described above to `FALSE` and reboot the server.

Configuring Third-Party Event Actions

On the Alert Actions tab, you can select actions to take place when a third-party component exceeds a threshold or changes state. You can configure event actions for any of the following onboard third-party components, if available on your server.

- Adaptec SCSI
- LSI Logic SCSI
- QLogic SCSI
- Promise IDE
- Intel LAN Adapter

To configure event actions for third-party indications:

1. On the PIC main window, click beside the third-party component name in the navigation pane.
2. Update the Alert Actions tab and change the event actions associated with a threshold type or state change condition.
3. Click <Apply> to save your changes.

The following table lists event information for third-party component instrumentation supported by PIC.

Controller	Choices
Adaptec SCSI*	**Storage Device Events Group** Storage device state information Storage device recovered error - Bad block repaired Storage device member marked down **Storage Controller Events Group** Storage Controller state information Storage Controller SMART event Storage Controller status unacceptable **Volume Set Events Group** Volume set state information Volume set recovered error Volume set Array status – offline **Spare Events Group** Spare not functional **Enclosure Events Group** Enclosure state information
LSI Logic SCSI*	**Storage Devices Events Group** Device Error (not responding) Device Warning (predicted failure(S.M.A.R.T.)) **Storage Controller Events Group** Controller Error (not responding) **Mass Storage Association Events** New Storage controller detected New device detected Existing controller changed Existing device changed
QLogic SCSI	**Storage Devices Events** New or Recovered Storage Device Error Storage Device Not Responding Device Warning (predicted failure (S.M.A.R.T.)) **Storage Controller Events** Informational SCSI Controller Event Non-Critical SCSI Controller Error Critical SCSI Adapter Event
Promise IDE	**Mass Store Logical Drive Events** IDE RAID Array OK Non-Critical IDE RAID Array Event IDE RAID Array Off-line **Disk Events** IDE Disk Status OK IDE Disk Status Critical

* Event actions do not distinguish between onboard controllers and add-in cards. This means that event actions are configured for all controllers by a specific third party, regardless of whether it is onboard or on an add-in card.

continued

Controller	Choices
Intel LAN Adapter (These events are available only for Windows 2000 servers)	**NIC Health Contributor** Cable unplugged/No LAN activity Adapter initialization failure **NIC Teaming Events** Primary Adapter is switching over and the Secondary Adapter took over Primary Adapter became active Secondary Adapter is deactivated from the team Initialization Failure The last Adapter has lost link. Network connection has been lost Preferred Primary Adapter has been detected The team has only one active adapter Secondary Adapter has re-joined the team Preferred Primary Adapter has taken over Network Connection restored

ICMB Devices

Highlight the ICMB item in the navigation pane to display details about devices connected to a managed server through the Intelligent Chassis Management Bus (ICMB). The ICMB bus allows multiple remote devices to be interconnected and management information shared among them. For example, your managed server could be configured as an ICMB primary server and report management information on other ICMB devices connected to it. Using ICMB, PIC can manage the power state of remote ICMB devices and view FRU information about those devices. The amount of FRU information available depends on the type of ICMB device being managed.

Through the PIC Console, you can switch your view of the primary managed server to one of the ICMB-managed devices and view the available information on that device without losing the connection with the primary server. You can change your view back to the primary server or any other ICMB-managed device at any time.

PIC lets you configure the ICMB management features of the primary managed server and the remote ICMB-managed devices:

- **Local ICMB Server Configuration—**With this option you can enable the local server as a management point, enable the full sensor view of remote devices, and change the discovery period for remote devices.
- **Remote ICMB Chassis Configuration—**With this option you can configure each remote device discovered via ICMB. You can manage the remote device, enable full sensor view for the remote device, and set the event polling rate for the remote device.

The ICMB menu lets you reclaim inactive ICMB system resources on the primary server. Doing so frees the memory taken up by the SDR and FRU information on the primary server for any remote device that is no longer visible on the network via ICMB.

Switching Views Between Primary (Managing) Server and an ICMB Device

To view an ICMB-managed device in the navigation pane of the PIC main window, do the following:

1. On the PIC Main Menu Bar, click the ICMB->View Managed Server(s) menu selection.
2. Select the ICMB device to view.
3. Click <OK>.

