



Intel® Server Control, Version 3.x

Technical Product Specification

Intel Order Number-A44758-005



Revision 1.4

June 12, 2002

Enterprise Platforms and Services Marketing

Revision History

Date	Revision Number	Modifications
11/10/2000	1.0	Initial release.
12/14/2001	1.3	Updated with Spec Update information and misc corrections
6\12/2002	1.4	Updated with Spec Update information and misc corrections

Disclaimers

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

The Intel Server Control product and / or its components may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Copyright © Intel Corporation 2000-2002. *Other brands and names are the property of their respective owners.

Table of Contents

Section 1: Introduction

1. Introduction to Intel® Server Control (ISC)	1
1.1 Document Scope.....	2
1.1 Document Layout.....	2
1.2 Product Objectives.....	3
2. Architecture	4
2.1 ISC Console.....	4
2.1.1 Direct Platform Control.....	5
2.1.2 System Setup Utility (SSU).....	5
2.1.3 Platform Instrumentation Control (PIC).....	6
2.2 Other Components.....	7
2.2.1 Platform Management Technology.....	7
2.2.2 BMC LAN Alert.....	7
2.2.3 DMI Service Provider.....	8
2.2.4 Simple Network Management Protocol (SNMP).....	8
2.2.5 Platform Event Paging.....	9
2.2.6 Internationalization.....	9
3. Visible Components	10
3.1 Component Features.....	11
3.1.1 Component Management with MIF files and DMI.....	11

Section 2: Platform Requirements

1. Introduction to Platform Requirements	1
2. Console Requirements	2
2.1 Supported Management Consoles.....	2
2.1.1 LANDesk® Server Manager 6.0.....	3
2.1.2 HP OpenView Network Node Manager for Windows NT.....	3
2.1.3 CA-Unicenter TNG.....	3
2.1.4 Stand-Alone ISC Console.....	4
2.2 Supported Console Hardware Configurations.....	4

3. Managed Server Requirements	5
3.1 Novell NetWare* Requirements.....	5
3.2 Windows 2000*/NT* Requirements	5
3.2 Red Hat* Linux* Requirements.....	5
3.3 SCO UnixWare* 7 Requirements	6
3.4 Additional Requirements for DMI-SNMP Translation.....	6

Section 3: Standalone Console

1. Introduction to Standalone Console	1
2. Standalone Console Menu Items.....	2
2.1 Main Menu	2

Section 4: Direct Platform Control

1. Introduction to Direct Platform Control (DPC)	1
2. Console Manager.....	3
3. Server Configuration	5
4. Security	6
5. Making a Connection.....	7
6. Console Redirection	8
7. DPC Plug-ins.....	9
7.1 Server Control	9
7.2 SEL Viewer	9
7.3 SDR Viewer.....	9
7.4 FRU Viewer.....	9
7.5 RSA Manager.....	9
8. Reboot from Service Partition	10
8.1 Run DOS/EFI Shell	11
8.2 Run Program...	12
8.3 Run Diagnostics	12
8.4 File Transfer.....	13
8.4.1 Upload.....	13
8.4.2 Download...	14
8.5 Redirection View	14

8.6	Configuration Status.....	15
9.	Modes of Operation	17
9.1	EMP Mode	17
9.2	Redirect Mode.....	17
9.3	PPP Mode	17
9.4	PPP-Redirect Mode.....	17
10.	DPC User Interface	18
10.1	EMP Mode	18
10.1.1	Main Window	18
10.1.2	View Menu	31
10.1.3	Window Menu	32
10.1.4	Help Menu.....	32
10.2	Connection Menu.....	34
10.2.1	Connect Dialog – LAN or Direct	34
10.2.2	Phonebook Dialog.....	35
10.2.3	Add Phonebook Entry	36
10.2.4	Modify Phonebook Entry	37
11.	Supported Features.....	38
11.1	Toolbar Buttons.....	38

Section 5: Service Partition

1.	Introduction to the Service Partition	1
2.	Service Partition Boot	2
2.1	Firmware / BIOS Service Boot Support	2
2.2	BIOS Setup Partition Type Configuration	3
2.3	Remotely Initiating Service Partition Boot.....	3
2.4	Local Boot from Service Partition	3
3.	Service Partition Installation.....	4
3.1	SCAN and PRESENT Bits.....	4
4.	Service Partition Operating System	5
4.1	Service Partition OS Installation	5
4.2	Service Partition OS / Country Kit CD Hidden Partition Support.....	5
4.3	Service Partition OS Initialization.....	5

Section 6: Diagnostic Test Package

1. Introduction to the Diagnostic Test Package	1
2. Remote Diagnostics	2
3. Test Descriptions.....	3
3.1 Processor FRU Tests	3
3.2 Baseboard FRU Tests.....	3
3.3 Memory FRU Tests	5
3.4 Hard Disk Drive FRU Tests	5
3.5 Floppy Disk Drive FRU Tests	6
3.6 SCSI CD-ROM Drive FRU Tests	6
3.7 Hot-Swap SCSI Backplane FRU Tests.....	6
3.8 Front Panel Enclosure FRU Tests	7
3.9 Power Share Backplane FRU Tests	7
4. Test Selection Menu Display.....	8
5. DiagWiz Hardware Configuration (dwizcfg.exe).....	9
5.1 DiagWiz Display FRU Status.....	9
6. Server Test Package.....	11
6.1 Test Packages	11
6.1.1 Quick Test	11
6.1.2 Comprehensive Tests.....	12
6.1.3 Comprehensive Tests with Continuous Looping	12
7. Test List.....	13

Section 7: Client System Setup Utility

1. Introduction to the Client System Setup Utility (CSSU) Application.....	1
2. Client Application Framework	3
2.1 Command Line Options.....	3
2.2 Initialization Files	3
3. CSSU Graphical User Interface.....	4
3.1 Main Menu Options	5
3.1.1 File Menu	5
3.1.2 Edit Menu	5

3.1.3	View Menu	5
3.1.4	Server Menu	6
3.1.5	Services Menu	6
3.1.6	Window Menu	7
3.1.7	Help Menu	7
3.1.8	Tool Bar	8
3.1.9	Status Bar	8
3.2	Phonebook Dialog Options	9
3.2.1	Add Phonebook Entry and Modify Phonebook Entry Dialogs	10
3.3	Connection Dialog Options	11
4.	Console Redirection Feature	12
4.1	The SSU Console Redirection Window	12
5.	Add-in Components	14
5.1	Resource Configuration Manager (RCM) Add-in	14
5.1.1	Device Window	15
5.1.2	System Resource Usage Window	16
5.2	Multiboot Manager (MBM) Add-in	18
5.2.1	User Interface / Operation	18
5.3	Password Manager (PWM) Add-in	19
5.3.1	Initialization Files	19
5.3.2	User Interface / Operation	19
5.4	System Event Log Add-In	22
5.4.1	Initialization Files	22
5.4.2	Internationalization	22
5.4.3	User Interface / Operation	22
5.5	Sensor Data Record Manager Add-In	22
5.5.1	Initialization and Customization Files	22
5.5.2	User Interface / Operation	22
5.6	Field Replaceable Unit Manager Add-In	22
5.6.1	Initialization Customization Files	22
5.6.2	User Interface / Operation	23
5.7	System Update Manager Add-in	23
5.8	Platform Event Manager Add-in	23
5.9	Configuration Save / Restore Manager Add-in	23

6. System Update Manager Add-in Component.....	24
6.1 Initialization Files	24
6.2 Internationalization	24
6.3 User Interface / Operation	24
6.3.1 Confirmation Dialog	26
6.4 Recovery Agent.....	26
6.4.1 General Update Process.....	27
7. Platform Event Manager Add-in Component	30
7.1 Initialization Files	30
7.2 Internationalization	30
7.3 User Interface / Operation	30
7.3.1 Platform Event Manager Window	30
7.3.2 Platform Event Paging Dialog	31
7.3.3 BMC LAN-Alert Dialog	32
7.3.4 Platform Event Action Dialogs	34
7.3.5 Emergency Management Port Dialog	35
8. Configuration Save/Restore Manager Add-in Component.....	36
8.1 Initialization Files	36
8.2 Internationalization	36
8.3 User Interface / Operation	36
8.3.1 CSR Main Window.....	36
8.3.2 Configuration Data.....	37

Section 8: Platform Instrumentation Control

1. Introduction to Platform Instrumentation Control (PIC)	1
2. Platform Instrumentation	2
2.1 Local Response Agent	3
3. PIC Graphical User Interface	4
3.1 Main Menu	5
3.1.1 File Menu	6
3.1.2 View Menu	6
3.1.3 Configure Menu	7
3.1.4 ICMB Menu.....	7
3.1.5 Help Menu	8

3.2	Toolbar.....	8
3.3	Navigation Pane.....	10
3.3.1	Health.....	10
3.4	Presentation Pane.....	12
3.4.1	Group Information.....	12
3.5	LCD Display.....	16
3.6	Status Bar.....	17
3.7	Popup Menus.....	18
3.7.1	Presentation Pane Popup Menu.....	18
3.7.2	Toolbar Popup Menu.....	19
3.7.3	LCD Popup Menu.....	19
3.7.4	Status Bar Popup Menu.....	19
4.	Individual Sensor / Server Information.....	20
4.1	Sensor Settings Tab Page.....	21
4.1.1	Threshold Values Rounded Off.....	22
4.1.2	Avoiding a Reboot-Fail Retry Loop.....	22
4.2	Sensor Status Tab Page.....	23
4.3	Alert Actions Tab Page.....	24
4.3.1	Avoiding a Power On/Off Loop.....	27
4.4	Sensor Information Tab Page.....	27
4.5	Inventory Information Tab Page.....	28
5.	PIC Dialogs.....	30
5.1	Options Dialog.....	30
5.2	Restoring Factory Defaults Dialog.....	31
5.3	Watchdog Timer Dialog.....	31
5.4	Paging Configuration Dialog.....	32
5.5	ICMB Configuration Dialog.....	34
5.6	ICMB Remote Server(s) Dialog.....	35
6.	Sensor Controls.....	37
6.1	Chassis.....	37
6.2	Fan 39.....	
6.3	Memory Array.....	40
6.4	Memory Device.....	41
6.5	PCI Hot Plug Device.....	43

6.6	Power Supply	44
6.7	Power Unit.....	45
6.8	Processor.....	46
6.9	System Information	47
6.9.1	Field Replaceable Unit (FRU)	48
6.9.2	Operating System	49
6.9.3	System BIOS	50
6.9.4	System Event Log (SEL).....	51
6.10	System Slots	52
6.11	Temperature	54
6.12	Third Party Instrumentation.....	56
6.13	Voltage.....	59

Section 9: ICMB

1.	Intelligent Chassis Management Bus (ICMB)	1
1.1	ICMB	1
1.1.1	Setting Up an ICMB Connection	1
1.1.2	Configuring the Management Point Server	2
1.2	Setting Up ICMB.....	2
1.2.1	Discovering Remote ICMB Systems	3
1.2.2	Viewing and Managing Viewing Remote ICMB Systems.....	4

Section 10: Platform Event Paging

1.	Platform Event Paging (PEP) Overview	1
2.	Page Configuration.....	3
2.1	Platform Event Manager Add-In	3
2.1.1	Platform Event Manager Window	3

Section 11: LAN Alerting

1.	Introduction to LAN Alerting	1
2.	Hardware Interface	2
3.	Configuration	3
4.	Client Address Resolution	5

5. Platform Event Filtering and LAN Alert	6
5.1 Event Record Data	6
6. SNMP Trap Format Used for LAN Alerts	8
6.1 Header	8
6.2 Protocol Data Unit (PDU)	8
6.3 Variable Bindings Field.....	9
7. LAN-Alert Sequence	11
8. LAN-Alert Viewer	12
8.1 Alert Viewer	12
8.2 Program Menu	13
8.3 Tray Status Reporting Icon.....	14
8.4 View Details Dialog	14
8.5 Configure Dialog	15

Section 12: Install / Uninstall

1. Introduction to Install and Uninstall	1
2. Supported Operating Systems	2
3. Internationalization	3
4. Recommended Files and Registry Tree Structures	4
4.1 Source Files	4
4.2 Windows Registry	4

Section 13: Common Interface

1. Introduction to the Common Interface	1
1.1 ISC Instrumentation Controls	1
1.2 ISC Core Components	1
1.3 DMI Managed Object Toolkit (MOT) Engine.....	2
1.4 DMI Managed Object Toolkit (MOT) Engine.....	2
1.5 Navigator Container	2
2. FRU Implementation	3
2.1 Screen Display	3
2.1.1 Navigation Pane	3
2.1.2 Presentation Pane	4

2.1.3	Description.....	4
2.1.4	Container Functionality	5
2.1.5	Supported Commands.....	5
2.2	Available FRU Information.....	6
3.	SDR Implementation.....	7
3.1	Screen Display	7
3.2	Navigation Pane	7
3.2.1	Display Name Rules for Sensor Record.....	7
3.3	Presentation View	8
3.4	Description	9
3.5	Container Functionality.....	10
3.5.1	Supported Commands	10
4.	SEL Implementation	12
4.1	Screen Display	12
4.2	Viewer	12
4.3	Container Functionality.....	13
4.3.1	Supported Commands.....	13
4.4	Available Information.....	14
5.	RSA Implementation.....	15
5.1	Screen Display	15
5.2	Available Information.....	16

Section 14: Security

1.	Introduction to Security	1
2.	Security Implementation	2
2.1	Platform Instrumentation	2
2.1.1	New Authentication Scheme	2
2.1.2	LRA Notification-Only Control	2
2.1.3	SNMP Read-only Access Control	3
2.2	DPC/CSSU Security.....	3
2.3	LAN Based Security (IP Filtering).....	3
2.4	Invalid Password Handling	3
2.5	Session Expiration.....	3
2.6	Setup.....	4

2.7 Password Length and Character-set Support..... 4

Appendix A: ISC 3.5 Update

ISC 3.5 Update I

Compliance with IPMI 1.5 I

 Korean GUI Translation II

 DPC Status Configuration Dialog Enhancements II

 Removal of Service Partition Remote Diagnostics V

 Defeature of CSSU SUA Remote BIOS Update..... V

 DPC over LAN Access / CSSU over LAN Access V

Appendix B: Summary Errata Table

Summary Errata Table I

 Application Errata..... I

 Documentation Changes.....XX

List of Figures

Section 1: Introduction

Figure 1 - 1: Intel® Server Control Components	10
--	----

Section 2: Platform Requirements

No figures appear in this section.

Section 3: Standalone Console

Figure 3 - 1: ISC Standalone Screen.....	1
--	---

Section 4: Direct Platform Control

Figure 4 - 1: Direct Platform Control Components.....	2
Figure 4 - 2: DPC Console Manager	3
Figure 4 - 3: DOS Shell Window	11
Figure 4 - 4: Run Program Dialog.....	12
Figure 4 - 5: Upload Dialog	13
Figure 4 - 6: Download Dialog	14
Figure 4 - 7: Configuration Status - Capabilities Screen.....	15
Figure 4 - 8: Configuration Status - Status Screen	16
Figure 4 - 9: Configuration Status - EMP Status Screen	16
Figure 4 - 10: DPC Main Window	19
Figure 4 - 11: Power On Server Dialog - Serial Connection.....	23
Figure 4 - 12: Power On Dialog	24
Figure 4 - 13: Reset with a Serial Connection	24
Figure 4 - 14: Reset Server Dialog - LAN Connection	25
Figure 4 - 15: DOS Shell Window.....	26
Figure 4 - 16: Run Program Dialog.....	27
Figure 4 - 17: Upload Dialog	28
Figure 4 - 18: Download Dialog	29
Figure 4 - 19: Configuration Status - Capabilities Screen.....	31

Figure 4 - 20: Configuration Status - Status Screen	31
Figure 4 - 21: Configuration Status - EMP Configuration Screen	32
Figure 4 - 22: Help Topics Window	35
Figure 4 - 23: About the DPC Console Manager Dialog	35
Figure 4 - 24: Connect Dialog - LAN	36
Figure 4 - 25: Connect Dialog - Direct	36
Figure 4 - 26: Phonebook Dialog	37
Figure 4 - 27: Add Phonebook Entry	38
Figure 4 - 28: Modify Phonebook Entry	39

Section 5: Service Partition

Figure 5 - 1: Service Partition	1
---------------------------------------	---

Section 6: Diagnostic Test Package

Figure 6 - 1. Service Partition-based Remote Diagnostics	2
Figure 6 - 2. Execution of the Testmenu.bat File	8
Figure 6 - 3. DiagWiz Test Configuration Screen Display	9
Figure 6 - 4. DiagWiz FRU Status Display	10

Section 7: Client System Setup Utility

Figure 7 - 1. System Setup Utility Framework	2
Figure 7 - 2. Client Main Window	4
Figure 7 - 3. Phonebook Dialog	9
Figure 7 - 4. Add Phonebook Entry Dialog	10
Figure 7 - 5. Connect Dialog	11
Figure 7 - 6. Console Redirection Window during Server Reboot	12
Figure 7 - 7. Console Redirection Window - MDI Child Window	13
Figure 7 - 8. Resource Configuration Main Window	14
Figure 7 - 9. Device Window	15
Figure 7 - 10. System Resource Usage Window	17
Figure 7 - 11. Multiboot Manager Main Window	18
Figure 7 - 12. Password Manager Main Window	20

Figure 7 - 13. System Update Manager Main Window	25
Figure 7 - 14. SUM Verify Operation Confirmation Dialog	26
Figure 7 - 15. Platform Event Manager Main Window	30
Figure 7 - 16. Platform Event Paging Dialog	31
Figure 7 - 17. BMC LAN-Alerting Dialog.....	32
Figure 7 - 18. Platform Event Action Dialogs.....	34
Figure 7 - 19. Emergency Management Port Dialog.....	35
Figure 7 - 20. CSR Manager Main Window	36

Section 8: Platform Instrumentation Control

Figure 8 - 1: Platform Instrumentation Control and Platform Instrumentation	2
Figure 8 - 2: PIC Container	4
Figure 8 - 3: Main Menu	5
Figure 8 - 4: Toolbar.....	8
Figure 8 - 5: PIC Main Dialog, Toolbar Hidden	9
Figure 8 - 6: Navigation Pane.....	10
Figure 8 - 7: Health View in Main Dialog.....	11
Figure 8 - 8: Presentation Pane, Large Icon View	12
Figure 8 - 9: Presentation Pane, Small Icon View	13
Figure 8 - 10: Presentation Pane, List View	13
Figure 8 - 11: Presentation Pane, Detail View.....	14
Figure 8 - 12: Arrange Icons by Name, List Icon View.....	15
Figure 8 - 13: Arrange Icons by Status, List Icon View	16
Figure 8 - 14: LCD Display Pane.....	17
Figure 8 - 15: Managed Server without LCD, or LCD Hidden.....	17
Figure 8 - 16: Status Bar	18
Figure 8 - 17: PIC Main Dialog, Status Bar Hidden	18
Figure 8 - 18: Presentation Pane Popup Menu.....	19
Figure 8 - 19: Toolbar Popup Menu.....	19
Figure 8 - 20: LCD Popup Menu.....	19
Figure 8 - 21: Status Bar Popup Menu	20
Figure 8 - 22: Tab Pages in Presentation Pane.....	21
Figure 8 - 23: Sensor Settings Tab Page	22
Figure 8 - 24: Sensor Status Tab Page	24

Figure 8 - 25: Alert Actions Tab Page	26
Figure 8 - 26: Sensor Information Tab Page	29
Figure 8 - 27: Inventory Information Tab Page	30
Figure 8 - 28: Options Dialog	31
Figure 8 - 29: PIC Watchdog Timer Dialog.....	33
Figure 8 - 30: Paging Configuration.....	33
Figure 8 - 31: ICMB Configuration Dialog.....	35
Figure 8 - 32: ICMB Remote Server(s) Selection Dialog	36
Figure 8 - 33: PIC Main Dialog, Managing a Remote Server via ICMB.....	37
Figure 8 - 34: Chassis Sensor Status	39
Figure 8 - 35: Fan Sensor Settings.....	40
Figure 8 - 36: Memory Array Sensor Status	41
Figure 8 - 37: Memory Device Sensor Status	43
Figure 8 - 38: PCI Hot Plug Device Sensor Information	44
Figure 8 - 39: Power Supply Sensor Status.....	45
Figure 8 - 40: Power Unit Sensor Status	46
Figure 8 - 41: Processor Sensor Status	47
Figure 8 - 42: Field Replaceable Unit (FRU) Inventory Information	49
Figure 8 - 43: Operating System Information.....	50
Figure 8 - 44: System BIOS Information.....	51
Figure 8 - 45: System Event Log Information	52
Figure 8 - 46: PHP System Slots Sensor Information.....	53
Figure 8 - 47: Non-PHP System Slots Sensor Information	54
Figure 8 - 48: Temperature Sensor Settings	55
Figure 8 - 49: Third Party Alert Actions	57
Figure 8 - 50: Voltage Sensor Settings.....	60

Section 9: ICMB

Figure 9 - 1: Enabling ICMB Features	4
Figure 9 - 2: Viewing Remote Servers via ICMB.....	5
Figure 9 - 3: Displaying Remote Server Information.....	5

Section 10: Platform Event Paging

Figure 10-1. Platform Event Manager Main Window	3
Figure 10-2. Platform Event Paging Dialog	4
Figure 10-3. Platform Event Action Dialogs.....	6

Section 11: LAN Alerting

Figure 11 - 1: Hardware Interface.....	2
Figure 11 - 2: IP-UDP Packet in Ethernet Network.....	5
Figure 11 - 3: LanAlert Viewer.....	12
Figure 11 - 4: Windows Program Menu.....	13
Figure 11 - 5: Status Icon.....	14
Figure 11 - 6: LanAlert Viewer - Alert Details.....	14
Figure 11 - 7: LanAlert Configuration	15
Figure 11 - 8: Alert Notification Dialog.....	15

Section 12: Install / Uninstall

No figures appear in this section.