The tree in the navigation pane is replaced with information about the new device. At any time you can change views to another ICMB device by repeating the steps above. To return your view to the primary server in the navigation pane of the PIC main window, click the ICMB->View Managing Server menu selection on the PIC Main Menu Bar.

Configuring ICMB on the Primary (Managing) Server

To configure ICMB on the primary (managing) server, do the following:

1. If you are viewing an ICMB device instead of the primary server, on the PIC Main Menu Bar click the ICMB->View Managing Server menu selection to switch to the primary server.
2. In the PIC navigation pane, click beside the ICMB component name in the navigation pane.
3. Change the configuration on the ICMB tab in the presentation pane.
4. Click <Apply> for any changes made to the ICMB configuration.

Configuring the Watchdog Timer Value

Each baseboard supported by PIC has a watchdog timer implemented in the hardware; the timer is disabled by default. When enabled, the timer continually decrements to test the response of the server operating system. Under normal operating conditions, the Platform Instrumentation software periodically resets the time to prevent it from reaching a value of zero. If the OS hangs, the timer counts down to zero.

If the timer reaches a value of zero, indicating an OS hang, the watchdog timer resets the system. The default timer value is two minutes with minimum and maximum allowable settings of two to sixty minutes.

To configure the watchdog timer value, do the following:

1. On the PIC Main Menu Bar, click the Configure->Watchdog Timer Value menu.
2. Update the timer value.
3. Click <OK>.

Paging

PIC lets you configure the paging features available on a server. If the server hardware does not support paging, the Paging Configuration menu item is grayed out.

Initiating a Page

To specify that a page be sent in response to an alert, check the "Send a Page" box in the Alert Actions tab for any sensor or threshold event.

NOTE

Don't configure a shutdown/power control action for events where you specify paging notification. If you select a paging notification and a shutdown option for the same event, the page will not be sent because the operating system will be shut down.

Paging Configuration

Select Configure->Paging Configuration from the main menu in PIC and enter the following information. The configuration you enter here is global to the server and not sensor-specific—the same page is sent in response to all events that you configure with the "Send a Page" action.

Global Paging Enabled: This checkbox specifies whether the paging feature is globally enabled or disabled. If this item is disabled, you cannot enable the paging action in the Alert Actions dialog.

Default Pager #: This is the number paged when a paging action is triggered. If this value is blank, no paging occurs. The Test Page button calls this number.

Enter the full pager number the way it should be dialed, including the initial number if any needs to be dialed to get a dial tone, commas (',') for pause characters, area code, etc. For example, "9,6903115" specifies a 9 to dial out, a pause, then a local number without an area code. After the pager number, you can include another pause, then enter any numeric data to be sent (such as a code, a number to call back, etc.). All numeric data must be entered in the Pager Number field. For example, you might enter a modem phone number to dial back, followed by a numeric ID, etc. Alphabetic data is not allowed.

Additional Pager #1 and #2: These are additional pager numbers to be called after the default pager number when a paging event occurs. Enter all data including the numeric message as described above.

These additional numbers are called if a paging event occurs, but are not called when the Test Page button is pressed. To test one of these numbers, you must copy it to the Default Pager # field, then press the Test Page button.

Paging Properties: You can configure a page to be sent multiple times with the following fields:

- **Number of Pages:** specifies how many times each pager number will be paged (from 1 to 100). Number of Pages defaults to 1, and if set to 1, the Repeat Paging Interval value is not needed.
- **Repeat Paging Interval:** specifies the interval in minutes between each cycle of pages (one cycle includes sending a page to all configured pager numbers). The minimum and default value of Repeat Paging Interval is one minute. The maximum value is 1440 minutes (24 hours).

Before saving the information, you can press the Test Page button to verify that the default pager number is paged.

Click the OK button to save the information and exit from the screen. Click the Cancel button to restore the previous information and exit from the screen.

Customizing PIC Administrator Options

PIC options let you set the PIC console refresh rate, which determines how often PIC is updated with current information from the server. You can specify whether temperatures display in Celsius or Fahrenheit, and whether to restore PIC settings to the factory defaults. These settings are global and affect any open PIC session.

To configure the refresh interval or temperature display format:

1. On the PIC Main Menu Bar, click the View->Options menu selection.
2. Change the refresh interval or temperature display format on the Options dialog.
3. Click <OK>.

NOTE

For servers that support server health update events, configuring the console refresh interval is not necessary or applicable. For other servers, when configuring the console refresh interval, selecting a frequent refresh interval impacts system performance on both the console and the managed server because ASMe polls for the health status of each monitored sensor. Selecting a less frequent console refresh interval provides a reasonable information update, while minimizing the overhead on system performance. The console refresh interval does not impact how quickly the server system responds to event notifications (e.g., threshold crossings) only how quickly the ASMe main screen display updates with server information. A value of 15 seconds or greater for console refresh value provides a reasonable compromise.

Default Values and Restoring Default Values

PIC installs with the following default values:

- PIC console refresh interval: 10 seconds
- Temperature display format: Celsius
- Watchdog feature: off
- Watchdog timer: two minutes
- Sensor threshold: values as defined in the Sensor Data Records (SDR) file

To restore default PIC settings for threshold values and the watchdog feature:

1. On the PIC Main Menu Bar, click the Configure->Restore Factory Defaults menu selection.
2. Click <OK> on the confirmation dialog.

Some configurations are not affected by the Restore Factory Defaults option. Event actions you have configured, the temperature display format, and the console refresh rate are not affected when you click the Restore Factory Defaults menu item.

Default threshold values are stored in Sensor Data Records (SDR) in nonvolatile storage on the baseboard. These values are determined and configured during baseboard manufacturing and are therefore not documented in this manual.

Event indications may be generated if restoring the default threshold value crosses the current sensor value. For example:

- User defined threshold limit 13.5 V
- Current sensor value 13.0 V
- Default threshold value 12.5 V

When you select the Restore Factory Defaults action, the restore may cause a threshold crossing. In the above example, PIC would detect a threshold crossing and generate an event indication. The actions associated with that indication would occur.

To avoid the possibility of unwanted event indications when restoring default settings, adjust the user-defined threshold value so the current sensor value is not between the user-defined threshold value and the default threshold value.

PIC Event Messages

Event actions that you can specify in PIC include alert messages that may be displayed at the server, sent in a broadcast, or sent in an email message. The message text is based on the event information. The text contains the DMI group and information about the attribute that caused the error.

Messages Displayed at the Server

The general format of messages that display at the server is:

```
Event reported for <attribute_name> attribute in the
<group_name> group
```

For example, the message:

```
Event reported for Upper Critical Threshold attribute in the
Temperature Sensor group
```

means that one of the system's temperature sensors reported a value above the upper critical threshold you have set.

Broadcast Messages

The following table lists broadcast messages that can be sent across the network to client computers. These messages will appear on the display of any computer logged into the server or with a network drive mapped to the affected server. The general format of broadcast messages is:

```
Check <group_name> at server <server_name>
```

Broadcast Messages

Message	Description
Check Temperature Sensor at <server> Check Temperature Probe at <server>	A temperature sensor reported a change in state (OK/Noncritical/Critical).
Check Voltage Sensor at <server> Check Voltage Probe at <server>	A voltage sensor reported a change in state (OK/Noncritical/Critical).
Check Security Sensor at <server> Check Physical Container Global Table at <server>	System chassis front or side panel has been opened, or it was open and has been closed.
Check Cooling Fan at <server>	System fan has stopped or restarted.
Check Memory Array at <server>	A memory error was reported.
Check Host Adapter at <server>	A SCSI board reported a state change.
Check Logical Unit at <server>	A SCSI device reported a state change.
Check Controller Information at <server>	A RAID controller reported a state change.
Check Physical Drive Information at <server>	A RAID drive reported a state change.
Check Processor at <server>	A processor error was reported.
Check Power Unit Global Table at <server>	A power unit redundancy state change was reported.
Check Power Supply at <server>	A power supply failed.
Check Indication Control Group at <server>	The LAN Adapter reported a threshold crossing.
Check Storage Device Events at <server>	A SCSI device reported a state change.
Check Storage Controller Events at <server>	A SCSI controller reported a state change.
Check System Slot at <server>	A PHP slot reported a state change.