Section 13: Common Interface

Figure 13 - 1: FRU Manager	3
Figure 13 - 2: SDR Grid.....	9
Figure 13 - 3: SDR Properties Dialog	11
Figure 13 - 4: SEL Manager.....	12
Figure 13 - 5: SEL Properties Dialog.....	14
Figure 13 - 6: RSA Manager Options Dialog	15
Figure 13 - 7: RSA Manager - View 1.....	16
Figure 13 - 8: RSA Manager - View 2.....	16

Section 14: Security

No figures appear in this section.

List of Tables

Section 1: Introduction

No tables appear in this section.

Section 2: Platform Requirements

Table 2 - 1: PIC Command-line Parameters..... 2

Section 3: Standalone Console

No tables appear in this section.

Section 4: Direct Platform Control

Table 4 - 1: Run Program - Options	12
Table 4 - 2: Upload Dialog - Options	13
Table 4 - 3: Download Dialog – Options	14
Table 4 - 4: File Menu - Options	21
Table 4 - 5: Connect Menu Options.....	22
Table 4 - 6: Power On with a Serial Connection Options.....	23
Table 4 - 7: Power On with a LAN Connection Options	24
Table 4 - 8: Reset with a Serial Connection Options	25
Table 4 - 9: Reset with a LAN Connection.....	25
Table 4 - 10: Run Program Dialog - Options	27
Table 4 - 11: Upload Dialog - Options	29
Table 4 - 12: Download Dialog - Options.....	30
Table 4 - 13: Connect Dialog - Options	37
Table 4 - 14: Phonebook Dialog - Options.....	38
Table 4 - 15: Add Phonebook Entry - Options	38
Table 4 - 16: Modify Phonebook Entry - Options	39
Table 4 - 17: DPC Console - Supported Features	40
Table 4 - 18: Toolbar Buttons.....	40
Table 4 - 19: DPC Status Bar Information	41

Section 5: Service Partition

No tables appear in this section.

Section 6: Diagnostic Test Package

Table 6 - 1: Processor FRU Tests	3
Table 6 - 2: Baseboard FRU Tests	3
Table 6 - 3: Memory FRU Tests	5
Table 6 - 4: Hard Disk Drive FRU Tests	5
Table 6 - 5: Floppy Disk Drive FRU Tests	6
Table 6 - 6: SCSI CD-ROM Drive FRU Tests	6
Table 6 - 7: Hot-Swap SCSI Backplane FRU Tests	6
Table 6 - 8: Front Panel Enclosure FRU Tests	7
Table 6 - 9: Power Share Backplane FRU Tests	7
Table 6 - 10: Diagnostics Test List	13

Section 7: Client System Setup Utility

Table 7 - 1: Command Line Options	3
Table 7 - 2: CSSU Tool Bar Options	8
Table 7 - 3: Phonebook Dialog Options	9
Table 7 - 4: Add Phonebook Entry Dialog Options	10
Table 7 - 5: Connect Dialog Options	11
Table 7 - 6: Resource Configuration Manager Options	15
Table 7 - 7: Device Window Options	16
Table 7 - 8: System Resource Usage Window Options	17
Table 7 - 9: Multiboot Manager Main Window Options	19
Table 7 - 10: Password Manager Main Window Options	20
Table 7 - 11: System Update Manager Main Window Options	25
Table 7 - 12: Checkpoint File Format	29
Table 7 - 13: Platform Even Manager Main Window Options	31
Table 7 - 14: Platform Event Paging Options	32
Table 7 - 15: BMC LAN-Alert Dialog Options	33

Table 7 - 16: Platform Event Action Dialog Options.....	34
Table 7 - 17: Emergency Management Port Dialog Options.....	35
Table 7 - 18: CSR Manager Main Window Options	37

Section 8: Platform Instrumentation Control

Table 8 - 1: View Menu Options	6
Table 8 - 2: Toolbar Options.....	8
Table 8 - 3: Audio and Visual Notifications	27
Table 8 - 4: Shutdown and Power Control Actions	27

Section 9: ICMB

No tables appear in this section.

Section 10: Platform Event Paging

No tables appear in this section.

Section 11: LAN Alerting

Table 11 - 1: SEL Event Record (Type 02h) Format	6
Table 11 - 2: Trap PDU format used by LAN-Alert per RFC 1157	8
Table 11 - 3: Variable Bindings Fields	9
Table 11 - 4: LanAlert Viewer - User Controls	13
Table 11 - 5: Configure Dialog - Options	15

Section 12: Install / Uninstall

No tables appear in this section.

Section 13: Common Interface

Table 13 - 1: Presentation Pane Information Available.....	4
Table 13 - 2: FRU Manager File Commands.....	5
Table 13 - 3: Available FRU Information.....	6

Table 13 - 4: SDR Tree View Details..... 8
Table 13 - 5: SDR Grid Fields 9
Table 13 - 6: SDR Menu - Supported Commands 10
Table 13 - 7: SEL Menu - Supported Commands..... 13

Section 14: Security

Table 14 - 1: ASCII Character Codes Supported by the DPC Password 3

Intel® Server Control, Version 3.x TPS

Section 1: Introduction

Table of Contents

1. Introduction to Intel® Server Control (ISC)	1
1.1 Document Scope.....	2
1.1 Document Layout	2
1.2 Product Objectives	3
2. Architecture	4
2.1 ISC Console	4
2.1.1 Direct Platform Control	5
2.1.2 System Setup Utility (SSU)	5
2.1.3 Platform Instrumentation Control (PIC)	6
2.2 Other Components.....	7
2.2.1 Platform Management Technology	7
2.2.2 BMC LAN Alert	7
2.2.3 DMI Service Provider	8
2.2.4 Simple Network Management Protocol (SNMP)	9
2.2.5 Platform Event Paging	9
2.2.6 Internationalization.....	9
3. Visible Components	10
3.1 Component Features.....	11
3.1.1 Component Management with MIF files and DMI.....	11

List of Figures

Figure 1 - 1: Intel® Server Control Components 10

List of Tables

No tables appear in this section.

1. Introduction to Intel® Server Control (ISC)

Intel® server systems are designed with a number of integrated hardware components that help the network administrator with server management functions. Intel Server Control v3.x is a server management tool that provides real time monitoring and alerting for server hardware sensors. ISC is implemented as client-server architecture.

The Server Manager Console (client) provides the graphical user interface for the instrumented components on the managed server (server). ISC uses the standard Desktop Management Interface (DMI) 2.0 framework for managing Intelligent Platform Management Interface (IPMI) hardware components.

The agents that provide information on the status of the server components are located on each managed server. Remote Access Protocol (RAP) or Remote Procedure Call (RPC) provides the communication between the console and the managed servers.

RAP (used with DMI 1.0) uses the Internetwork Packet Exchange (IPX) transport protocol for communications to a Novell NetWare* Server and IP (or IPX) for communications to a Windows* NT* server. RPC (used with DMI 2.0) is used to allow ISC-based components to communicate between the console applets and the managed server instrumentation.

ISC is bundled with Intel server systems to provide a differentiated management solution. It consists of a set of components that address multiple server states and access paths. The state of the server can be 'powered off', 'Operating System (OS) not operational' or 'OS operational'. The access path to the server can be Local Area Network (LAN), modem, or direct connect. The design of ISC is motivated by the following goals:

- One integrated solution for remote management of servers over LAN, modem and serial communications.
- A single 'look and feel' for all Enterprise Server Group (ESG) server management software.
- A single installation framework.
- Modular components for easy integration into existing Original Equipment Manufacturer (OEM) management stacks, with well-documented interface points for OEM integration and extensibility.
- The ability for each component within ISC to snap into selected Enterprise System Management Consoles (HP Openview*, CA Unicenter* TNG*), as well as the LANDesk® Server Manager workgroup management console.
- Support for standalone execution and execution within the Microsoft Management Console and web browsers (Internet Explorer* and Netscape Navigator*) for each component (Platform Instrumentation Control, Direct Platform Control, Client System Setup Utility, etc).

1.1 Document Scope

This Technical Product Specification (TPS) describes the architecture and features of Intel Server Control v3.x. It also provides an overview of the installation process and presents a description of the ISC Graphical User Interface (GUI), which encompasses Platform Instrumentation Control (PIC), Platform Instrumentation (PI), Direct Platform Control (DPC), Remote Diagnostics, and Client System Setup Utility (CSSU).

This document is not an installation guide. It should not be used as product instructions.

1.1 Document Layout

This document is organized as follows:

- **Section 1, Introduction:** An overview of the architecture and components of ISC.
- **Section 2, Platform Requirements:** Console and Managed Server hardware / operating system requirements; supported Enterprise System Management Consoles
- **Section 3, ISC Standalone Console:** Operating ISC without an Enterprise System Management Console
- **Section 4, Direct Platform Control:** Architecture and operation and user interface for the Direct Platform Control application within the ISC product.
- **Section 5, Service Partition:** Architecture and operation of the Service Partition and Service Partition boot
- **Section 6, Diagnostic Test Package:** Description of available off-line diagnostic tests and the Diagnostic Wizard
- **Section 7, Client System Setup Utility:** Description of the setup information visible and server system configuration options that can be managed from the console workstation.
- **Section 8, Platform Instrumentation Control:** Description of alerts that can be set and server statuses that can be viewed from the console.
- **Section 9, Intelligent Chassis Management Bus (ICMB):** Definition of the Intelligent Chassis Management Bus.
- **Section 10, Platform Event Paging:** Description of the paging feature and the events for which pages may be generated
- **Section 11, Local Area Network (LAN) Alerting:** Description of the LAN notification procedure, which sends alerts for critical system failures to the remote system administrator.
- **Section 12, ISC Install and Uninstall:** Description of the install and uninstall process, including registry changes
- **Section 13, Common Interface for FRU, SDR, and SEL:** The graphical user interface for the Field Replaceable Unit (FRU), Sensor Data Records (SDR), and System Event Log (SEL) viewers.
- **Section 14, Security:** Description of ISC security procedures, including a method of authentication.

1.2 Product Objectives

The primary objectives of ISC V3.x are as follows:

- Deliver industry-leading management solutions for ESG platforms.
- Develop and deliver standards based server management-building blocks that reduce Total Cost of Ownership (TCO).
- To improve management capabilities provided by ISC for Intel Architecture (IA) platforms.

2. Architecture

The primary components of ISC can be broken down as follows:

ISC Console

- Direct Platform Control
 - Service Partition
 - Service Partition Boot
 - Remote Diagnostics
 - Configuration Utilities
- System Setup Utility (SSU)
 - Local SSU
 - Client SSU
- Platform Instrumentation Control
 - Platform Instrumentation
 - ICMB
 - Local Response Agent (LRA)
- LRA Paging

Other Components

- Platform Management Technology
- Platform Event Paging (PEP)
- Management Console Integration
- Internationalization

These components are introduced briefly in the following sections and are discussed in detail later in this specification.

2.1 ISC Console

The ISC Console consists of the software portion of the architecture that is installed at the workstation or Windows NT server. This is used to manage the server. The ISC Console interacts with Enterprise System Management Consoles, or it can be used as a “stand-alone” application, using a web browser or Microsoft Management Console.

2.1.1 Direct Platform Control

Direct Platform Control is an application that provides emergency and out-of-band management access to the server, using a LAN, modem, or a direct serial line connection. DPC provides a user-friendly interface for monitoring and controlling the platform management features of the system. DPC consists of a Windows 32* GUI that communicates directly to the Platform Management Technology resident on the server.

DPC shares the on-board Emergency Management Port (EMP) hardware with the server operating system. Since DPC does not communicate with the server-resident operating system, it can be used to manage the server even if the operating system and the primary processors of the server are not operational. Because the platform-resident support for DPC is available on 5-V standby, DPC can be used to communicate with and control a powered down server.

2.1.1.1 Service Partition

The Service Partition is a special partition on the system drive that is based on ROM-DOS*. It may contain the SSU, Diagnostics, or other American National Standard Institute (ANSI) text-based DOS programs.

The Service Partition provides a standard communication stack. It can be used over a modem or a serial port in a multitasking environment to support remote control of SSU, diagnostics, or any other utility that is designed to be compatible with this environment. The Service Partition also supports the redirection of a text-based console over all of the supported communication paths.

2.1.1.2 Service Partition Boot

Using the capabilities provided by Direct Platform Control on the console and the Platform Management Technology on the server, the management console makes a LAN or modem connection to a target server, regardless of the operational state of the target server. The console can then instruct the target server to be booted from the Service Partition.

2.1.1.3 Remote Diagnostics

Remote Diagnostics are a set of diagnostics tools, based on the Modular Test Architecture (MTA) diagnostics, that are commonly used during factory testing. These diagnostics are located on the Service Partition and are run using DPC.

2.1.1.4 Configuration Utilities

The configuration utilities are comprised of SSU and BIOS Setup. BIOS Setup is accessible through DPC while the Local SSU is accessed through the Client SSU interface.

2.1.2 System Setup Utility (SSU)

The System Setup Utility provides a system level view of the server including the system resource configuration, multi-boot configuration, password setups, System Event Log manager, Field Replaceable Unit manager, and Sensor Data Record manager.

2.1.2.1 Local SSU

The Local SSU allows the user to perform configuration tasks at the server instead of performing the tasks remotely, at a console.

2.1.2.2 Client SSU

The CSSU interface consists of a Windows 32 graphical user interface resident on a console workstation. This communicates with the SSU agents and framework resident on the Service Partition at the server.

2.1.3 Platform Instrumentation Control (PIC)

Platform Instrumentation Control is a server management tool that provides real time monitoring and alerting for server hardware sensors. PIC consists of a Windows 32 graphical user interface that communicates to the platform instrumentation resident on the server. PIC is designed to dynamically detect and display the management capabilities of ESG platforms.

2.1.3.1 Platform Instrumentation

Platform Instrumentation consists of all of the server-resident software required for monitoring and controlling the server when the operating system is on-line. The core instrumentation is implemented as platform instrumentation under the DMI 2.0 management framework.

2.1.3.2 Intelligent Platform Management Bus (ICMB)

The ICMB protocol is used for inter-chassis communications. In other words, it provides a way for intelligent devices on the Intelligent Platform Management Bus (IPMB) in one chassis to communicate with intelligent devices on the IPMB in another chassis. This is possible because the server provides two ICMB connectors so multiple servers can be daisy chained together.

The ICMB provides additional troubleshooting and status capabilities by providing information that can be used to predict and identify failures on multiple servers. It is used to provide remote power control and status information on servers that cannot be normally obtained through in-band channels.

2.1.3.3 Local Response Agent (LRA)

Event responses are directed from the Local Response Agent (LRA). This agent, running on the managed server, is capable of receiving DMI indications from the baseboard, and from several on-board devices: Adaptec* and Symbios* SCSI, AMI* RAID, and the Intel[®] PRO 100™ LAN adapter instrumentation software. It can also perform autonomous local control actions, such as powering down the server.

2.1.3.4 LRA Paging

The LRA uses the DMI interface to trigger a paging action, which will be performed by the Baseboard Management Controller (BMC). PIC allows configurations of the paging feature via modification of the data in the DMI group.

2.2 Other Components

2.2.1 Platform Management Technology

All ISC components rely on a foundation of hardware and firmware support supplied by the Platform Management Technology. The core parts of this technology are:

- Intelligent Platform Management Interface (IPMI) – This is the core protocol used by the firmware management controllers to communicate to each other and to the platform instrumentation software.
- Intelligent Platform Management Bus (IPMB) – This is a set of specifications that define how the firmware management controllers communicate on the local platform Management Bus.
- Intelligent Chassis Management Bus Bridge (ICMB) – This is a set of specifications that define how the firmware management controllers communicate with the remote chassis / system connected to the Management Bus.
- Platform BIOS – The system BIOS on the platform provides functionality to configure and control the system management aspects of the system during the pre-OS Boot State.
- Emergency Management Port (EMP) – This hardware support allows for remote access of the system during various stages of system operation, including the times when the system is powered off.
- Platform Event Paging – This feature allows a firmware based paging capability on the platform.

2.2.2 BMC LAN Alert

The BMC LAN Alert capability is built into the Platform Management Technology. This feature allows the platform to proactively alert the system administrator of critical system failures and state changes, independent of the state of the operating system or the server management software running on the host operating system. BMC LAN Alert causes the platform management controllers to generate a Simple Network Management Protocol (SNMP) trap and send it to a target management station or broadcast it to a specified subnet, using the Universal Datagram Packet/ Internet Protocol (UDP/IP) protocol via a regular LAN connection.

When the system administrator is notified by an alert, the ISC software can be used to remotely view server the health / status, system logs, and current configuration; reconfigure, reset or power off or on the server; or execute off-line diagnostics to further analyze the condition of the server. The available functionality depends on the availability of the ISC tools (PIC, DPC, etc.) based on the current server state.

The format of the traps generated by the BMC LAN Alert feature is based on the standard Platform Event Trap (PET) format approved by the Wired-for-Management (WfM) 2.0 specifications.

Traps can be configured for the following events:

- Temperature Sensor out of range
- Voltage Sensor out of range
- Chassis Intrusion (Security Violation)
- Power Supply Fault
- BIOS: Uncorrectable Error Correcting Code (ECC) error
- BIOS: Power On Self Test (POST) Error Code
- Boot Failures (Note: The page will be repeated for each successive processor boot failure until the log limit is reached.)
- Fatal Non-Maskable Interrupt (NMI) (from source other than Front Panel NMI or Uncorrectable ECC Error)
- Watchdog Timer reset, power down, or power cycle
- System restart (reboot)
- Fan failures

The BMC LAN Alert feature has the ability to generate traps during pre-boot and post-boot states, provided that the BMC is functional and there is power to the system.

The BMC maintains a table of up to 16 entries for all event filters. The BMC generates a trap when an event matches one of the filters.

The BMC stores the IP address for the *trap destination*. This is the system that will receive the SNMP trap generated by the BMC. In addition, BMC will store a *broadcast flag* that will allow the BMC to send traps to all systems on a particular IP subnet. In the future, the BMC will maintain a list of the *trap destinations*.

The Platform Instrumentation (PI) communicates with the BMC to make sure that the IP address matches the IP address configuration on the host. If someone changes the IP configuration on the host OS, or if it changes automatically through DHCP, the PI sends the notification to the BMC to change the IP address.

Note: If the NIC is part of a teaming or fail-over pair that uses DHCP, ISC may not be able to synchronize the BMC with the operating system network configuration information. Do not use the server management assigned NIC as part of the teaming pair. Instead, install an add-on NIC for use as the part of the teaming or fail-over pair or Use a static IP address for the server's server management assigned NIC if it is to be included in a teaming or fail-over pair.