Email Messages

The Platform Instrumentation software on the server determines the content and subject line of email messages generated by an email alert. Messages have the following form:

```
Check Voltage Probe at server <server-name>
Event Type:Status Changed from OK to Upper Non-Critical
Event Severity:Non-Critical
Component:Acer Corporation, Baseboard
Group:Voltage Probe
Instance:4
```

Configuring Email Alerts

To use email alerting, email capability is required on your network. Use PIC to configure the Email Alert settings for each managed server.

Use the Alert Actions tab for individual sensors to set an Email Alert notification for that sensor.

NOTE

Don't select a shutdown/power control action for events where you specify email notification. If you select email notification and a shutdown option for the same event, the email will not be sent because the operating system will be shut down.

Email Settings

Configure email by selecting Configuration > Email Alert Configuration. This configuration is global to the server and is not sensor-specific.

Specify these settings on the Email Alert Configuration screen:

From Email ID: Specify the email ID of the sender of the message.

To Email ID: Specify one or more destination email IDs to receive the alert. Use standard Internet format. Use commas or semicolons to separate multiple email IDs. If this field is blank no email will be sent.

SMTP Server: Specify the name of the mail server.

Test Email

After entering the email configuration data, click the Test Email button to verify that email is sent as you expect. When you press the Test Email button, you receive a dialog where you fill out the subject line and the test message. After you enter the subject and message, click OK to send the test message. After sending a test email, verify that all destinations have received the test message.

NOTE

The subject and message that you enter in a test email are not the same subject and message that will be sent in an actual email alert. The PI software automatically determines the content of the alert message (see page 52).

Discovering Email Errors

If a test email or actual email alert is not generated or is not received, there are several possible reasons, including:

- You entered the SMTP server name wrong
- The network failed
- The SMTP server terminates the connection due to an abnormal condition or it times out for some reason

All of the above failures will result in an error message in the operating system's System Event Log on the server (not the same as the non-volatile System Event Log, or SEL that you view with ASMe tools). For example, the message might be "Test email was not sent" or "Email Alert was not sent" with a failure reason of "Unable to access the SMTP server" or "Server <server-name> not found".

You can view the System Event Log errors as follows:

- On a Windows system use the Event Viewer or Event Properties from the Control Panel > Administrative Tools.

5. Direct Platform Control (DPC) Details

Direct Platform Control (DPC) gives access to a remote server when it is online or offline, when the operating system is hung, or even when the server is powered off. When you receive notice that a server has malfunctioned (for example, by receiving a page), you can use DPC to investigate the cause of the alert, take corrective action, and restart the server into normal operation.

DPC uses a redirected text-based console that runs over a serial connection or the LAN. Since DPC does not communicate with the server OS, it can manage the server even if the OS and primary processors are not working. Because the server's emergency management hardware works on 5 V standby power, DPC can communicate with and control a powered-down server, assuming the AC power is connected.

You can use DPC to:

- Reboot a server
- Restart a server whether it is powered on or off
- View the System Event Log (SEL) for information about recent server activity
- View Sensor Data Records (SDRs) for information about sensor characteristics
- Review Field Replaceable Unit (FRU) inventories
- View current Remote Sensor Access (RSA) information
- Reboot a server to the service partition, if available
- Reset a remote server to either EMP mode or Re-direct Mode
- Maintain a Phonebook for remote server connection management
- Reboot to the service partition to run service partition-based utilities on the server such as running a command shell. You can also upload or download files to the service partition, run a remote program, or remote diagnostics if available

You can launch DPC from the ASMe Console or one of the supported third-party management consoles. DPC contains a security feature that requires a password entry before initiating a connection to a managed server.

For more information about using DPC, see its Help system.

Server Connections

DPC can communicate over a serial link (modem or direct connection) to the server's Emergency Management Port (EMP) or over the LAN to the server's Total Cost of Ownership (TCO) port. DPC is supported only on the onboard NIC1 interface (see your server product guide for more information). In either case it communicates through the Baseboard Management Controller (BMC) on the server, not with the server operating system. Any operating system can be running on the server.