2.2.3 DMI Service Provider

The DMI Service Provider is a piece of software code that interfaces between the platform instrumentation at the server and the ISC Console software. It is responsible for Management Information Format (MIF) access and coordinates requests between PIC and the platform instrumentation.

2.2.4 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is a standard management framework. Its functions are similar to that of DMI. However, DMI and SNMP operate differently; they speak a different “language.” ISC takes advantage of a mapping standard to translate data from one framework to the other, thereby allowing both SNMP and DMI users to use ISC.

2.2.5 Platform Event Paging

Platform Event Paging is built into the platform management technology. This feature allows the platform to proactively alert the system administrator of critical system failures and state changes, independently of the state of the operating system or server management software. Platform Event Paging enables the platform to contact a numeric paging service using an external modem.

When an alert or a page notifies the system administrator, s/he can use the PIC software to remotely view server health / status, system logs, and current configuration. The administrator can also reconfigure, reset or power off / on the server; or execute off-line diagnostics to further analyze the condition of the server remotely. The available functionality depends on the availability of the ISC tools (PIC, DPC etc.) based on the current state of the server.

2.2.6 Internationalization

ISC components will detect the default system language and attempt to load the corresponding language resource files. If successful, all GUI display strings will be in the default system language. However, if the appropriate language resource files are not available, the default language resource files will be used. The default language resource files are in US English.

All strings and resources used within the add-ins are stored in dynamic-link libraries. Each library contains all the required strings and resources for a particular language and locale. The environment is extensible. Extra dynamic link libraries supporting additional languages and locales can be added to the product at anytime.

3. Visible Components

All components rely on a foundation of hardware and firmware support supplied by the platform management technology. The following components are considered “visible.” In other words, these components have a user interface:

- Platform Instrumentation Control (PIC) communicates via the LAN connection to the Platform Instrumentation (PI) resident on the Server. Standard DMI/RPC protocol is used for the communication.
- Direct Platform Control (DPC) communicates to the Emergency Management Port (EMP) on the server. The access path is via LAN, modem or via direct serial connection. This functionality is available when the system is powered off/on, and/or the OS on the server is functional/non-functional. DPC also allows for a text-based console/keyboard redirection for the server and the remote booting of the Service Partition on the target server.
- System Setup Utility (SSU) can be run remotely from an ISC console, using the communication path provided by the DPC.
- Diagnostics (resident on the Service Partition) can be remotely invoked from an ISC console, using the functionality to remotely boot the Service Partition. Again, the communication path is provided by the DPC.

These components are displayed in the following figure as they fit into the ISC product.

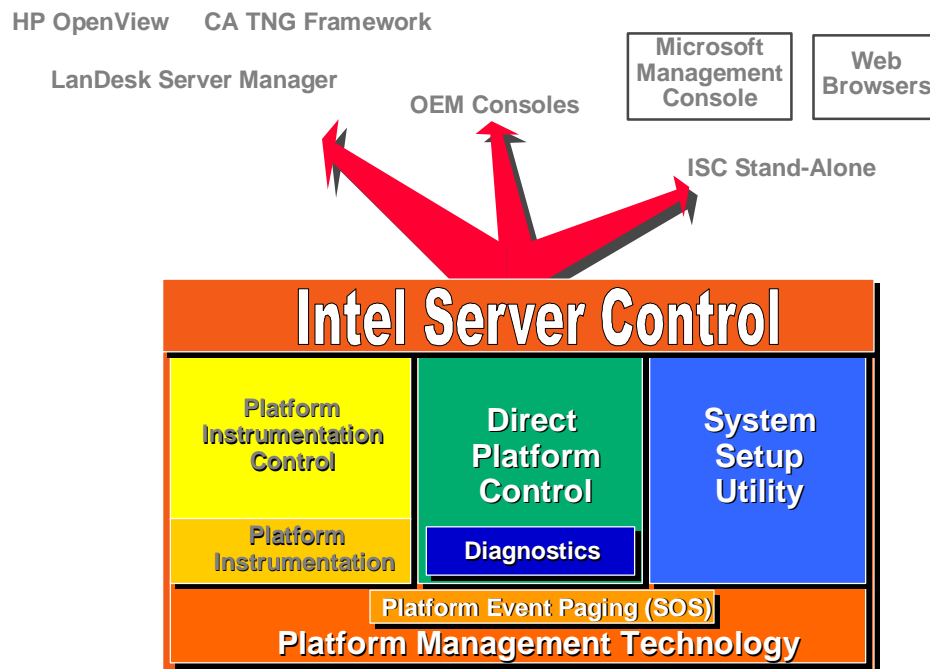


Figure 1 - 1: Intel® Server Control Components

3.1 Component Features

PIC provides the user with the ability to track system status, configure, diagnose, and manage hardware conditions such as:

- Temperature
- Voltage
- Cooling fans
- Chassis intrusion
- ECC memory
- Processors
- Power supplies

Each of these conditions has a threshold or range of acceptable values. The values, current readings, error status, and timer settings can be read and set through PIC. If a parameter crosses a threshold (referred to as an *event*), PIC invokes the action that was pre-determined by the user.

For example, if the temperature reaches a level that is outside the pre-set or user-defined threshold, PIC can:

- Display a message or sound an alert
- Shut down the server
- Log the system event

PIC also allows the user to view:

- System hardware inventory
- BIOS and system slot information
- Platform instrumentation from previous versions of LANDesk[®] Server Control (LSC)

If integrated on the server platform, the user can view:

- Onboard Adaptec SCSI controller status
- Onboard Symbios SCSI controller status
- Onboard American Megatrends, Inc. (AMI) RAID controller status
- Onboard Intel LAN adapter status

3.1.1 Component Management with MIF files and DMI

PIC uses the Desktop Management Interface (DMI) to manage components, such as IPMI-based hardware sensors, inventory information, and third-party instrumentation on server systems. PIC manages the baseboard, chassis, onboard Adaptec and Symbios SCSI controllers, onboard AMI* RAID controllers, and onboard Intel LAN adapters. PIC will also manage servers that were installed with previous versions of LANDesk[®] Server Control (LSC).

Each DMI component must provide a Management Information Format (MIF) file, which describes the manageable attributes of that component. For example, the current reading of a temperature sensor is an attribute that could be listed in a MIF file.

PIC can manage components on the local management console (where the PIC GUI is running) or on a remote server. For SNMP management consoles, PIC includes a translator that allows the user to manage the DMI-enabled platform instrumentation from a remote SNMP application.

The Desktop Management Task Force (DMTF) created and maintains the DMI standard. For more information about MIF files and DMI, see <http://www.dmtf.org>.

Intel® Server Control, Version 3.x TPS

Section 2: Platform Requirements

Table of Contents

1. Introduction to Platform Requirements	1
2. Console Requirements.....	2
2.1 Supported Management Consoles	2
2.1.1 LANDesk® Server Manager 6.0.....	3
2.1.2 HP OpenView Network Node Manager for Windows NT.....	3
2.1.3 CA-Unicenter TNG.....	3
2.1.4 Stand-Alone ISC Console	4
2.2 Supported Console Hardware Configurations	4
3. Managed Server Requirements	5
3.1 Novell NetWare* Requirements.....	5
3.2 Windows 2000*/NT* Requirements	5
3.3 Red Hat* Linux* Requirements.....	5
3.4 SCO UnixWare* 7 Requirements	6
3.5 Additional Requirements for DMI-SNMP Translation.....	6

List of Figures

No figures appear in this section.

List of Tables

Table 2 - 1: PIC Command-line Parameters..... 2

1. Introduction to Platform Requirements

This section discusses the requirements at the server and workstation, in terms of supported management consoles, operating system requirements, and hardware requirements.

Part of Intel® Server Control (ISC) is installed at the server and the other part is installed at a workstation. The ISC Console Software is installed on a Windows NT* server or workstation or on a Windows 98* workstation. The ISC Console Software allows interaction with the managed server.

The ISC Server Instrumentation Software is installed at the NetWare*, Windows NT, Red Hat Linux*, or UnixWare* server to enable it to become a managed server. The term “managed server” refers to the Linux*, NetWare, Windows NT or UnixWare server that is to be managed from the ISC Console.

2. Console Requirements

2.1 Supported Management Consoles

ISC components integrate into an Enterprise System Management Console (ESMC), which must already be in place at the Console station. The ISC installation process detects the Enterprise System Management Console and configures the ISC components to launch from within the application. ISC components appear as a component of the ESMC application, rather than as a separate application at the console workstation.

Once installed, the ESMC runs a primary discovery process to discover the managed servers attached to the network. ISC ties into the initial discovery process of the servers and runs a secondary discovery process. This process is necessary to identify the Operating System (OS) loaded on the server, the system type, the chassis type, and whether the Desktop Management Interface (DMI) service provider and instrumentation is installed on the server system.

Once the managed server is selected and Platform Instrumentation Control (PIC) is launched from within the Enterprise System Management Console, the Console must provide the Remote Procedure Call (RPC) type, network type, network address, and optionally, the host name as parameters to the PIC command line. PIC uses the following command line parameters. The parameters are keyed for flexible ordering and various optional parameter combinations are included.

Table 2 - 1: PIC Command-line Parameters

Key	Definition	Examples	Optional/Required
/rpc:	RPC type.	DCE, ONC	Required
/net:	Network type.	TCPIP, IPX	Required
/addr:	Machine address.	(TCP/IP) 137.46.123.123:8000 (IPX) 112233441122334455660000	Required
/name:	Displayable machine name. If not present, machine address will be displayed as the machine name.	PrintServA	Optional

An example command line is:

```
C:\>PIC.exe /rpc:DCE /net:TCPIP /addr:137.46.123.123 /name:PrintServA
```

Note: RPC type is determined by OS type: Distributed Computing Environment (DCE) for Windows NT, Open Network Computing (ONC) for NetWare and UnixWare.

Indications and events are passed between the Enterprise System Management Console and PIC with either Simple Network Management Protocol (SNMP) or DMI. The method used is dependent on the Enterprise System Management Console.

For a DMI-enabled Enterprise System Management Console event, actions must be configured within PIC. For each event, the user may identify a series of actions, which are to take place. For example, in case of a temperature error, the user may indicate a range of activities from simply logging the event to shutting down the server on which the temperature error occurred.

For an SNMP-based Enterprise System Management Console, to manage the DMI information supplied by PIC at an SNMP-based management workstation, Management Information Base (MIB) files, located on the ISC installation CD-ROM, must be compiled on the SNMP Enterprise System Management Console. It is then possible to use the DMI-SNMP Translator to integrate DMI management with SNMP. In this case, the management requests from SNMP are translated to DMI and responses are translated from DMI to SNMP.

The following Enterprise System Management Console are supported by ISC v3.x

- LANDesk* Server Manager 6.1
- HP OpenView* Network Node Manager 6.0X for Windows NT
- CA Unicenter TNG * 2.2 for Windows NT
- Stand-alone ISC Console, using:
 - ISC container
 - Microsoft Management Console
 - Internet Explorer* v3.02 or above
 - Netscape Navigator* v3.0 or above with ActiveX* snap-in

2.1.1 LANDesk® Server Manager 6.0

The LANDesk® Server Manager (LDSM) console dynamically builds its feature set when communication is established with a managed server. If the managed server is running the ISC Platform instrumentation software, the LDSM 3.02 console adds an option for “Intel Server Control” as a launch point in the Tools branch of the LDSM navigation tree. The LDSM 6.0 console adds an option for “Intel Server Control” as an option under the Snap-in Branch.

2.1.2 HP OpenView Network Node Manager for Windows NT

The HP OpenView Network Node Manager Console auto-detects servers running the ISC Platform instrumentation software. ISC-enabled servers display on the HP Console network map and an “Intel Server Control Applet” option is added as an option in the Tools Menu.

2.1.3 CA-Unicenter TNG

The CA-Unicenter TNG Console auto-detects servers running the ISC Platform instrumentation software if the ISC to CA discovery service is enabled. This service can be started either from TNG Unicenter "Auto Discovery" dialog or from the Windows NT "Services" applet.

The "Intel TNG-ISC AutoDiscovery" service creates a new "Intel Server Control" TNG object for each server having the ISC Platform instrumentation software. That TNG object displays on the map as a child of the "ISC World View" and as a child of the ISC-enabled server. The “ISC World View” displays all ISC-enabled servers.

2.1.4 Stand-Alone ISC Console

The stand-alone ISC Console can be used to manage ISC-enabled servers without installing an Enterprise System Management Console application. This environment is implemented as an ActiveX control that runs within its own container or third party “container applications,” such as Microsoft Management Console, Microsoft Internet Explorer (versions 3.02 or greater) or Netscape Navigator (versions 3.0 or greater).

2.2 Supported Console Hardware Configurations

Windows 98

- Intel® Pentium® microprocessor or higher.
- At least 32 MBs of RAM.
- Remote Registry Service. It must be installed before ISC. See the systems requirements section of the file enuReadme.txt on the software kit CD of additional information.
- At least 60 MBs of available disk space.
- PIC requires an additional 10 MBs.

Windows 2000/NT

- Windows NT Server or Workstation 4.0(SP 5), or Enterprise Edition.
- Intel® Pentium® microprocessor or higher.
- At least 64 MBs of RAM.
- For Windows NT, Remote Access Service must be installed. If it is not installed the Direct Platform Control (DPC) component will not be installed.
- At least 60 MBs of available disk space.
- PIC requires an additional 10 MBs.

3. Managed Server Requirements

ISC can be used to manage NetWare®, Windows NT®, Red Hat Linux®, or UnixWare® servers running on several Intel system boards. A complete list of supported server system boards and qualified BIOS revision levels can be found in the README.TXT file provided with ISC.

3.1 Novell NetWare* Requirements

The following are required to manage a Novell NetWare server:

- NetWare 4.2, 5.0.
- One of the Intel baseboards specified in the release notes.
- At least 24 MBs of RAM.
- At least 30 MBs of available disk space.
- NetWare SNMP NLM installed (required only for connectivity to an SNMP management console).
- An account with administrative rights.

3.2 Windows 2000*/NT* Requirements

The following are required to manage a Windows NT server:

- Windows 2000, NT Server 4.0 (SP 5), or Enterprise Edition.
- One of the Intel baseboards as specified in the release notes.
- 64 MBs of RAM.
- 60 MBs of available disk space.
- Windows NT SNMP or SNMP service must be installed (required only for connectivity to an SNMP management console).
- An account with administrative rights.

3.3 Red Hat* Linux* Requirements

If you intend to manage a Linux file server, it must be meet the following minimum requirements:

- Red Hat Linux 6.1 running multiple-processor kernel.
- 32 MBs of RAM.
- 60 MBs of available disk space.

3.4 SCO UnixWare* 7 Requirements

The following are required to manage a UnixWare 7 server:

- SCO UnixWare 7.1.
- Intel® Pentium® or higher processor-based server.
- One of the Intel baseboards specified in the release notes
- A minimum of 32 MBs of RAM.
- A minimum of 30 MBs of available disk space.
- An account with root or equivalent rights.

3.5 Additional Requirements for DMI-SNMP Translation

SNMP support must be installed in order to integrate ISC with an SNMP-based management framework. SNMP installation information may be found in Windows NT, NetWare, or UnixWare documentation.

Intel® Server Control, Version 3.x TPS

Section 3: Standalone Console

Table of Contents

- 1. Introduction to Standalone Console 1
- 2. Standalone Console Menu Items..... 2
 - 2.1 Main Menu 2

List of Figures

Figure 3 - 1: ISC Standalone Screen..... 1

List of Tables

No tables appear in this section.

This page intentionally left blank

1. Introduction to Standalone Console

The Standalone Console is an ActiveX* container that provides for the discovery of servers over the Local Area Network (LAN). The Standalone Console consists of a Win32* graphical user interface (GUI) that provides for the discovery of servers over the LAN and serves as a launch vehicle for Platform Instrumentation Control (PIC), Direct Platform Control (DPC), and Client System Setup Utility (CSSU).

As demonstrated by the following figure, the Standalone Console GUI is comprised of a menu bar, a tool pane and a presentation pane. The tool pane shows the launch icons for the installed tools.

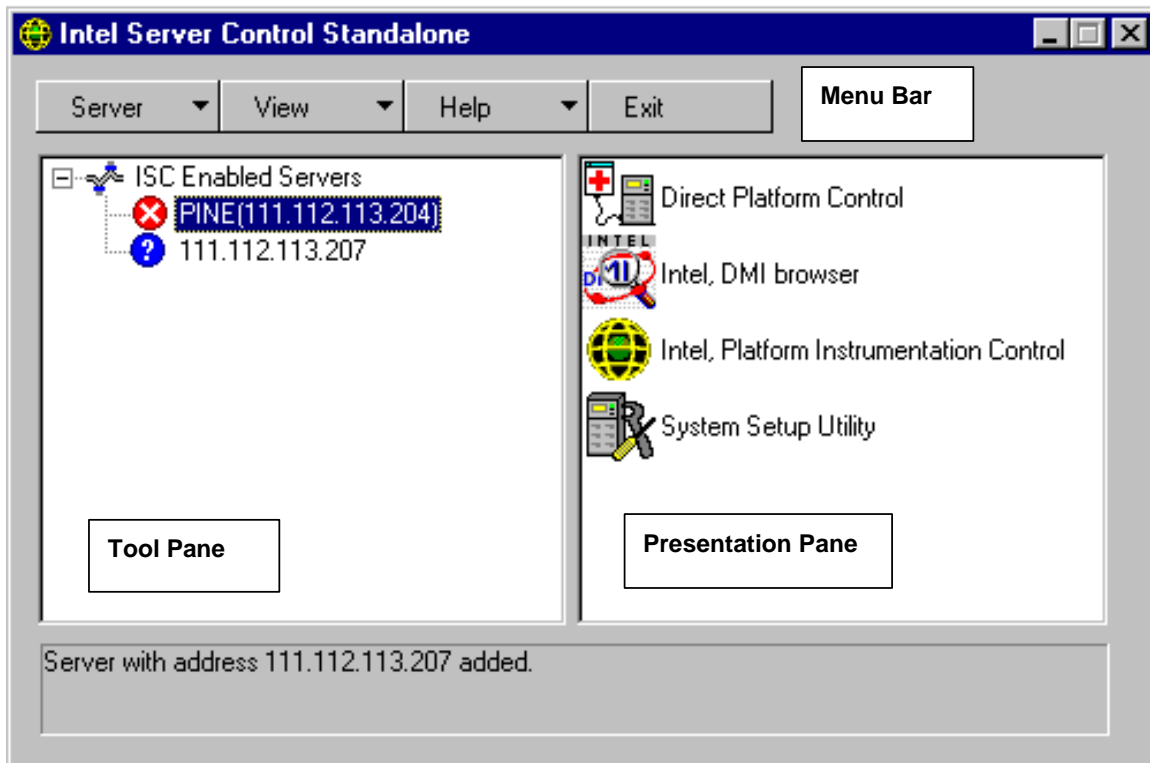


Figure 3 - 1: ISC Standalone Screen

As displayed in the figure under the heading of “ISC Enabled Servers”, critical ISC errors are displayed as a red circle enclosing a white “X.” Non-critical errors are displayed with a yellow triangle (not displayed). Servers that are not enabled with full ISC functionality are displayed as a blue circle encompassing a white “?” The server name is listed to the right of the icon.

2. Standalone Console Menu Items

2.1 Main Menu

The main menu options may be outlined as:

Server Menu

Add	Adds a server to server list
Delete	Deletes a server from server list
Discover	Launches the discovery tool
Delete All	Deletes all listed servers
Stop Discovery	This option cancels the current discovery

View Menu

Icon View	Displays list view items using icons.
List View	Displays list view items in list format.

Help Menu

Contents	Opens the ISC Standalone Console help topics.
About	Opens the ISC Standalone Console version information screen.