Configuration of the server's serial and LAN connections is described beginning on page 13. For ASMe-supported servers, BIOS Setup is not required for console redirection to allow DPC communications over the COM2 serial port (EMP).

Starting the DPC Console

The preferred way to start DPC is to double-click the DPC Console icon in the tool pane of your management software (such as ASMe Console) after selecting the appropriate managed server. You can start DPC without a connection from the Windows Start menu under Programs> Acer Server Manager Enterprise.

You can also launch DPC Console using the command line. Depending on the connection type (modem, direct serial connection, or LAN), use one of the following commands:

`DPCConsole /modem=[phonenumber]`
where [`phonenumber`] is the phone number of the server.

`DPCConsole /direct= [comX]`
where [`comX`] is the COM port of the client workstation's direct connection.

`DPCConsole /lan=[IPaddress orDNSname]`
where [`IPaddress or DNSname`] is the IP Address or the DNS Name of the server.

DPC Features

Use the DPC menus or click a toolbar button to access DPC features. The menu items and toolbar change according to what features are available on the server. When one of the DPC managers is active its menu is added to the DPC Console.

SEL Manager

The System Event Log (SEL) is a collection of log entries stored in nonvolatile flash memory on the server. The BIOS and OS write entries to the SEL. The DPC SEL Manager lets you:

- View SEL events.
- View the properties of the non-volatile storage area for SEL.
- Save SEL events to a file.
- Print the SEL events to a local printer.
- Clear SEL records from the non-volatile storage area on the server.

SEL events display as a sequential record of managed server events, one event per row. You can sort each column by clicking on the column heading.

SDR Manager

Sensor threshold values and other data are stored in Sensor Data Records (SDR) in nonvolatile storage on the server. The DPC SDR Manager lets you:

- View Sensor Data Records.
- View the properties of the non-volatile storage area for SDR.
- View SDR information in a previously stored file.
- Save SDR information to a file.

The SDR Manager displays with a navigation (tree view) pane, a presentation pane and a description pane. Selecting a specific Sensor Data Record from the tree view displays the corresponding SDR information in the presentation pane.

FRU Manager

Field Replaceable Units (FRUs) are components installed in your managed server. FRU information stored on the server includes a component description, manufacturer, model, part number, component number, serial number, and revision level. The DPC FRU Manager lets you:

- View FRU inventory.
- View the properties for a FRU.
- Save FRU inventory information to a file.

The FRU Manager displays a hierarchical tree of FRU areas (chassis, product, and board), and detailed inventory information about a selected area. Select an area in the tree to see its associated inventory information in the presentation pane on the right. A description of each field you select is displayed in the right bottom pane.

RSA Manager

The Remote Sensor Access (RSA) Manager lets you view server baseboard FRU and SDR information.

The RSA Manager displays a tree view on the left and a property view on the right. The tree view displays all detected sensors. The property view displays tabs of sensor status or sensor information for the sensor selected in the tree view.

If the connected server is powered down, some sensors cannot be read and their current status will display as Unknown.

Phonebook

DPC includes a phonebook (shared with CSSU) that stores server entries, including the name, server phone number, and server LAN address (specified either as an IP address or DNS name). You can add, modify, or delete phonebook entries.

Rebooting to the Service Partition

You can use DPC to reboot the server to its service partition.

The service partition is a special partition on the hard disk that you establish when initially setting up the server (see page 11). The service partition contains utilities, diagnostics, and other software required for remote management. The service partition is not marked as an active partition and the server only boots from it by a special request. It is not normally visible to the server user.

After the server reboots to the service partition, you can run text-based programs installed on the service partition.

To boot to the service partition:

- The connected server must contain BIOS support for booting to the service partition.
- A service partition must be installed on the server hard drive.
- You must have administrative rights for this connection on the server.

Displaying Configuration Status

The Configuration dialog box displays the server's configuration status. You can view this status information whenever the DPC Console is connected to a managed server. Information appears in several areas:

Supported Viewers: Status on the FRU, SEL, SDR, and RSA viewers.