Exit Menu

Intel® Server Control, Version 3.x TPS

Section 4: Direct Platform Control

Table of Contents

1. Introduction to Direct Platform Control (DPC)	1
2. Console Manager	3
3. Server Configuration	5
4. Security	6
5. Making a Connection	7
6. Console Redirection	8
7. DPC Plug-ins	9
7.1 Server Control	9
7.2 SEL Viewer	9
7.3 SDR Viewer.....	9
7.4 FRU Viewer.....	9
7.5 RSA Manager.....	9
8. Reboot from Service Partition	10
8.1 Run DOS/EFI Shell	11
8.2 Run Program... ..	12
8.3 Run Diagnostics	12
8.4 File Transfer	13
8.4.1 Upload.....	13
8.4.2 Download... ..	14
8.5 Redirection View	14
8.6 Configuration Status.....	15
9. Modes of Operation	17
9.1 EMP Mode	17
9.2 Redirect Mode	17
9.3 PPP Mode	17
9.4 PPP-Redirect Mode.....	17
10. DPC User Interface	18
10.1 EMP Mode	18
10.1.1 Main Window	18
10.1.2 View Menu	31
10.1.3 Window Menu	32

10.1.4	Help Menu.....	32
10.2	Connection Menu.....	34
10.2.1	Connect Dialog – LAN or Direct	34
10.2.2	Phonebook Dialog.....	35
10.2.3	Add Phonebook Entry	36
10.2.4	Modify Phonebook Entry	37
11.	Supported Features.....	38
11.1	Toolbar Buttons.....	38

List of Figures

Figure 4 - 1: Direct Platform Control Components.....	2
Figure 4 - 2: DPC Console Manager	3
Figure 4 - 3: DOS Shell Window	11
Figure 4 - 4: Run Program Dialog.....	12
Figure 4 - 5: Upload Dialog	13
Figure 4 - 6: Download Dialog	14
Figure 4 - 7: Configuration Status - Capabilities Screen	15
Figure 4 - 8: Configuration Status - Status Screen	16
Figure 4 - 9: Configuration Status - EMP Status Screen	16
Figure 4 - 10: DPC Main Window	18
Figure 4 - 11: Power On Server Dialog - Serial Connection.....	22
Figure 4 - 12: Power On Dialog	23
Figure 4 - 13: Reset with a Serial Connection	23
Figure 4 - 14: Reset Server Dialog - LAN Connection	24
Figure 4 - 15: DOS Shell Window.....	25
Figure 4 - 16: Run Program Dialog.....	26
Figure 4 - 17: Upload Dialog	27
Figure 4 - 18: Download Dialog	28
Figure 4 - 19: Configuration Status - Capabilities Screen	29
Figure 4 - 20: Configuration Status - Status Screen	30
Figure 4 - 21: Configuration Status - EMP Configuration Screen	30
Figure 4 - 22: Help Topics Window	33
Figure 4 - 23: About the DPC Console Manager Dialog	33
Figure 4 - 24: Connect Dialog - LAN	34
Figure 4 - 25: Connect Dialog - Direct	34
Figure 4 - 26: Phonebook Dialog.....	35
Figure 4 - 27: Add Phonebook Entry	36
Figure 4 - 28: Modify Phonebook Entry	37

List of Tables

Table 4 - 1: Run Program - Options	12
Table 4 - 2: Upload Dialog - Options	13
Table 4 - 3: Download Dialog – Options	14
Table 4 - 4: File Menu - Options	20
Table 4 - 5: Connect Menu Options.....	21
Table 4 - 6: Power On with a Serial Connection Options.....	22
Table 4 - 7: Power On with a LAN Connection Options	23
Table 4 - 8: Reset with a Serial Connection Options	24
Table 4 - 9: Reset with a LAN Connection.....	24
Table 4 - 10: Run Program Dialog - Options	26
Table 4 - 11: Upload Dialog - Options	27
Table 4 - 12: Download Dialog - Options	28
Table 4 - 13: Connect Dialog - Options	35
Table 4 - 14: Phonebook Dialog - Options.....	36
Table 4 - 15: Add Phonebook Entry - Options	36
Table 4 - 16: Modify Phonebook Entry - Options	37
Table 4 - 17: DPC Console - Supported Features	38
Table 4 - 18: Toolbar Buttons.....	38
Table 4 - 19: DPC Status Bar Information	39

This page intentionally left blank

1. Introduction to Direct Platform Control (DPC)

The Intel® Server Control (ISC) Standalone application includes three major components to manage a server: Platform Instrumentation Control (PIC), DPC, and Client System Setup Utility (SSU). DPC provides emergency and out-of-band management access to the server through a modem or direct serial line connection. It also provides the ability to run DOS-based programs and diagnostics.

DPC communicates to the server through the Emergency Management Port (EMP), a server management feature that supports remote system management using a modem or serial line connection to the COM2 port or via the Local Area Network (LAN) connection. Since DPC does not communicate with the server-resident operating system, it can be used to manage the server even if the operating system and the primary processors of the server are not operational. The DPC management console can also connect via the network adapter when the operating system is down. Because the platform-resident support for DPC is available on 5-V standby, DPC can be used to communicate with and control a powered down server.

The capabilities provided by the DPC user interface include:

- Establish connection to remote servers
- Server Control: Reset and Power on/off operations of server
- SEL Viewer: Retrieve and display System Event Log (SEL) entries
- SDR Viewer: Retrieve and display Sensor Data Records (SDR)
- FRU Viewer: Retrieve and display Field Replaceable Unit (FRU) information
- RSA Viewer: Remote Sensor Access (RSA) information
- Phonebook for remote connection management
- Modes of operation: DPC / Console redirection

Remote control of service partition, which includes the following: file transfer, program execution, and diagnostics.

Note: Available features are platform dependent.

DPC provides a user-friendly interface, the DPC Console, for monitoring and controlling the platform management features of the system. The DPC Console is a Windows 32 graphical user interface (GUI) that communicates with the Platform Management Technology resident on the server. It is the user interface to the Emergency Management Port. The GUI is designed as a set of ActiveX controls that communicates to the server using a combination of proprietary and standard networking, and serial line protocols.

The GUI integrates into a variety of widely deployed enterprise and workgroup management consoles, as well as into the ISC Standalone container. DPC relies on the management console or ISC Standalone for discovery of servers over the LAN. It supports a user-configurable phone book for aiding in dialing modem-based connections.

The following figure illustrates the architecture of the Direct Platform Control (DPC) components of the ISC product.

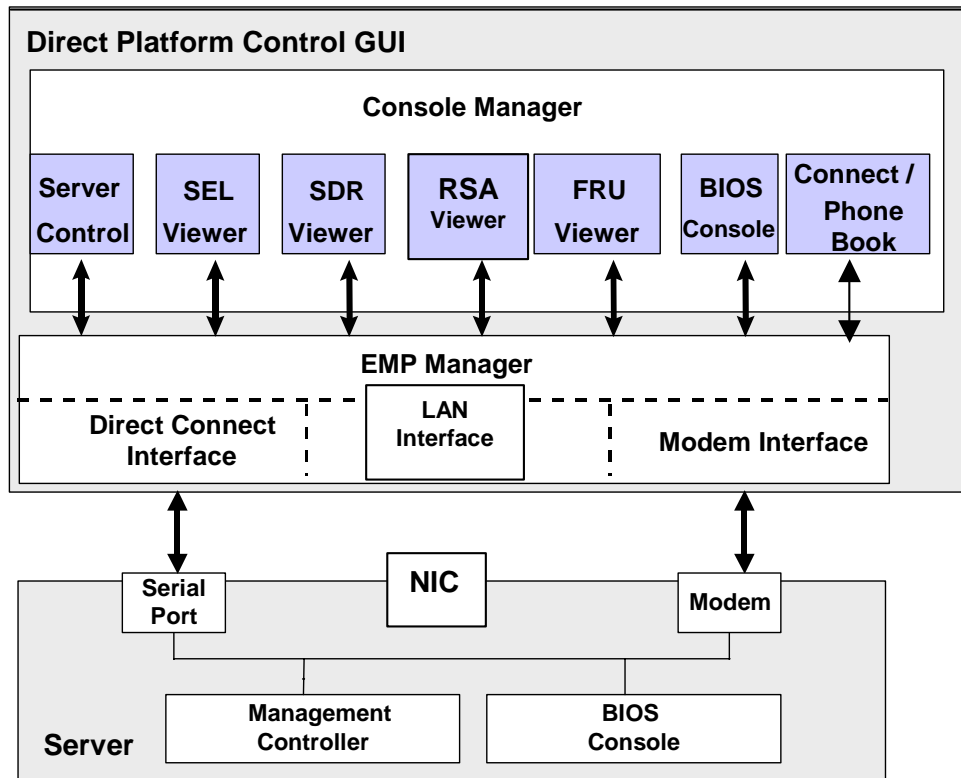


Figure 4 - 1: Direct Platform Control Components

Using the capabilities provided by these elements, the management console is able to make a modem or Network Interface Card (NIC) connection to a target server regardless of the operational state of the server. The console can then bring the target server into a service mode by rebooting the server to the service partition, where it can perform remote operations. The DPC session to the server is secured via a BIOS-level password. The same password is used to negotiate a Point-To-Point Protocol (PPP) connection after re-boot of server is initiated.

2. Console Manager

The DPC Console will support all COM ports on the client system, along with any Windows* NT/98/2000 compatible modem. The console uses the Windows Internet Protocol (API) to determine if a modem is connected and available. The DPC depends on Windows to have a pre-configured the modem (even for LAN connections); the console will configure the modem itself.

The Console Manager integrates the management plug-ins and provides a graphical user interface to launch individual plug-ins, such as the SEL Viewer, SDR Viewer, RSA Viewer, FRU Viewer, Server Control, etc. The Console Manager display consists of a menu and toolbar at the top of the display and a status bar at the bottom. The menu and toolbar provide the options to initiate plug-ins and other support functions such as modem functions and LAN functions. The status bar is used to display connection status information like server name, line status, mode, etc.

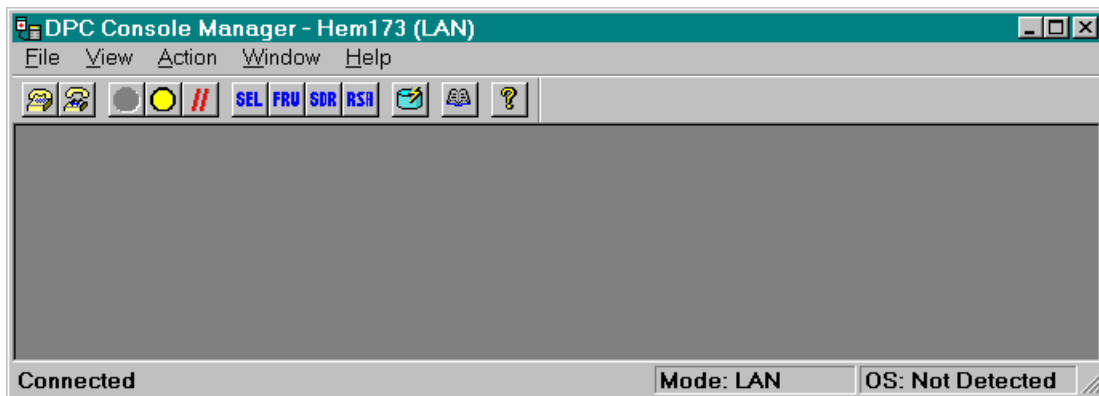


Figure 4 - 2: DPC Console Manager

A connection can be initiated by using the menus or toolbar icons to select the server on the dial-up line, to select the direct line with the appropriate serial port, or the LAN connection with associated Internet Protocol (IP) address. This module integrates a Phonebook to maintain the list of servers and their telephone numbers. To make a connection, the user only needs to type the server name or select it from the list and click “Connect.”

The DPC Console prompts for a password before initiating a connection, even if the server is not configured with a password. If a password for the server is configured in BIOS setup, the user must enter it. If no password has been configured, the user may press the ENTER key to bypass this field. The password is not stored in the phonebook. Therefore, it must be entered each time the user begins the connection process.

Three modes of operation are available: EMP Mode, BIOS Console Redirect Mode, and LAN mode.

In EMP mode, the console allows the user to launch one of the management plug-ins either from the tool bar or from the action menu.

In the BIOS Console Redirect Mode, the console launches a separate window and operates as a terminal. Remote server management BIOS settings can be reset / modified in this window.

In LAN mode the user has the same functionality as in EMP Console, but the NIC is provides the connection instead of the modem port.

3. Server Configuration

The BIOS on the target server supports booting from a service partition installed on the local hard disk. The EMP firmware and the BIOS on the target server together support the request and execution of a service boot.

EMP must be configured on the server to allow DPC to connect to the server using the EMP port. By default, DPC requires the use of the COM2 serial port connected to an external modem or with a serial cable.

The server must use a Hayes*-compatible 28800 Bits Per Second (BPS) modem that is listed in the Windows NT Hardware Compatibility list provided by Microsoft*. The server modem must be set in auto-answer mode for the DPC Console to be able to connect to it. Also, the recommended modem settings are the following: baud rate 19.2K, IRQ 3 or 4, and BIOS COM port settings of 2F8 with CTS/RTS + CD.

DPC requires the following elements:

- EMP firmware running on the target server.
- BIOS Console Redirection for remote access to pre-boot BIOS setup.

For running a DOS shell, DOS based programs and diagnostics; DPC needs additional elements to be available at the server.

- BIOS support on the target server for booting from a service partition.
- A service operating system (OS) such as DOS or ROM-DOS installed on the target server's service partition with a third party TCP/IP stack which includes PPP.
- A remote service agent running on the target server.
- OS agents.

With the capabilities provided by these elements, the management console may make a modem connection to a target server regardless of the target server's operational state. The console can then bring the target server into a service mode by rebooting the server to service partition, where it can perform remote operations. The DPC session to the server is secured via a BIOS-level password. The same password is used to negotiate PPP connection after re-boot of server is initiated.

4. Security

When connecting to the server, DPC ensures security of the server with a password. The maximum length of the password is sixteen alphanumeric characters. For enhanced security, the password is case-sensitive. The user enters the password at the DPC Console and it is sent to the server in clear text for non-LAN connections only. LAN connections do not use clear text passwords and have security that has been enhanced over previous versions of ISC.

Unlike a serial connection, a LAN connection does not send the password over the wire, rather a Challenge Handshake Authentication Protocol (CHAP) is used. This uses a 'one-way' hashing algorithm to determine the hash value and it is computationally infeasible to determine the password or secret key used for the calculation. The client and the authenticator share the password. The password is never passed over the link.

Additional security while connecting over LAN is attained by the use of a message authentication code or hash, which accompanies potentially dangerous commands (such as power-off). The current implementation of this hash, or message digest, is MD2 – Message Digest version 2

Additionally, if the user fails to enter the correct password in three successive attempts, the server rejects the password and locks up the interface for 30 seconds. The DPC Console displays a "Password rejected" message and disconnects the line. An appropriate event is logged in the SEL.

The password is not saved on the machine running the DPC Console and it is not stored in memory while DPC is running.

In addition to password security, all communication with the DPC is logged in the SEL viewer and the operating system event (system) logs. Because of this, a security breach can be detected. In addition, BIOS restricted mode prevents unwanted users from accessing servers in DPC mode.

5. Making a Connection

DPC can initiate a connection on either a serial line, a dial-up line, or LAN connection. DPC initially expects the server to be in EMP mode and it attempts to connect using EMP protocols. After successfully connecting, the EMP supported actions, such as Power on/off, Reset and the SEL/SDR/FRU/RSA/Redirect Viewers are enabled, depending on the server configuration.

The Power off and Reset operations ensure a graceful shutdown in case an OS is running. For these actions, DPC will generate a Server Management Software (SMS) message with the OS shutdown option. This operation may take more time depending on the number of applications running on the server. In the EMP mode, the user can at any time request for a reboot of the server to the service partition by selecting the option from a menu or the toolbar. When the user requests a “power off”, DPC will send a “Shutdown command” followed by the “power off” command.

Note: A connection via LAN must be secure in order for the power actions to be made available. If the connection is not a secure connection, the title bar will display “LAN – Unsecure” and the power actions will be disabled.

Command line launch of the DPC Console is available. The command line syntax is as follows:

```
C:\> DPCConsole /modem=[phone number]
```

where [phone number] is the phone number of the server you wish to connect to, or

```
C:\> DPCConsole /direct= [comX]
```

where [comX] is the com port of the direct connection.

```
C:\> DPCConsole /lan=[ipaddress or dns name]
```

where [ipaddress or dns name] is the IP Address Domain Name System (DNS) Name of the server.

For example:

```
DPCConsole /modem=555-1212
```

```
DPCConsole /direct=1
```

```
DPCConsole /lan=255.255.255.0
```

6. Console Redirection

The Console Redirection control enables a display of “redirected” data from server when the server switches over to BIOS console redirection. In this mode, the Console launches a separate window, which emulates an American National Standard Institute (ANSI) terminal. The Redirect window display is the same as the server console display and will operate like a remote terminal. All the user keystrokes are translated and transmitted to a remote server and the corresponding responses from the server are displayed.

The Console Redirection is active only when the server is operating in “real” mode. When the server is running in DOS/ Extensible Firmware Interface (EFI), redirection is available, since DOS is considered to be running in real mode. When an OS like Windows NT/98/2000 is running on the server, console redirection is not available, since the machine is switched to protected mode when an OS is running.

The operation of switching between EMP and Redirect modes will depend up on the setting of the EMP access mode in the BIOS setup of the server. This mode can be one of the following:

- Preboot only
- Always active
- Disabled

The server enters console redirect mode only if this feature is enabled through BIOS setup. The DPC Console will enter the redirect mode under the following conditions:

- When DPC Console is connected to the server in EMP mode and the server is switched to redirect mode, the Baseboard Management Controller (BMC) sends a special “EMP active” message.
- While initiating a connection, if DPC Console fails to connect in EMP mode within ten seconds. In this case, the user is given the option to switch to redirect mode, assuming that the server may be in the redirect mode. However, no data is displayed in redirect window if the redirection is either not enabled or EMP is disabled in the BIOS setup or server is in “protected” mode running OS.

7. DPC Plug-ins

The Plug-ins available through DPC include:

- Server Control
- SEL Viewer
- SDR Viewer
- FRU Viewer
- RSA Manager

7.1 Server Control

The Server Control plug-in provides power up / down and reset functions. The power up / down function is used to power-on or power-off the server. This function also allows the user to set post-power-up options, which can be used to set the operating mode to EMP active or BIOS redirection on the next power on.

The server firmware that responds to the DPC Console will operate on Standby Power either set on the LAN connection or EMP. The reset function can be used to generate reset on the server with a post-reset option similar to the power up / down function. The power down and reset functions are disabled if the server is in “restricted“ mode for EMP operations. However, the power up function is available even when the server is in “restricted” mode.

7.2 SEL Viewer

The SEL Viewer plug-in provides access to the System Event Log on the server and will have the functionality to display the SEL records. SEL data includes information on events, such as the occurrence of a fan outage or a temperature that has exceeded a pre-determined height.

Note: SEL information is displayed on supported servers only.

7.3 SDR Viewer

This plug-in allows the user to view the Sensor Data Records, retrieved from the SDR Repository. The SDR Viewer can be optionally either to display records of a particular sensor type or to display records for all sensor types.

7.4 FRU Viewer

The FRU Viewer allows the user to display the Field Replaceable Unit data. The information displayed includes chassis information, baseboard information and product information.

7.5 RSA Manager

This menu provides the user with RSA (Remote Sensor Access) data from the server’s baseboard FRU and SDR information area. This allows the user to view live data from the servers sensors.

8. Reboot from Service Partition

Note: The reboot to service partition is NOT supported on direct line connection.

The option to reboot from the service partition allows the user to run DOS-based utilities that are installed on the service partition. When the user initiates this menu option, the DPC Console first checks for the presence of a service partition on the server and allows a reboot only if the server partition is detected. This option also checks the power status of the server and switches on the power if it is currently powered off.

The DPC will reboot the server with OS shutdown option. This reboot makes all server services inaccessible to end-users. This operation is allowed only when the DPC Console is in EMP mode and if the server's BIOS supports booting from a service partition installed on the local hard disk. Reboot to Service Partition can occur only if the server is not set in 'EMP Restricted Mode.' The status bar updates accordingly once the connection has completed.

With a LAN connection, all EMP based actions are available even after switching to the TCP connection.

In case BIOS fails to boot from the service partition, an error message will be displayed in the redirection window. In this case the user needs to terminate the service boot operation.

After establishing the PPP connection, the DPC no longer communicates to the EMP controller. All actions that are supported in EMP mode are disabled. The user interface is modified to allow the user to run the DOS/EFI shell, DOS/EFI commands and diagnostics. After switching to a PPP connection, the user will need to disconnect from the server and reconnect to again operate in EMP mode.