Security: Displays the following settings:

- Authentication level: Indicates User or Administrator level. Administrator level exists if you are logged in with administrative rights. User level applies to these situations:
  - — EMP (serial) connection when EMP mode is set to "restricted".
  - — LAN connection over the Total Cost of Ownership (TCO) port where a secure session is not available (e.g., someone else is already connected).
  - — Restricted LAN access mode.
- Activation Mode: Indicates whether the server is always active or just during pre-boot.
- Chassis Intrusion: Indicates whether intrusion protection is set or not set.

Firmware: Displays the Intelligent Platform Management Interface (IPMI) and Baseboard Management Controller (BMC) revisions on the server.

Aside from these designated areas, the Configuration dialog box also indicates the server's power state, the operating system (if detected), and the presence of a service partition.

NOTE

For DPC Console to detect a connected server's operating system, the server must have Platform Instrumentation (PI) installed.

6. Client SSU (CSSU) Details

The Client SSU (CSSU) allows you to remotely run the System Setup Utility (SSU) software or other utilities on the server. CSSU can connect to the server using a modem, serial port, or LAN. You start a CSSU session by requesting a service boot of a particular server through the Emergency Management Port. The service partition includes the ROM-DOS† operating system and SSU, and may contain other utilities you install. As the server boots to the service partition, a network stack and agent are started and communication switches to the required protocol.

Use CSSU to:

- Modify the server's boot device order or security settings
- Change the server configuration settings
- View or clear the System Event Log (SEL)
- View Field Replaceable Unit (FRU) information
- View the Sensor Data Record (SDR) table

The specific functions available in CSSU vary depending on the server to which you are connected. Only a single instance of CSSU can be running and you can make only one connection at a time.

You can launch CSSU from the Start Menu under Programs> Acer Server Manager Enterprise or from the Run command in the Windows Start menu. When launched from the Program Group, the main CSSU window displays and waits for your input. When launched from the Run command with the appropriate parameters, CSSU attempts to connect to the server with the specified phone number, IP address, or DNS name. When the connection is established, the main CSSU window displays the connection information in the status bar. If the connection cannot be established, you receive an error message and the main CSSU window waits for your input.

CSSU Operation

When CSSU connects to a server, it causes the server to reboot to the service partition.

CSSU stores the configuration values you enter in non-volatile memory in the server. These values take effect when you reboot the server to its normal boot sequence. The BIOS checks the values against the actual hardware configuration, and if the values do not agree, the BIOS generates an error message. You must then run CSSU (or run SSU locally on the server) to specify the correct configuration before the server boots. CSSU always includes a checksum with the configuration data, so the BIOS can detect any potential data corruption before the actual hardware configuration occurs.

One SSU item that you cannot configure with CSSU is the EMP serial port settings. You can only view these items with CSSU.

Console Redirection Window

The console redirection window displays the server boot process when the CSSU connection to the server is by modem or by LAN. This window cannot accept user input. Its purpose is to help users get more information during a server reboot to the service partition.

After the server completes the reboot to the service partition, the console redirection window closes.

Phonebook

The Client SSU shares a phonebook with DPC. You can use the phonebook to establish connections with supported platforms. Open the phonebook from the Server menu or using the phonebook icon on the toolbar.

CSSU Managers

CSSU includes a set of plug-ins called Managers, which include:

- Multiboot Manager
- Password Manager
- System Event Log (SEL) Manager
- Sensor Data Record (SDR) Manager
- Field Replaceable Unit (FRU) Manager
- System Update Manager with functionality that is system dependent
- Platform Event Manager
- Configuration Save/Restore Manager

You can start each manager from the Services menu or from toolbar icons. Only one version of each manager can be running at a time (for example, you cannot run two instances of the FRU manager). When you start a manager, its menu is added to the CSSU toolbar.

The managers are described briefly in the following sections. For more information about the managers, see the CSSU help.

Multiboot Manager

The Multiboot Manager lets you:

- Set boot device priority.
- Save boot device priority to non-volatile memory.