When the user is finished with Service Partition, they must select Reset (only for LAN connection) or Disconnect (Serial or Dial-up), to reboot the server out of Service Partition. A confirmation dialog will be shown prior to resetting the server.

While booted to Service Partition, the Service Partition menu is displayed. It has the following items:

- Run DOS/EFI Shell
- Run Program
- Run Diagnostics
- File Transfer
- Redirection View

8.1 Run DOS/EFI Shell

This option is used to start a DOS or EFI command shell. The DOS or EFI command prompt can only be started when no other DOS or EFI based software is running. The DPC Console opens a redirection window to display the response and the keystrokes are transmitted to the server. The user may use the DOS or EFI command shell to change directory and run diagnostics or use the Action menu item.

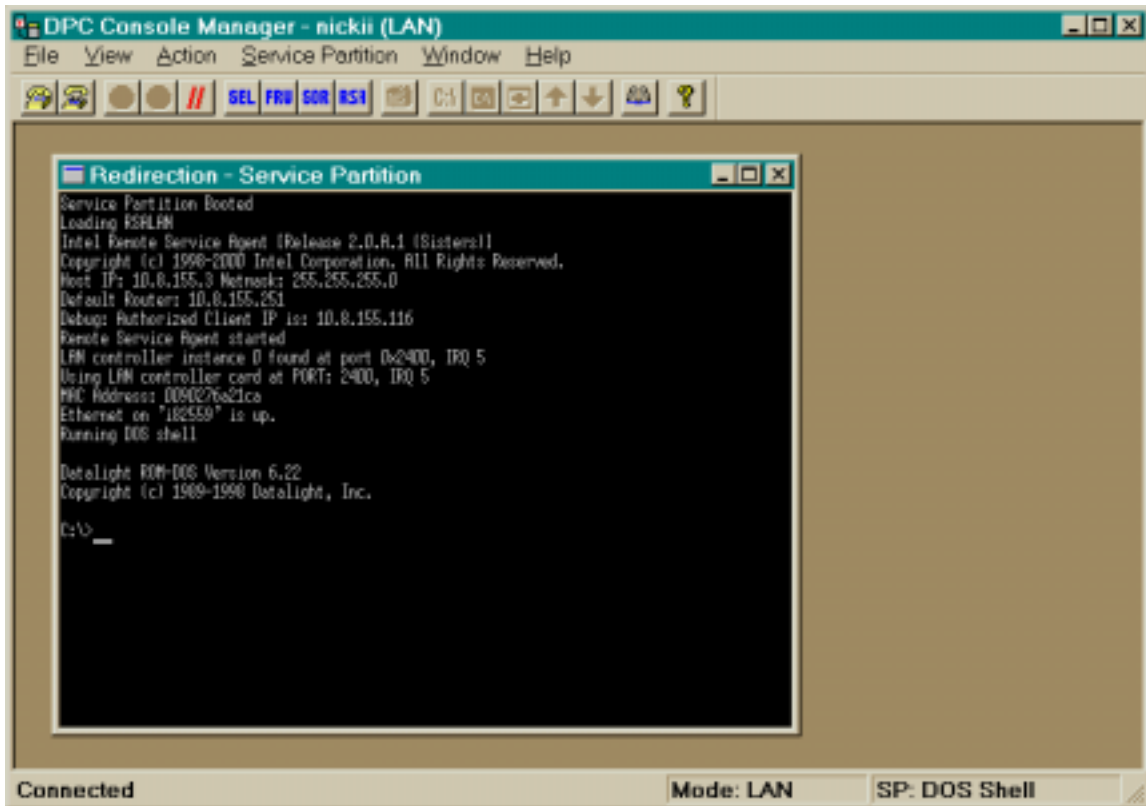


Figure 4 - 3: DOS Shell Window

8.2 Run Program...

This menu option is used to run a program on the server. This dialog behaves very similar to the Windows Run... option available from the Windows Start menu.

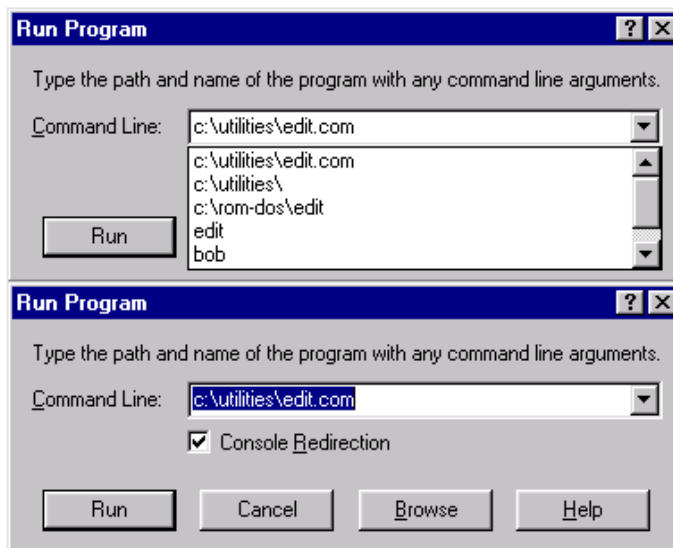


Figure 4 - 4: Run Program Dialog

Table 4 - 1: Run Program - Options

Option	Description
Command Line:	Type the path and filename of the program on the server to execute. In addition, command line option can be included. Optionally, select the command from the combo-box. The command can be edited and will be saved as a new entry if edited. The combo box is sorted by most recently used item.
Console Redirection:	Console redirection is checked by default. Uncheck this if no console redirection is required. If this is unchecked and a program does not terminate on its own, the user will be unable to run any other programs, DOS shell, diagnostics or perform any file transfer operations.
Run:	Pressing this button executes the command line as given on the server. In addition, the entry is saved to the combo-box.
Browse:	When this button is pushed the standard Windows File Open dialog is shown as a directory browser. The files and directories listed are from the server. If a file is selected/ entered and OK is pressed the path and filename of the selected file (or a new file name entered by the user) will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Cancel:	Pressing this button dismisses the dialog with no further action.

8.3 Run Diagnostics

This menu item is selected to run the diagnostics remotely on the server. This is a pre-configured DOS or EFI program with an exception that user cannot edit the program path. This action creates a redirection window and executes the diagnostic program, which launches the initial screen.

8.4 File Transfer

This is a cascading menu used to transfer files between the Client and the Server in binary mode. The following menu items are provided:

- Upload...
- Download...

8.4.1 Upload...

This menu option is used to transfer files from the client to the server in binary mode. When the user clicks this menu option, a dialog is displayed with the following controls:

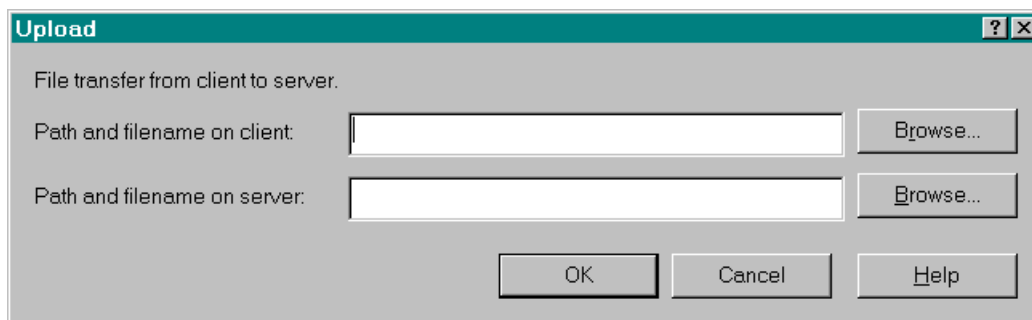


Figure 4 - 5: Upload Dialog

Table 4 - 2: Upload Dialog - Options

Option	Description
Path and filename on the client:	This is the directory structure and the name of the file that needs to be transferred. If this file does not exist on the client, an error message is displayed to the user.
Browse (client):	When this button is pushed the standard Windows File Open dialog is shown. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Path and filename on the server:	This is the directory path and the name of the file, as it will be stored on the server. If the directory structure does not exist on the server an error message is displayed to the user. The user can confirm the directory structure by using the browse capability. The user can use Run DOS/EFI Shell menu option specified earlier to create the directory path to be used here. If the file already exists, it will be over written. If no filename is provided, the client filename will be the default. The transfer is done in binary mode i.e. no conversion for CR-LF (carriage return and line feed is performed).
Browse (server):	When this button is pushed the standard Windows File Open dialog is shown as a directory browser. If a file is selected/ entered and OK is pressed the path and filename of the selected file (or a new file name entered by the user) will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
OK:	Press this button to start the upload process, after the correct file paths have been specified.
Cancel:	Click this button to dismiss the dialog, without uploading any file.
Help:	Click this button to view the help related with this dialog.

8.4.2 Download...

This menu option is used to transfer files from the server to the client in binary mode. When the user clicks this menu option, a dialog is displayed with the following controls:

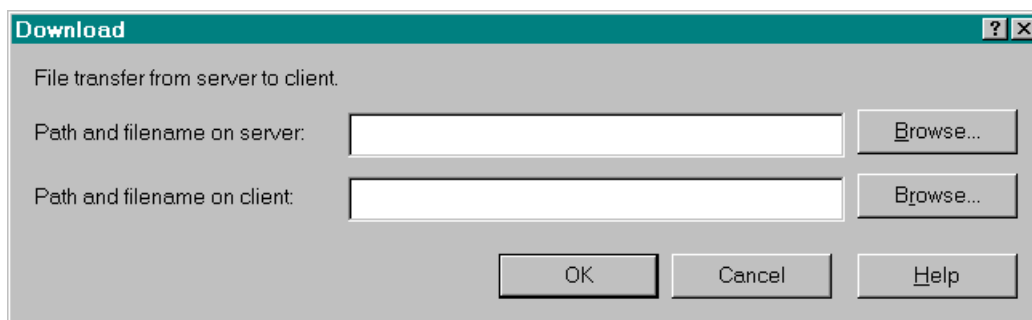


Figure 4 - 6: Download Dialog

Table 4 - 3: Download Dialog – Options

Option	Description
Path and filename on the server:	This is the directory structure and the name of the file that needs to be transferred. If this file does not exist on the server, an error message is displayed to the user. The user can confirm the directory structure by using the browse capability. The transfer is done in binary mode i.e. no conversion for CR-LF (carriage return and line feed is performed).
Browse (server):	When this button is pushed the standard Windows File Open dialog is shown. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Path and filename on the client:	This is the directory path and the name of the file, as it will be stored on the client. If the directory structure does not exist on the client an error message is displayed to the user. If the file already exists it will be over written. If no filename is specified the server filename will be the default.
Browse (client):	When this button is pushed the standard Windows File Save dialog is shown as a directory browser. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
OK:	Click this button to start the download process, after the correct file paths have been specified. The named file is downloaded from the server to the client in binary mode.
Cancel:	Click this button to dismiss the dialog, without downloading any file.
Help:	Click this button to view the help related with this dialog.

8.5 Redirection View

This is a checked menu item. If the service partition redirection view is visible, this item is checked. Selecting this menu item toggles the visibility of the service partition view.

8.6 Configuration Status

This new ISC 3.x tool displays an information dialog that gives the chassis status and EMP configuration of the server. This information is available when the DPC Console successfully connects in EMP mode. The information is displayed in three groups with separate tabs for each group.

Service partition is updated in the phonebook automatically, whenever a connection is made to the server and whenever server status and configuration is retrieved.

- **Capabilities:**
This group gives the SEL, SDR, FRU, Power Inter Lock Status, Secure mode, and intrusion status.

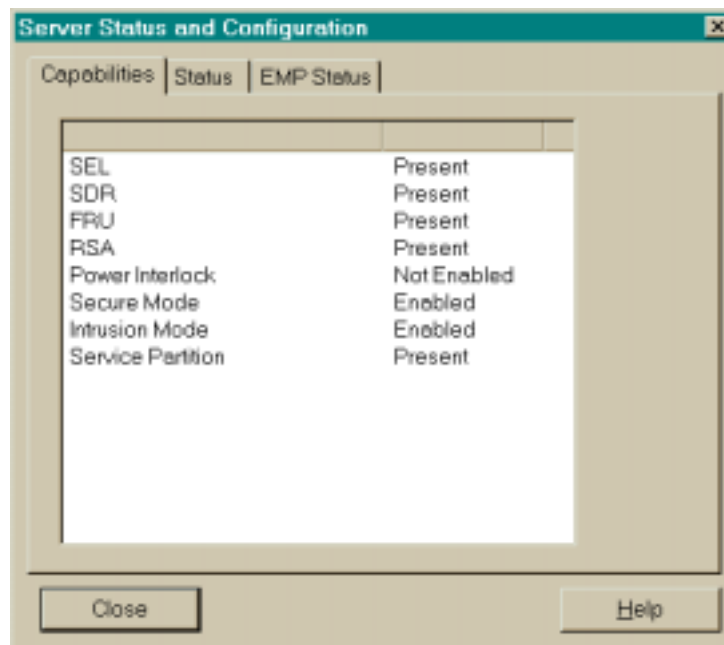


Figure 4 - 7: Configuration Status - Capabilities Screen

- Status:**
 Displays the Power status, Interlock active status, Power fault, Cooling fault, secure mode and intrusion active and OS run status.

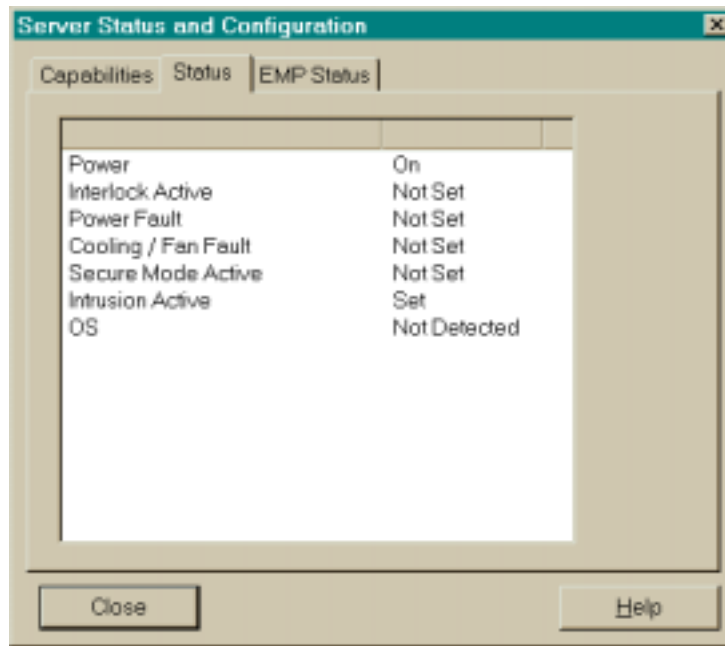


Figure 4 - 8: Configuration Status - Status Screen

- EMP Configuration:**
 Gives Restriction mode and Activation mode status.

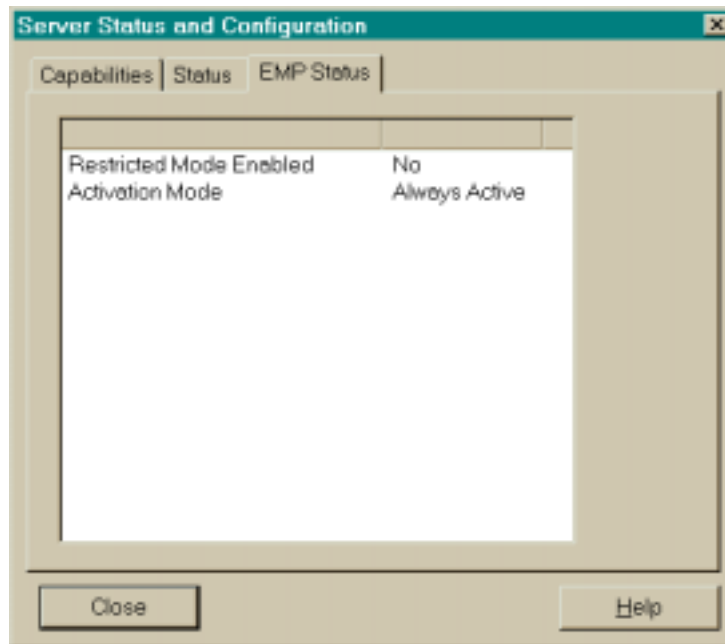


Figure 4 - 9: Configuration Status - EMP Status Screen

9. Modes of Operation

DPC displays the current operational mode in the status bar. The following modes are displayed.

- EMP Mode
- Redirect Mode
- PPP Mode
- PPP-Redirect Mode
- LAN Mode

These modes are described in the following sections.

9.1 EMP Mode

DPC always initiates a connection in this mode. If DPC fails to establish a connection, it allows the user to switch to redirect mode. EMP mode is supported in the existing DPC Console.

9.2 Redirect Mode

Redirect mode is active when server is running BIOS console redirection. DPC emulates an ANSI terminal and the redirected data is decoded and displayed in a separate window. At the same time, the keystrokes are redirected to the BIOS running on the server. This mode is supported in the existing DPC Console.

9.3 PPP Mode

PPP mode is entered when the user selects the option to reboot from the service partition, and a successful PPP connection is established. This mode allows the user to run the DOS-based utilities that are resident on the service partition.

9.4 PPP-Redirect Mode

PPP-Redirect mode is similar to the Redirect mode but differs in that it uses the TCP/IP stack for the data transfer. DPC supports two methods of executing DOS based utilities. The first method is selecting a utility from the program list. This program list is a set of standard utilities, which are pre-configured with full program path. The second method is to use DOS command shell to get the command prompt and execute the utilities. For both of these methods, DPC opens a redirection window and starts protocol based console redirection process with the server.

This mode can be entered only through “PPP mode”. When DOS shell or text based programs are executed, DPC issues “StartProtRedir” command to the server to enable PPP based redirection. Some of the utilities may not display any data and thus do not require redirection. Therefore, DPC stores this status in the configuration data for all the utilities.

Only one DOS-based utility or command shell may be running at one time. Because DOS is a single-threaded OS, DOS programs cannot be executed concurrently with the File Transfer Service.

10. DPC User Interface

This section provides a detailed description of the GUI for DPC and the management plug-ins.

At start-up, DPC displays the main menu, toolbar and a status bar. These can be used for start-up actions like making connection and launching a plug-in. The status bar is always active and displays the server status information (server name, line status and the mode).

10.1 EMP Mode

The main window of the DPC Console Manager in EMP Mode is displayed in Figure 4 - 10. The sections following the diagram describe the components and menu items on this screen.

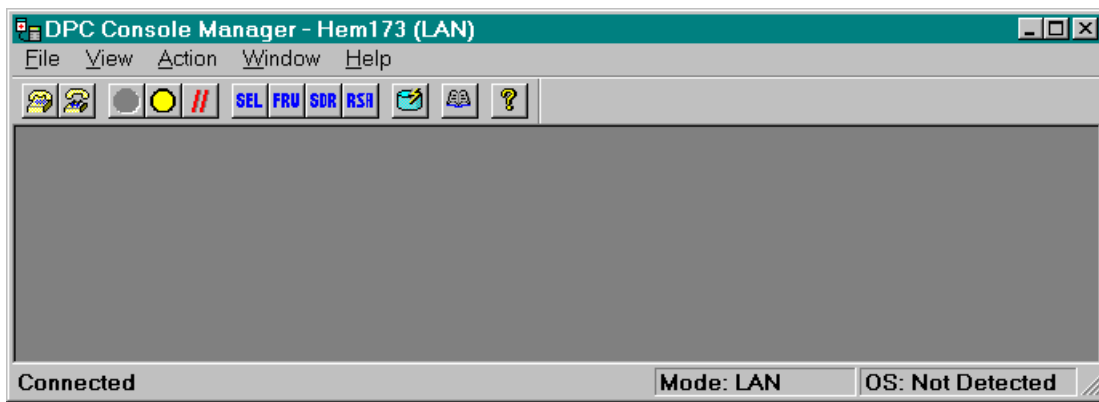


Figure 4 - 10: DPC Main Window

10.1.1 Main Window

The Main Menu options may be outlined as follows. Details of the Main Menu options follow in the sections below.

File Menu

- Connection
- Open
- Close
- Save As
- Print
- Phonebook
- MRU
- Exit

Connect Menu

New

Disconnect

Action Menu

Power On

Power Off

Reset

Reboot Service Partition

Configuration Status

View Menu

SEL Manager

SDR Manager

FRU Manager

RSA Manager

Toolbar

Status Bar

Window Menu

Close

Close All

Cascade

Tile

Arrange Icons

Help Menu

Help Topics

About

10.1.1.1 File Menu

The File menu provides standard file menu operations like Open, Close, Exit, etc. Menu items change depending on the active plug-in. When no plug-ins are active only “exit” menu item is displayed.

Table 4 - 4: File Menu - Options

Option	Description
Connection	The Connection menu item is a cascading menu that when selected has two elements, New... and Disconnect, which are used to connect and disconnect from a server and are described below. A menu separator appears after this item.
Open	The Open menu item displays the standard Windows File Open Dialog.
Close	The Close menu item closes the current view. If no view is present this item is grayed.
Save As	<p>The Save As... menu item saves information for the FRU, SEL and SDR Managers as described in the Common User Interface (UI) for SEL, SDR and FRU EPS document. If the FRU, SEL, RSA, or SDR Manager is not the active view this item is grayed.</p> <p>RSA Save As file format displays each tree item on a separate line with a blank line in between. If the tree item is a leaf the RSA Sensor information follows, one line for each piece of information. The entire tree and corresponding sensor information are saved to the file. The file has an RSA extension, but can be changed by the user in the File Save As dialog.</p>
Print	<p>The Print menu item prints information for the FRU, SEL and SDR Managers as described in the Common UI for SEL, SDR and FRU EPS document. If the FRU, SEL, RSA, or SDR Manager is not the active view this item is grayed.</p> <p>The RSA print format is similar to the SDR print format. Each tree item is printed with a blank line in between each item. If the item is not a leaf item it is bolded. If the tree item is a leaf the RSA Sensor information follows, one line for each piece of information. The selected tree item and all child items are printed. This means that if the root is selected, the entire tree is printed.</p>
Phonebook	For look and feel see the Phonebook section in the Phonebook and Connect Dialog Section.
MRU	The MRU is the Most Recently Used file list. Up to five file names will be displayed here. When a name is selected the file will be opened in the appropriate manager (FRU or SDR). See Open... for further discussion.
Exit	This option gracefully disconnects and cleans up, then terminates the execution of the DPC Console application. This option raises confirmation dialog before closing the application.

10.1.1.2 Connect

The Connect menu item is a cascading menu that when selected has two elements, New... and Disconnect, which are used to connect and disconnect from a server and are described below. A menu separator appears after this item.

Table 4 - 5: Connect Menu Options

Option	Description
New	<p>This menu item is used to initiate a connection with a server. This command terminates the existing connection if any, before initiating a new connection. The user is asked to confirm disconnect before initiating the re-connection. This menu displays the Connect dialog. The Connect dialog is shown below and is followed by a description of the controls and features of the dialog. The last selection made by the user is saved and when the dialog is shown again, these are the default selections shown.</p> <p>For look and feel see Connect Dialog in the and Collect Dialog section.</p>
	<p>Making a Connection:</p> <p>An EMP connection can be initiated in "dial-up" (modem and direct), or "LAN" modes. The DPC Console initially expects the server to be in the "EMP mode" of operation.</p> <p>If the connection is successful, the status bar indicates "Connected". If the "EMP Active" message is not received within 10 seconds it reports an "EMP not active" message and you will be disconnected from the server.</p> <p>Service partition is updated in the phonebook automatically, whenever a connection is made to the server and whenever server status and configuration is retrieved.</p>
	<p>Password Operation:</p> <p>When connecting to the server, the user is prompted to enter a password. If the server indicates the password is invalid, it reports back with a password error message and allows the user to enter the password again. If the user fails to enter the correct password in three successive attempts, the server rejects the password and locks up the interface for 30 seconds. The DPC Console displays a "Password rejected" message and disconnects the line.</p>
Disconnect	<p>This menu option is used to terminate the existing connection. The user will be asked to confirm the action. This action also closes any open managers (SEL, SDR, FRU, RSA). If the console is in Service Partition mode, disconnecting reboots the server out of Service Partition.</p>

When connecting to the server, the user is prompted to enter the password (16 characters maximum). If the server indicates that password is invalid, it reports back with a password error message and allows the user to enter the password again. If the user fails to enter the correct password in three successive attempts, the server rejects the password and locks up the interface for 30 seconds. The DPC Console displays "Password rejected" message and disconnects the line.

The DPC Console can enter redirect mode directly if the server is already in redirect mode and a connection is initiated. The EMP password entered by the user is stored and used for reconnection whenever the server switches from redirect mode to EMP mode. However, while in redirect mode, the user is prompted to enter the BIOS password if BIOS is setup with a password.

10.1.1.3 Action Menu

This menu is used to initiate an action with the remote server. When the user selects a menu item, the system checks the connection status and in the case of no connection, prompts the user with Connect dialog. The management plug-ins are launched only after establishing the connection. The menu items on this menu are as follows.

10.1.1.3.1 Power On

This menu item allows the user to power the server on, with post-power-up options. Clicking the menu item displays the Power On Dialog, shown below. Note that the dialog is different for serial, modem and LAN connections.

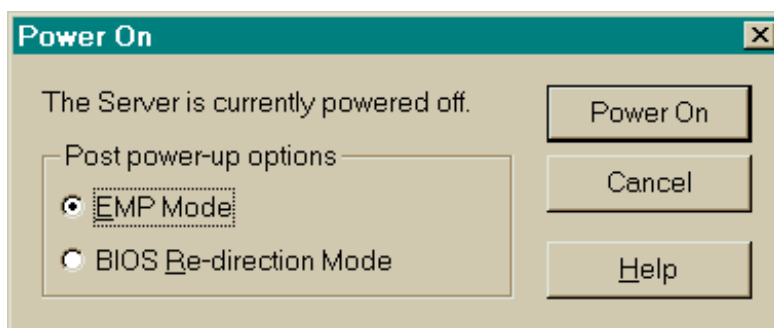


Figure 4 - 11: Power On Server Dialog - Serial Connection

Table 4 - 6: Power On with a Serial Connection Options

Option	Description
Post Power Up Options:	<p>These buttons allow the user to select the mode (EMP active or Allow BIOS Re-direct) effective for this power on operation. The default selection is EMP active.</p> <p>EMP Mode: This button sets the mode to EMP active for this power-on and the server will come up in EMP mode. The server will come up in EMP mode even though the Console Redirection is enabled on the server.</p> <p>BIOS Re-Direction Mode: Selecting this button, sets the server to come up in redirect mode for this power-on. The server switches to redirect mode only if the Console Redirection is enabled in the BIOS set up. In this case, the DPC Console displays a dialog "Server switched to Redirect mode. Switching to redirect mode".</p>
Power On:	Pressing this button powers on the server with the selected option.
Cancel:	Pressing this button dismisses the dialog with no further action taken. ESC will accomplish the same task.
Help:	Pressing the help button displays the usage information for the Power Off Server dialog in a help window. The key combination ALT-H will press the Help button.

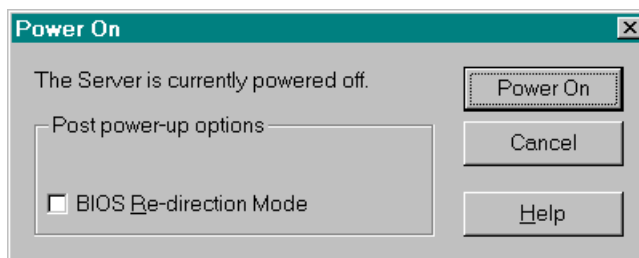


Figure 4 - 12: Power On - LAN Connection

Table 4 - 7: Power On with a LAN Connection Options

Option	Description
Post Power Up Options:	This button allows BIOS Re-direction Mode for this power on operation. The default selection is un-checked. EMP mode is always active for a LAN connection, which is why there is no option for this.
Power On:	Pressing this button powers on the server with the selected option.
Cancel:	Pressing this button dismisses the dialog with no further action taken. ESC will accomplish the same task.
Help:	Pressing the help button displays the usage information for the Power Off Server dialog in a help window. The key combination ALT-H will press the Help button.

10.1.1.3.2 Power Off

This menu item allows the user to power the server off. Clicking the menu item displays a confirmation dialog. When the server has powered off an informational message box telling the user if the power off action was successful is displayed.

10.1.1.3.3 Reset...

This menu item allows the user to reset the server with post power on options.

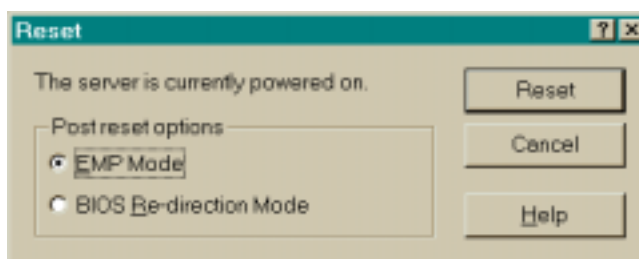


Figure 4 - 13: Reset - Serial Connection

Table 4 - 8: Reset with a Serial Connection Options

Option	Description
Post Power Up Options:	This group is used to select the power on option, i.e., EMP active or allow BIOS Re-direct, effective after reset. The default selection is EMP active. EMP Mode: Selecting this button sets the server in EMP mode after Reset operation. The server comes up in EMP mode even through the Console Redirection is enabled on the server. BIOS Re-direction Mode: Selecting this button with Reset operation sets the server to come up in redirect mode. The server switches to redirect mode only if the Console Redirection is enabled in the BIOS set up. In this case, the DPC Console displays a dialog “Server switched to Redirect mode. Switching to redirect mode”.
Reset Server:	Pressing this button initiates the System Reset with the selected options.
Cancel:	Pressing this button dismisses the dialog with no further action taken. ESC will accomplish the same task.
Help:	Pressing the help button displays the usage information for the connect dialog in a help window. The key combination ALT-H will press the Help button.

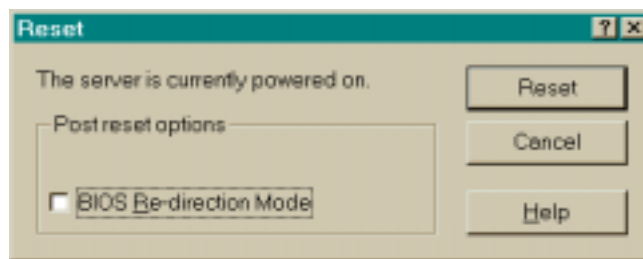


Figure 4 - 14: Reset Server Dialog - LAN Connection

Table 4 - 9: Reset with a LAN Connection

Option	Description
Post Power Up Options:	This group is used to select the power on option allow BIOS Re-direct, effective after reset. The default selection is un-checked. EMP mode is always active for a LAN connection, which is why there is no option for this.
Reset Server:	Pressing this button initiates the System Reset with the selected options.
Cancel:	Pressing this button dismisses the dialog with no further action taken. ESC will accomplish the same task.
Help:	Pressing the help button displays the usage information for the connect dialog in a help window. The key combination ALT-H will press the Help button.

10.1.1.3.4 Reboot Service Partition

This menu option is used to reboot the server from the service partition. When the user selects this option, a warning message requiring confirmation is displayed to indicate that the server is running an OS and a reboot will cause the OS to shutdown. A reboot will make all server services inaccessible to end-users.

This operation is allowed only when the DPC Console is in EMP mode and if the server's BIOS supports booting from a service partition installed on the local hard disk. Reboot to Service Partition can occur only if the server is not set in 'EMP Restricted Mode'.

After the "Reboot" command, the server enables console redirection and attempts to reboot from the service partition. The user can view all the pre-boot messages in the redirection window. In case BIOS fails to boot from the service partition, an error message will be displayed in the redirection window. In this case the user needs to terminate the service boot operation.

On successful completion of service boot, the status bar is updated accordingly. The menu options available are also updated based on the functionality available from Service Partition.

When the user is finished with Service Partition, they must select Reset (only for LAN connection) or Disconnect (LAN or Dial-up), to reboot the server out of Service Partition. A confirmation dialog will be shown prior to resetting the server.

While booted to Service Partition, the Service Partition menu is displayed. It has the following items:

- **Run DOS/EFI Shell**

This option is used to start a DOS or EFI command shell. The DOS or EFI command prompt can only be started when no other DOS or EFI based software is running. The DPC Console opens a redirection window to display the response and the keystrokes are transmitted to the server. The user may use the DOS or EFI command shell to change directory and run diagnostics or use the Action menu item.

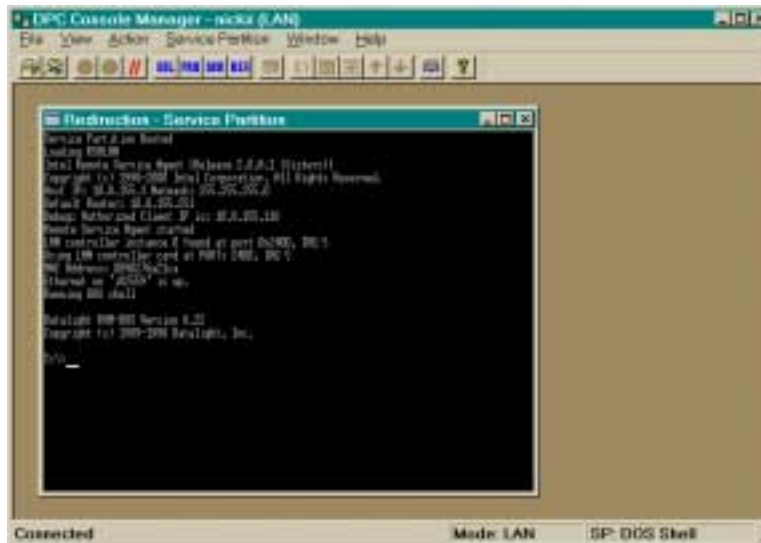


Figure 4 - 15: DOS Shell Window

- **Run Program**

This menu option is used to run a program on the server. This dialog behaves very similar to the Windows Run... option available from the Windows Start menu.

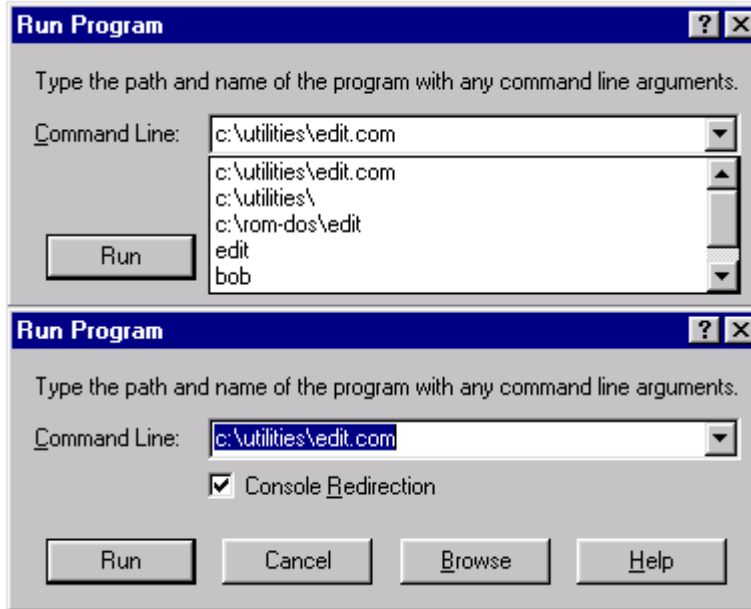


Figure 4 - 16: Run Program Dialog

Table 4 - 10: Run Program Dialog - Options

Option	Description
Command Line:	Type the path and filename of the program on the server to execute. In addition, command line option can be included. Optionally, select the command from the combo-box. The command can be edited and will be saved as a new entry if edited. The combo box is sorted by most recently used item.
Console Redirection:	Console redirection is checked by default. Uncheck this if no console redirection is required. If this is unchecked and a program does not terminate on its own, the user will be unable to run any other programs, dos shell, diagnostics or perform any file transfer operations.
Run:	Pressing this button executes the command line as given on the server. In addition, the entry is saved to the combo-box.
Browse:	When this button is pushed the standard Windows File Open dialog is shown as a directory browser. The files and directories listed are from the server. If a file is selected/ entered and OK is pressed the path and filename of the selected file (or a new file name entered by the user) will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Cancel:	Pressing this button dismisses the dialog with no further action.

- **Run Diagnostics**

This menu item is selected to run the diagnostics remotely on the server. This is a pre-configured DOS or EFI program with an exception that user cannot edit the program path. This action creates a redirection window and executes the diagnostic program, which launches the initial screen.

- **File Transfer**

This is a cascading menu used to transfer files between the Client and the Server in binary mode. The following menu items are provided:

- Upload...

This menu option is used to transfer files from the client to the server in binary mode. When the user clicks this menu option, a dialog is displayed with the following controls:

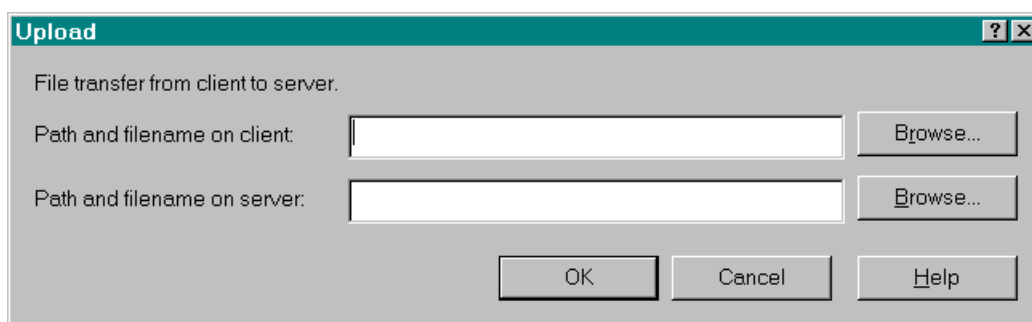


Figure 4 - 17: Upload Dialog

Table 4 - 11: Upload Dialog - Options

Option	Description
Path and filename on the client:	This is the directory structure and the name of the file that needs to be transferred. If this file does not exist on the client, an error message is displayed to the user.
Browse (client):	When this button is pushed the standard Windows File Open dialog is shown. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Path and filename on the server:	This is the directory path and the name of the file, as it will be stored on the server. If the directory structure does not exist on the server an error message is displayed to the user. The user can confirm the directory structure by using the browse capability. The user can use Run DOS/EFI Shell menu option specified earlier to create the directory path to be used here. If the file already exists, it will be over written. If no filename is provided, the client filename will be the default. The transfer is done in binary mode i.e. no conversion for CR-LF (carriage return and line feed is performed).
Browse (server):	When this button is pushed the standard Windows File Open dialog is shown as a directory browser. If a file is selected/ entered and OK is pressed the path and filename of the selected file (or a new file name entered by the user) will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
OK:	Press this button to start the upload process, after the correct file paths have been specified.
Cancel:	Click this button to dismiss the dialog, without uploading any file.
Help:	Click this button to view the help related with this dialog.