Password Manager

The Password Manager lets you:

- Set the BIOS system administrator (supervisor) password
- Set the BIOS user password
- Set BIOS security options

System Event Log Manager

The System Event Log (SEL) contains a sequential record of events that have occurred in the remote server. The SEL can help you determine the cause of server system failures. With the SEL Manager you can:

- Examine SEL records by number, timestamp, generator ID, sensor, or event type
- Save SEL records to a file on the local or remote system
- Clear SEL records from the nonvolatile storage area on the server system

For each entry in the System Event Log, the SEL Manager displays:

- A record identifier
- Time stamp information
- The sensor type
- A generator identifier
- The sensor number
- An event description

You can sort the columns in the SEL Manager by clicking the column heading.

Sensor Data Records Manager

The Sensor Data Records (SDR) Manager displays information recorded from each configured sensor in the managed server. Record data is displayed in hexadecimal or binary form. The contents of the SDR file can help determine the cause of server system failures.

Using the SDR Manager, you can:

- Examine Sensor Data Records
- Examine SDRs by Record type
- Save SDRs to a file on the local or remote system

The SDR Manager displays detailed information when you select a specific sensor type in the SDR information tree.

Field Replaceable Unit Manager

The Field Replaceable Unit (FRU) Manager displays a hierarchical tree of FRU components and detailed inventory information for each selected unit. Highlight a component in the tree to see its associated inventory information. The information, based on the Intelligent Peripheral Management Interface (IPMI) specification, includes part numbers, serial numbers, manufacturer's names, version numbers, and asset tag numbers.

The contents of the FRU inventory files can help identify components that may be of interest while troubleshooting a system failure. Using the FRU Manager, you can:

- Examine individual FRU inventory areas
- Save FRU inventory information to a file on the local or remote system

System Update Manager

The System Update Manager lets you update the server BIOS or firmware code for various controllers such as the baseboard management controller (BMC) and hot swap controllers (HSC). The SUM provides the following operations, although not all servers support all types of updates:

- Determines the current revision of system BIOS and firmware on server controllers.
- Updates BIOS and/or firmware.
  - — Updates the system BIOS with a BIOS file (.BIO file).
  - — Updates operational code for controllers using files composed of Hex Format code (.HEX file).
  - — Updates the BIOS and/or firmware using a user-specified Update Information File (.UIF file). The .UIF file lists all the controllers to be updated, the type of update to be done, and the .BIO and .HEX files to be used for the update.
- For controller firmware, verifies the code currently loaded against an external hex file, of either .HEX or .UIF format.

Starting the System Update Manager adds the Update and Verify buttons in the System Update dialog.

Platform Event Manager

The Platform Event Manager provides an interface for configuring Platform Event Paging (PEP), BMC LAN configuration, and viewing the Emergency Management Port (EMP) serial configuration.

Configuration Save/Restore Manager

The Configuration Save/Restore Manager provides a way to save the non-volatile system settings on a server to a file, and allows those settings to be written back into non-volatile storage on a server. These settings include the entire contents of CMOS and ESCD, EMP non-volatile settings, and event paging and filtering non-volatile settings.

7. Glossary

The following terms and abbreviations are used in this document:

Term	Description
CSSU	Client System Setup Utility lets you run SSU remotely from a client
DMI	Desktop Management Interface
DPC	Direct Platform Control
EMP	Emergency Management Port—the serial interface on a server
ESMC	Enterprise Server Management Console, a non-ASMe or third-party management console that can integrate with ASMe software
FRU	Field Replaceable Units
ICMB	Intelligent Chassis Management Bus
IPMI	Intelligent Platform Management Interface
ASMe	Acer Server Manager Enterprise
LDSM	LANDesk Server Manager
MBE	Multiple Bit Error
MIF	Management Information Format, used by DMI for describing component instrumentation
NIC	Network Interface controller—a network access port
NMI	Non-Maskable Interrupt
PIC	Platform Instrumentation Control, which runs on the client system
PI	Platform Instrumentation, which runs on the managed server system
RAID	Redundant Array of Inexpensive Disks
RPC	Remote Procedure Call
SBE	Single Bit Error
SBE	Single-Bit Error
SCSI	A type of bus used to access peripherals such as hard disks
SDR	Sensor Data Records
SEL	System Event Log
SMI	System Management Interrupt
SNMP	Simple Network Management Protocol, a standard network protocol for management information
SSU	System Setup Utility lets you do low-level configuration on a server
SUM	System Update Manager
TCO	Total Cost of Ownership port—a particular network access port on a server

8. Platform Compatibility Matrix

Table 1 lists ASMe features specific to hardware platforms. Columns in the table indicate specific platforms while rows describe specific features.