- **Download...**

This menu option is used to transfer files from the server to the client in binary mode. When the user clicks this menu option, a dialog is displayed with the following controls:

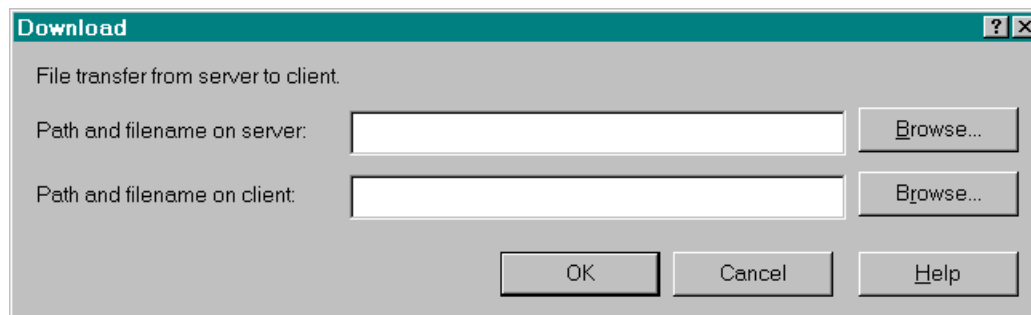


Figure 4 - 18: Download Dialog

Table 4 - 12: Download Dialog - Options

Option	Description
Path and filename on the server:	This is the directory structure and the name of the file that needs to be transferred. If this file does not exist on the server, an error message is displayed to the user. The user can confirm the directory structure by using the browse capability. The transfer is done in binary mode i.e. no conversion for CR-LF (carriage return and line feed is performed).
Browse (server):	When this button is pushed the standard Windows File Open dialog is shown. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
Path and filename on the client:	This is the directory path and the name of the file, as it will be stored on the client. If the directory structure does not exist on the client an error message is displayed to the user. If the file already exists it will be over written. If no filename is specified the server filename will be the default.
Browse (client):	When this button is pushed the standard Windows File Save dialog is shown as a directory browser. If a file is selected and OK is pressed the path and filename of the selected file will be placed in the edit control. If cancel is pressed the File Open dialog is dismissed and no information is changed in the edit control.
OK:	Click this button to start the download process, after the correct file paths have been specified. The named file is downloaded from the server to the client in binary mode.
Cancel:	Click this button to dismiss the dialog, without downloading any file.
Help:	Click this button to view the help related with this dialog.

- **Redirection View**

This is a checked menu item. If the service partition redirection view is visible, this item is checked. Selecting this menu item toggles the visibility of the service partition view.

10.1.1.4 Configuration Status Menu Item

This displays an information dialog that gives the chassis status and EMP configuration of the server. This information is available when the DPC Console successfully connects in EMP mode. The information is displayed in three groups with separate tabs for each group.

Service partition is updated in the phonebook automatically, whenever a connection is made to the server and whenever server status and configuration is retrieved.

- **Capabilities:**
This group gives the SEL, SDR, FRU, Power Inter Lock Status, Secure mode, and intrusion status.

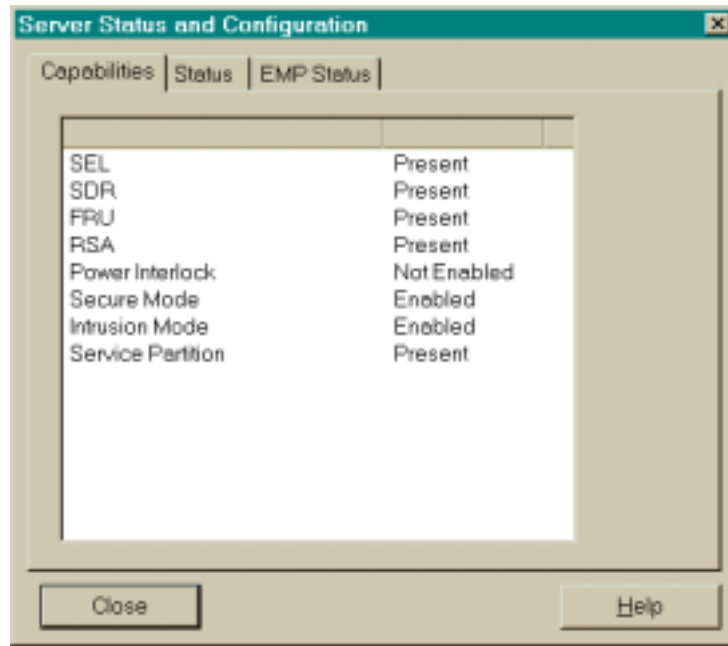


Figure 4 - 19: Configuration Status - Capabilities Screen

- **Status:**
Displays the Power status, Interlock active status, Power fault, Cooling fault, secure mode and intrusion active and OS run status.

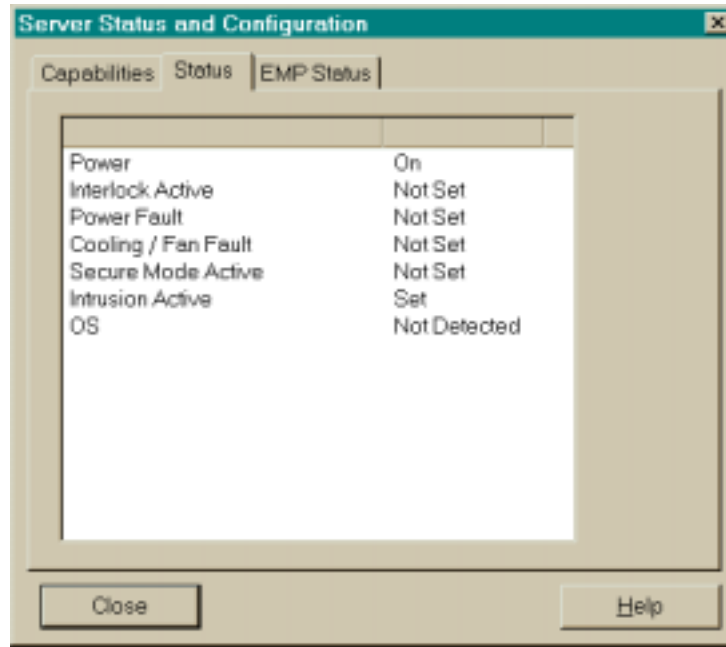


Figure 4 - 20: Configuration Status - Status Screen

- EMP Configuration:**
 Gives Restriction mode and Activation mode status.

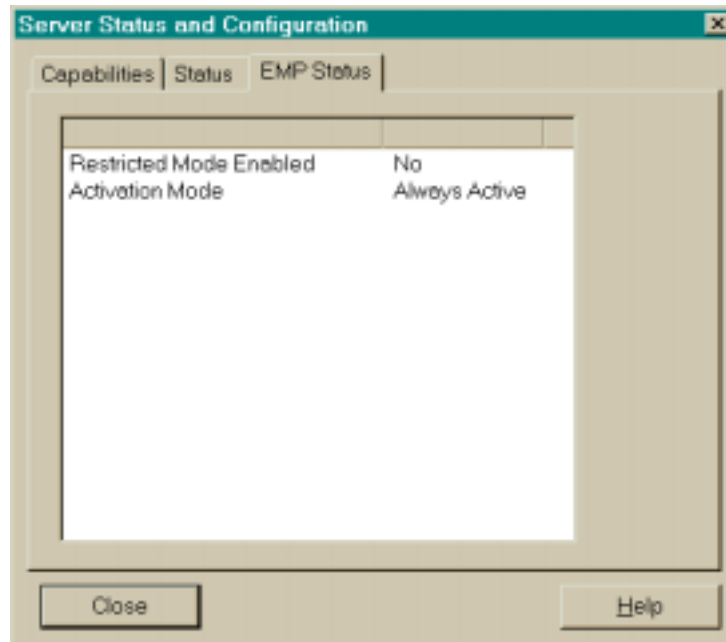


Figure 4 - 21: Configuration Status - EMP Configuration Screen

10.1.2 View Menu

The view menu is one of the main toolbar menus for DPC.

10.1.2.1 SEL Manager

The SDR Manager option loads the SEL Manager. When this option is selected, a Status Box is displayed to indicate that the manager is loading Sensor Event Log records from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If no server is connected when the SEL Manager is invoked, a Connect Dialog Box will appear.

See Section 13, SDR Implementation, for additional information.

10.1.2.2 SDR Manager

The SDR Manager option loads the SDR Manager. When this option is selected, a Status Box is displayed to indicate that the manager is loading Sensor Data Records from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If no server is connected when the SDR Manager is invoked, a Connect Dialog Box will appear.

See Section 13, SDR Implementation, for additional information.

10.1.2.3 FRU Manager

The FRU Manager option loads the FRU Manager. When this option is selected, a Status Box is displayed to indicate that the manager is loading Field Replaceable Unit information from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If the server is connected when the FRU Manager is launched, a Connect Dialog Box will appear.

See Section 13, FRU Implementation, for additional information.

10.1.2.4 RSA Manager

This RSA Manager option loads the RSA Manager. When this option is selected, Remote Sensor Access data is read from the server's baseboard FRU and SDR information area. All readings and display will be completely decoded based on the Intelligent Platform Management Interface (IPMI) 1.0 specification. The user will be given the option of choosing between Fahrenheit and Celsius for applicable fields via the RSA/Options menu item. This manager will display the value as it is retrieved from the server. The data does not update dynamically.

10.1.2.5 Toolbar

The Toolbar option provides the ability to selectively hide or show the toolbar. This option is always available, even if a manager is not currently active.

10.1.2.6 Status Bar

The Status Bar option provides the ability to selectively hide or show the Status Bar. The option is always available, even if a manager is not currently active.

10.1.3 Window Menu

This menu is used to manage the open windows in the console and contains the following items:

- Close
- Close All
- Cascade
- Tile
- Arrange Icons

10.1.3.1 Close

The Close menu item closes the current view. If no view is active, this item is grayed.

10.1.3.2 Close All

The Close All menu item closes all open views. If no views are open, this item is grayed.

10.1.3.3 Cascade

The Cascade menu item arranges all open views in a cascade pattern. One or more views must be open or this menu item is grayed.

10.1.3.4 Tile

The Tile menu item arranges all open views in a tiled pattern. One or more views must be open or this menu item is grayed.

10.1.3.5 Arrange Icons

One or more views must be open or this menu item is grayed.

10.1.4 Help Menu

The Help menu displays detailed information about the procedures and the options to operate the DPC console. This menu displays the following menu items.

- Help Topics
- About

10.1.4.1 Help Topics

The operating procedures are displayed in a separate window, i.e., help window. The help explains, the step-by-step sequence of various operations and options provided in the application.

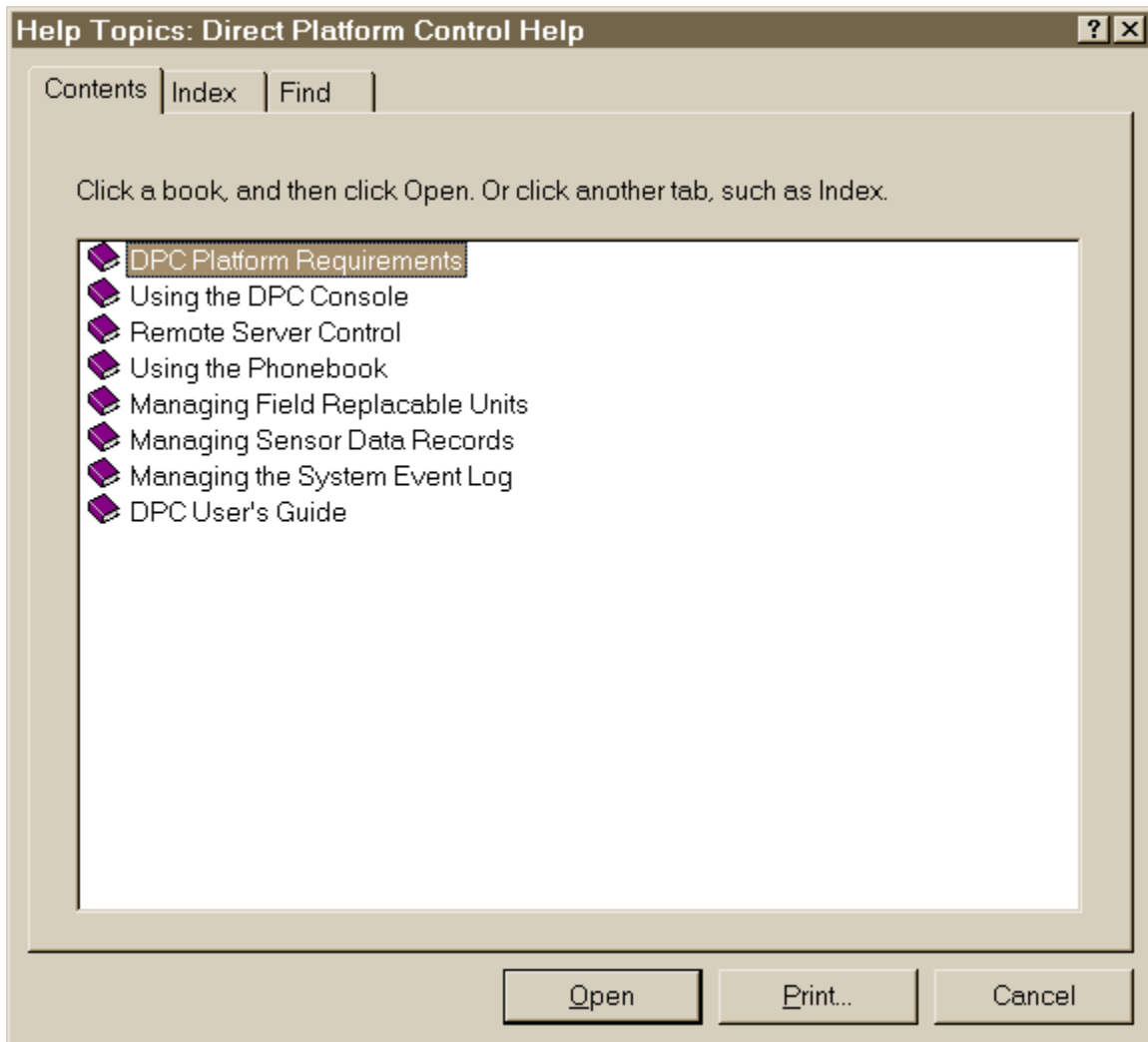


Figure 4 - 22: Help Topics Window

10.1.4.2 About The DPC Console

This option displays the version information and release build information for the product. If the current view is the SDR, SEL, RSA or FRU Manager this menu item is unique to the manager, see the *Common UI for SEL, SDR and FRU EPS* document for further explanation.



Figure 4 - 23: About the DPC Console Manager Dialog

10.2 Connection Menu

10.2.1 Connect Dialog – LAN or Direct

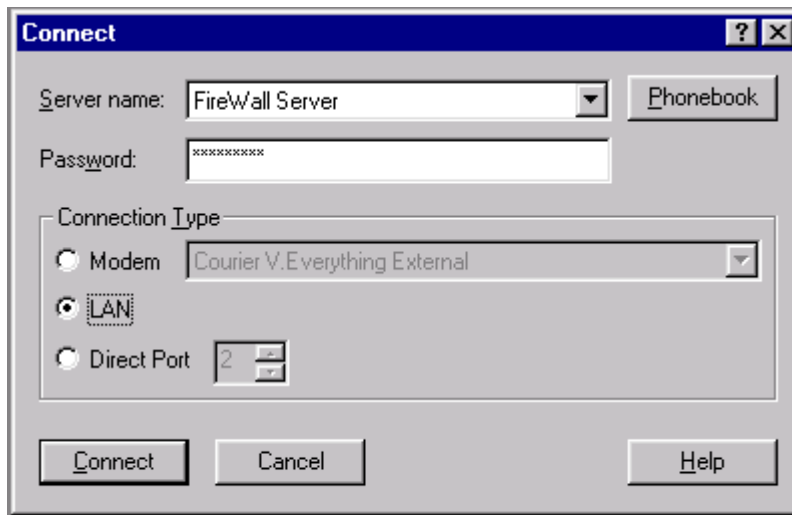


Figure 4 - 24: Connect Dialog - LAN

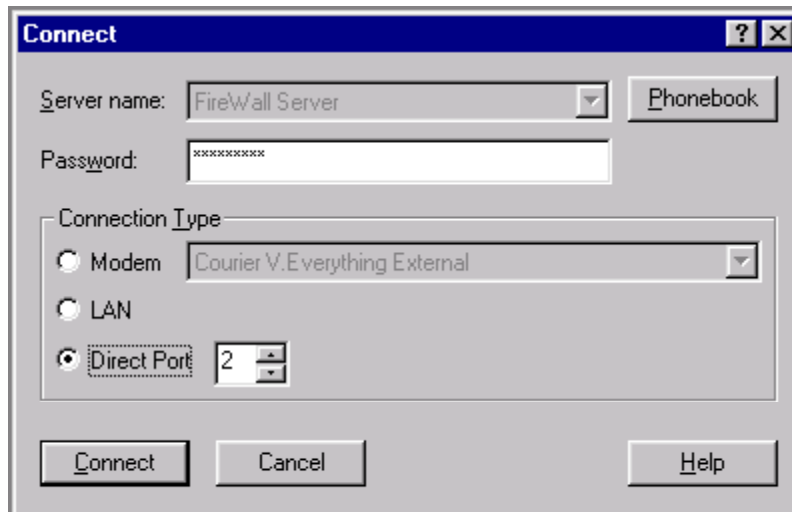


Figure 4 - 25: Connect Dialog - Direct

Table 4 - 13: Connect Dialog - Options

Options	Description
Server name:	This combo box is filled with server names from the phonebook.
Phonebook:	This button displays the phonebook dialog. When the user is finished editing the phonebook they are returned here and the Server name combo box is updated to reflect any changes.
Password:	This edit control is a password control. Text typed into the control is displayed with asterisks. The user types the password for the server selected in the Server name combo box. If this is a direct connection, the password is for the server connected with the serial cable.
Connection Type:	The user can choose Dial-up or LAN connections. The "RAS connections available" combo box is grayed if the user chooses a LAN connection. This combo box is filled with the RAS devices available for connection to a server.
Connect:	When the user presses the Connect button the dialog is dismissed and a connection is initiated.
Cancel:	When the user presses the Cancel button the dialog is dismissed and no further action is taken.
Help:	When the user presses the Help button, help is displayed for this dialog.

The user must enter either a phone number or a LAN address/DNS name. Both can be entered, but at least one must be entered.

10.2.2 Phonebook Dialog

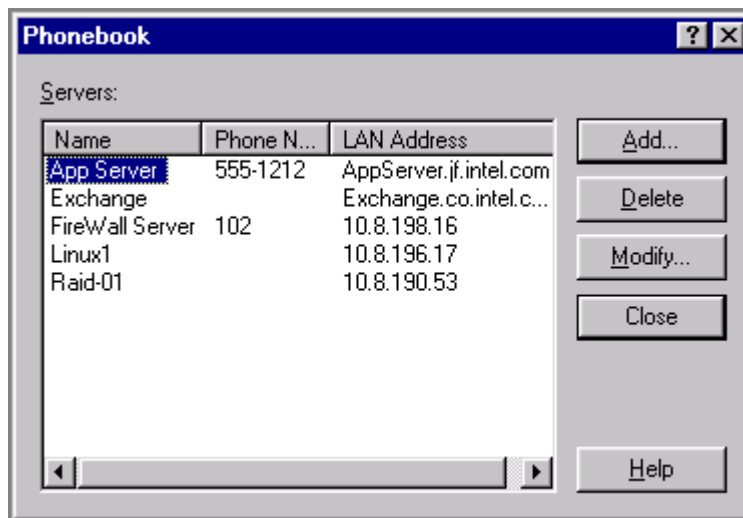


Figure 4 - 26: Phonebook Dialog

Table 4 - 14: Phonebook Dialog - Options

Options	Descriptions
Servers:	This is a list of servers derived from the phonebook file. Clicking on a header sorts the list. Clicking on the same header sorts the list in reverse order. Default sort order is Server Name in alphanumeric order.
Add:	Clicking on the Add button, displays the Add Phonebook Entry dialog. When the dialog is dismissed, the Servers list is updated to reflect any changes.
Delete:	Clicking on the Delete button, deletes the server entry selected in the Servers list from the phonebook file.
Modify:	Clicking on the Modify button, displays the Modify Phonebook Entry dialog. The Modify Phonebook Entry dialog is filled with the information for server selected in the Servers list. When the dialog is dismissed, the Servers list is updated to reflect any changes.
Close:	Clicking on the Close button dismisses the Phonebook dialog.
Help:	Clicking on the Help button displays help for this dialog.