Table 1. Platform Compatibility Matrix

Board/Chassis	SHG2	SSH4/SRSH4/SPSH4
New Features		
Email Alerts	Y	Y
SMaRT Tool Interface	Y	Y
Alerting-In Band		
ASMe paging	Y	Y
SNMP for Enterprise Sys. Mgt. Consoles	Y	Y
Desktop Management Interface indication	Y	Y
Network alerts (pop-up messages)	Y	Y
Alerting-Out Of Band		
Platform Event Paging	Y	Y
OOB LAN alerts (SNMP traps)	Y	Y
BIOS Console Redirection		
Over modem/serial	Y	Y
Over LAN	Y	Y
Direct Platform Control (DPC) Console Management Plug-In		
Server control	Y	Y
Console redirection	Y	Y
System Event Log manager	Y	Y
Sensor Data Records manager	Y	Y
Field Replaceable Unit manager	Y	Y
Remote Sensor Access manager	Y	Y
Auto answer on modem	Y	Y
Ease of Use		
Online help	Y	Y
Documentation	Y	Y
Java-based GUI	N	N
Fans		
Fan pack-digital	Y	Y
Fan pack-tach	Y	Y
Individual fans-digital	Y	Y
Individual fans-tach	Y	Y
Hot Swapping		
Hot swap disk drives	Y	Y
Hot swap power supply	Y[1]	Y
Hot swap fans	Y	Y

[1] Not available in all SKUs

continued

Table 1. Platform Compatibility Matrix (continued)

Board/Chassis		Altos G900
Industry Design Standards		
IPMI 0.9 compliant	N	N
IPMI 1.0 compliant	N	N
IPMI 1.5 compliant	Y	Y
Monitoring		
Component temperatures	Y	Y
Fan speeds	Y	Y
Baseboard voltage	Y	Y
Baseboard sensors	Y	Y
Chassis intrusion	Y	Y
Drive availability	Y	Y
Power supply health	Y	Y
Power supply redundancy	Y	Y
OOB Emergency Management		
Remote power control (on, off, reset)	Y	Y
Access to non-volatile logs	Y	Y
Remote sensor access	Y	Y
Service partition	Y	Y
OOB Remote Management		
Intelligent Chassis Management Bus	Y	Y
Direct Platform Control over LAN	Y	Y
Command for graceful OS shutdown	Y	Y
Management Consoles Supported		
HP OpenView Network Node Manager 6.1	Y	Y
CA Unicenter Framework TNG 3.0	Y	Y
ASMe Console	Y	Y
Remote Access		
LAN in-band (OS up)	Y	Y
LAN OOB (OS down)	Y	Y
Modem OOB (OS down)	Y	Y
Remote Boot/Access Service Partition		
Over modem/serial	Y	Y
Over LAN	Y	Y
Remote Diagnostics		
OOB hardware confidence tests	Y	Y

continued

Table 1. Platform Compatibility Matrix (continued)

Board/Chassis	SHG2	SSH4/SRSH4/SPSH4
Remote Management (in-band)		
Desktop Management Interface (IA32)[2]	Y	Y
Platform Instrumentation Control[3]	Y	Y
Remote Repair		
FW upgrades	Y	Y
BIOS upgrades	Y	Y
File upload and execution	Y	Y
Security		
CHAP Compliance	Y	Y
Passwords	Y	Y
Service Partition		
Client System Setup Utility (remote access)	Y	Y
DOS shell access (command prompt)	Y	Y
File transfer	Y	Y

[2] Operating Systems include Windows 2000 SP2.

[3] 32-bit Windows Console: Windows 2000 Professional SP2, Windows 2000 Advanced Server SP2, or Windows XP Server.