10.2.3 Add Phonebook Entry

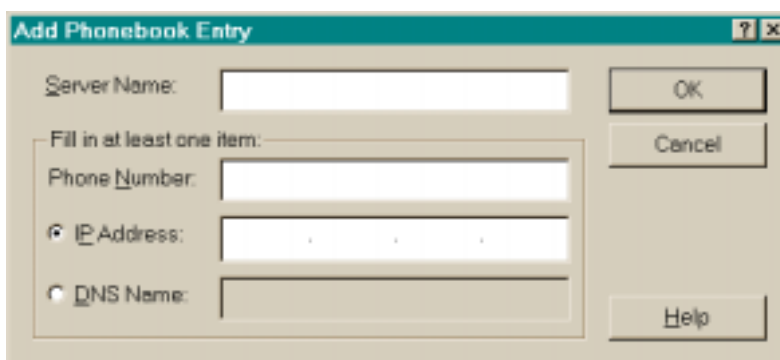


Figure 4 - 27: Add Phonebook Entry

Table 4 - 15: Add Phonebook Entry - Options

Options	Descriptions
Server Name:	The name of the server to add to the phonebook. The server name cannot already exist in the phonebook. This field must be filled in prior to clicking OK.
Phone Number:	The phone number of the server if connected by modem.
IP Address:	The IP Address of the server if connected by LAN.
DNS Name:	The DNS Name of the server if connected by LAN.
OK:	Pressing OK dismisses the dialog and adds the entry to the phonebook. If the Server Name already exists in the phonebook, a message is displayed to the user and the focus is set back to Server Name. Either the Phone Number or the IP Address / DNS Name must be filled in or a message is displayed to the user and the focus is set back to Phone Number.
Cancel:	Pressing Cancel dismisses the dialog and no further action is taken.
Help:	Pressing Help displays help for this dialog.

10.2.4 Modify Phonebook Entry



Figure 4 - 28: Modify Phonebook Entry

Table 4 - 16: Modify Phonebook Entry - Options

Options	Descriptions
Server Name:	Modify the name of the server here if desired. The name of the server must remain unique. It is not necessary to modify the server name.
Phone Number:	Modify the phone number of the server here if desired.
IP Address / DNS Name:	Modify the IP Address or the DNS Name here if desired.
OK:	Pressing OK dismisses the dialog and updates the phonebook file with the changes made. If the modified server name is not unique, an error is displayed to the user and the focus is set back to the Server Name field. If Phone Number or IP Address / DNS Name is not filled in, an error message is displayed to the user and the focus is set to Phone Number.
Cancel:	Pressing Cancel dismisses the dialog and no further action is taken.
Help:	Pressing Help displays help for this dialog.

11. Supported Features

The following table provides the list of supported features for DPC Console on supported platforms.

Table 4 - 17: DPC Console - Supported Features





Management plug-in	N440BX, T440BX, SC450NX, L440GX, C440GX+, Platforms	AD450NX, AC450NX Platforms	SPKA4
Server Control	√	√	√
Console Redirection	√	√	√
SEL Manager	√		√
SDR Manager	√		√
FRU Manager	√	√	√
RSA Manager			√
Service Partition			√
LAN			√
Auto Answer on Modem	√	√	









√ - Indicates support

11.1 Toolbar Buttons

The toolbar provides a shortcut to the functionality of the most commonly used menu items. The following is the list of toolbar buttons.

Table 4 - 18: Toolbar Buttons

Icon	Function	Corresponding Menu item	Description
	Connect	File: Connection / New	Displays the Connect dialog to initiate a connection
	Disconnect	File: Connection/Disconnect	Disconnects an existing connection
	Power On	Action: Power Control/Power On	Switches on the server power
	Power Off	Action: Power Control/Power Off	Switches off the server power

Icon	Function	Corresponding Menu item	Description
	Reset	Action: Power Control/Reset	EMP Mode: Resets the server with post reset options. Service Partition Mode: Resets the server out of Service Partition.
	SEL Manager	View: SEL Manager	Displays the SEL Manager
	SDR Manager	View: SDR Manager	Displays the SDR Manager
	FRU Manager	View: FRU Manager	Displays the FRU Manager
	RSA Manager	View: RSA Manager	Displays the RSA Manager
	Phonebook	File: Phonebook	Maintains entries for managed servers
	Reboot to Service Partition	Action: Reboot to Service Partition	Reboots the server to the Service Partition
	Help	Help: Help Topics	Displays the help topics

The status bar displays the status information in the following panes, when a new connection is initiated.

Table 4 - 19: DPC Status Bar Information

Screen location	Status information	Status description
1st pane (left most)	Server name	The server name is displayed when the connection is initiated on dial-up line. This field is blank for direct line connection.
2nd pane	Line	Displays line selection i.e., "Direct, LAN, or "Dial-up".
3rd pane	Mode	Indicates one of the console modes i.e., "EMP" or "Redirect" or "PPP" or "PPP-Redirect", or TCP (LAN).
4th pane (right most)	Line Status	Indicates all the status and error information while initiating connection and disconnection. Once the connection is successfully completed, it displays "Connected" throughout the DPC Console operation and then "Disconnected" when the line is disconnected.

This page intentionally left blank

Intel® Server Control, Version 3.x

Section 5: Service Partition

Table of Contents

1. Introduction to the Service Partition	1
2. Service Partition Boot	2
2.1 Firmware / BIOS Service Boot Support	2
2.2 BIOS Setup Partition Type Configuration	3
2.3 Remotely Initiating Service Partition Boot.....	3
2.4 Local Boot from Service Partition	3
3. Service Partition Installation.....	4
3.1 SCAN and PRESENT Bits.....	4
4. Service Partition Operating System	5
4.1 Service Partition OS Installation	5
4.2 Service Partition OS / Country Kit CD Hidden Partition Support.....	5
4.3 Service Partition OS Initialization.....	5

List of Figures

Figure 5 - 1: Service Partition..... 1

List of Tables

No tables appear in this section.

1. Introduction to the Service Partition

The Service Partition is installed on a separate file system partition on the server. It hosts the DOS / ROM-DOS / Extensible Firmware Interface (EFI) operating system, System Setup Utility (SSU), and Diagnostics agents and tests, and is used to run DOS-based applications and diagnostics – those Intel® Server Control (ISC) functions that require access to local, writable media. The Service Partition also supports the redirection of a text-based console over all of the supported communication paths.

The DOS operating system is configured with the Transmission Control Protocol / Internet Protocol (TCP/IP), Point-To-Point Protocol (PPP) and File Transfer Protocol (FTP) protocols, standard communication stacks that can be used over a modem, Local Area Network (LAN) connection, or a serial port to support remote control of SSU, diagnostics or any other utility designed to be compatible with this environment.

The Client SSU and Diagnostics agents are used to communicate with the remote console applications. The Client System Setup Utility (CSSU) and the Diagnostics components of the ISC product rely on the server’s Service Partition, illustrated in the following diagram

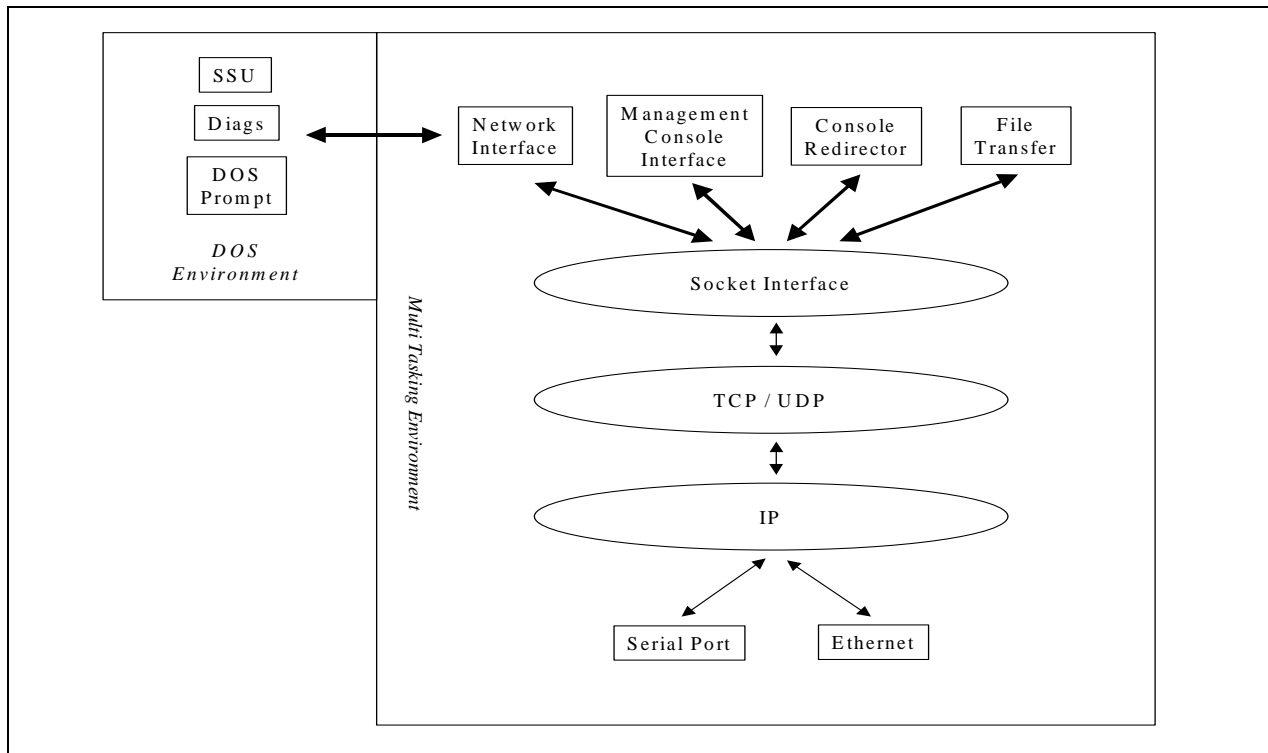


Figure 5 - 1: Service Partition

2. Service Partition Boot

Using the capabilities provided by Direct Platform Control on the console and the Platform Management Technology on the server, the management console can make a modem or LAN connection to a target server, regardless of the operational state of the server. The console may then instruct the target server to boot from the Service Partition.

The following components of the Platform Management Technology on the server provide the capabilities to remotely boot the server in the Service Partition mode:

1. Emergency Management Port (EMP) firmware running on the target server
2. BIOS Console Redirection for remote access to pre-boot BIOS setup
3. BIOS support on the target server for booting from a Service Partition
1. A service Operating System (OS) such as DOS/EFI or ROM-DOS installed on the Service Partition at the target server

The Baseboard Management Controller (BMC) supports a remote command, which instructs it to change the BIOS boot order to boot from the Service Partition. This command may be issued over any of the supported DPC communication paths to the target server.

The DPC then determines if the target server is running a functional operating system. If so, the DPC issues a request to an operating system agent on the server to shutdown and reboot the system. If this communication fails, the DPC issues a request to the firmware controllers to reset the system.

When the OS agent or the firmware controller executes the command to reset the system, the BIOS boots the DOS operating system from the Service Partition. The agents on the Service Partition are invoked, and they establish communication with the remote console using the same communication path. When the session between the agents and the console is concluded, the normal boot order is restored before the system is rebooted.

In addition to the remote Service Partition Boot, the Server may also be booted to the Service Partition locally by configuring the BIOS (in BIOS setup) to perform a one time boot from the Service Partition. Once the utilities and the tests are executed on the Service Partition, the system may be rebooted. The BIOS reverts to the normal boot order after the reboot.

2.1 Firmware / BIOS Service Boot Support

The firmware maintains three bits related to booting from the service partition.

4. BOOT bit: Request BIOS to perform a service partition boot
5. PRESENT bit: Service partition is present.
2. SCAN bit: Request BIOS to detect presence of service partition.

These bits are described in more detail in the sections that follow.

The BIOS and firmware also include support for a service boot watchdog timer. Prior to transferring control to the service partition, the BIOS starts a timer in the firmware. If software

on the service partition fails to boot and stop the timer, the handler for the timer restarts the system to the system normally.

2.2 BIOS Setup Partition Type Configuration

BIOS setup has an option to change the partition type. It defaults to type 98h, but can be changed to allow Original Equipment Manufacturers (OEMs) to utilize other types of service operating systems. However, the service operating system described in this document requires the partition type to be 98h.

2.3 Remotely Initiating Service Partition Boot

When the management console connects to the target server, it communicates with the server's EMP interface. An EMP command is sent from the management console to set the BOOT bit. The next time the target server boots, the BIOS checks the BOOT bit to determine if it should boot from the service partition.

If the BOOT bit is set, the BIOS does the following:

1. It enables the BIOS console redirection, even if it is not enabled in the normal BIOS setup, using the same serial port settings as EMP. This allows the remote user access to BIOS setup and the ability to see BIOS screen messages.
2. The BIOS searches the partition table for a partition type that uniquely identifies it as a service partition. The BIOS always clears the BOOT bit whether or not a service partition is found to prevent repeated attempts at booting to the service partition.
3. If a service partition is found, the BIOS sets the PRESENT bit, then loads and transfers control to the service partition boot sector. If a service partition is not found, the BIOS clears the PRESENT bit and boots normally.

or

If the BIOS does not find a service partition, it displays an error message on the screen and logs an error to the System Event Log. The user at the management console will see the error message via BIOS console redirection.

2.4 Local Boot from Service Partition

It is possible to boot the server from the service partition while working at the server console. This feature allows the user to run utilities from the service partition while physically present at the target server.

To activate a local boot from the service partition, the user must shutdown and restart the server, and then enter BIOS setup. In BIOS setup, the user enables a one-time boot from the service partition and reboots the system. After the system boots from the service partition, a command-line interface is available to allow the user to execute any software that has been installed on the service partition, or to load new software from the floppy diskette drive.

3. Service Partition Installation

The service partition must be available before the target server can be managed remotely. Installation of the service partition is accomplished in two steps, using utilities on the Country Kit CD.

1. A utility called Service Partition Administrator, which is similar to the DOS FDISK utility, is used to create the service partition. The system then reboots.
2. The service partition is formatted and software is installed onto it using another function of the Service Partition Administrator.

Following the successful installation of the service partition, the installation software sets the PRESENT bit.

The service partition is 39 MBs in size and is formatted with a FAT16 file system. However, to complete the installation of the service partition, there must be at least 40 MBs of un-partitioned space available on the system hard drive. The service partition can only be created on the first 8 GBs of available space on the system hard drive.

If the end user installs a new or replacement disk, the service partition should be installed prior to the installation of the end user OS. Users wishing to install the OS first must preserve sufficient space on the disk if they intend to install the service partition later. The service partition install process does not have the ability to resize existing partitions.

3.1 SCAN and PRESENT Bits

Each time the BIOS boots, it checks the SCAN bit. If the SCAN bit is set, the BIOS checks for the presence of a service partition. Depending on the outcome of the check, BIOS either sets or clears the PRESENT bit. Note that the PRESENT bit is also be set during the service partition installation. After the scan, BIOS clears the SCAN bit.

The PRESENT bit is used to aid in discovering servers that have a service partition installed. Its state should always indicate whether a service partition is installed. The SCAN bit is used to maintain the accuracy of the PRESENT bit. For example, if the disk containing a service partition is replaced, the PRESENT bit will incorrectly indicate that a service partition exists.

4. Service Partition Operating System

The service OS is a DOS-compatible / EFI operating system capable of hosting utilities, diagnostics and any other software required for remote management. It resides on the hidden service partition. The following sections describe the use of a service operating system.

4.1 Service Partition OS Installation

The service partition OS is installed following the creation of the hidden service partition. Installation is accomplished through utilities and batch files stored on the Country Kit CD.

4.2 Service Partition OS / Country Kit CD Hidden Partition Support

A special version of DOS is used to provide support for the hidden partition, which is not a normal, DOS-compatible type of partition. Therefore, the version of DOS that is installed on both the Country Kit CD and the hidden partition contains support to create and recognize the special hidden partition type.

4.3 Service Partition OS Initialization

When the service partition OS begins to run, software and drivers needed to initialize the remote environment are loaded through the config.sys and autoexec.bat files.

< This page intentionally left blank. >

Intel® Server Control, Version 3.x TPS

Section 6: Diagnostic Test Package

Table of Contents

1. Introduction to the Diagnostic Test Package	1
2. Remote Diagnostics	2
3. Test Descriptions.....	3
3.1 Processor FRU Tests	3
3.2 Baseboard FRU Tests.....	3
3.3 Memory FRU Tests	5
3.4 Hard Disk Drive FRU Tests	5
3.5 Floppy Disk Drive FRU Tests	6
3.6 SCSI CD-ROM Drive FRU Tests	6
3.7 Hot-Swap SCSI Backplane FRU Tests.....	6
3.8 Front Panel Enclosure FRU Tests.....	7
3.9 Power Share Backplane FRU Tests.....	7
4. Test Selection Menu Display.....	8
5. DiagWiz Hardware Configuration (dwizcfg.exe).....	9
5.1 DiagWiz Display FRU Status.....	9
6. Server Test Package.....	11
6.1 Test Packages	11
6.1.1 Quick Test.....	11
6.1.2 Comprehensive Tests	12
6.1.3 Comprehensive Tests with Continuous Looping.....	12
7. Test List.....	13

List of Figures

Figure 6 - 1. Service Partition-based Remote Diagnostics 2

Figure 6 - 2. Execution of the Testmenu.bat File 8

Figure 6 - 3. DiagWiz Test Configuration Screen Display..... 9

Figure 6 - 4. DiagWiz FRU Status Display..... 10

List of Tables

Table 6 - 1: Processor FRU Tests 3

Table 6 - 2: Baseboard FRU Tests 3

Table 6 - 3: Memory FRU Tests 5

Table 6 - 4: Hard Disk Drive FRU Tests 5

Table 6 - 5: Floppy Disk Drive FRU Tests 6

Table 6 - 6: SCSI CD-ROM Drive FRU Tests 6

Table 6 - 7: Hot-Swap SCSI Backplane FRU Tests 6

Table 6 - 8: Front Panel Enclosure FRU Tests 7

Table 6 - 9: Power Share Backplane FRU Tests 7

Table 6 - 10: Diagnostics Test List 13

1. Introduction to the Diagnostic Test Package

This section describes the off-line diagnostic tests that are available on Intel server platforms. It discloses a description of Modular Test Architecture (MTA) modules that are utilized to provide local test coverage for various platforms. It also provides information about non-generic tests that are developed to address unique server specific, diagnostics coverage requirements. This section includes:

- Remote diagnostics
- Test descriptions
- Diagnostic Wizard

Note: The remote diagnostics package is installed on the Service Partition. These off-line tests require a DOS environment (Service Partition) to be loaded on the server before they can be executed.

The goal of the test package is to identify hardware failures at the Field Replaceable Unit (FRU) level on Intel servers. Each supported FRU has one or multiple test modules associated with it. A test module is a group of tests that directly or indirectly tests a FRU. The tests sense hardware components then test the hardware that is detected. The results of FRU test failures are saved in a results file, TEST.SUM.

As an added feature, a Diagnostic Wizard is included and invoked at the completion of the test package to display the hardware configuration, analyze the test results, and display the pass or fail results for each FRU

The test package provides an easy to use interface with an the average test completion time of less than 20 minutes, depending upon the number of disk drives and the amount of memory installed. The tests are leveraged and ported to meet the requirements of the service partition from the Modular Test Architecture test suite.

2. Remote Diagnostics

The following diagram displays the architecture of the diagnostics.

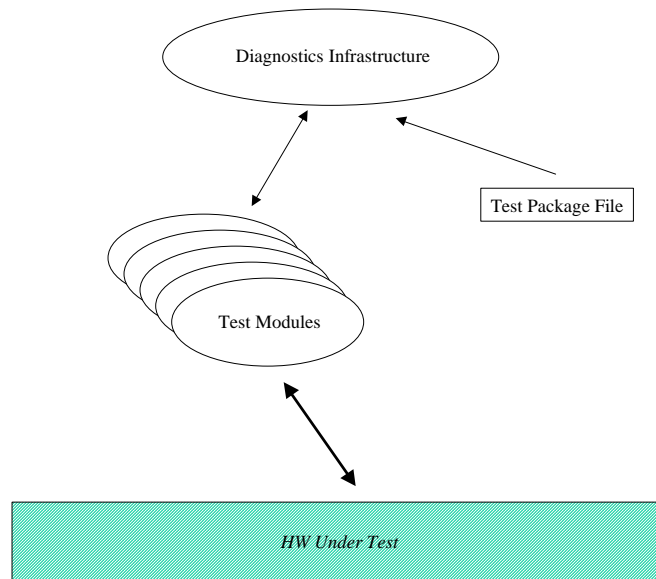


Figure 6 - 1. Service Partition-based Remote Diagnostics

The infrastructure relies on a test package file to determine the test modules and associated test parameters that it needs to run. The infrastructure automatically discovers the system configuration, displays it to the user, and runs the tests that the user selects. Upon completion of the tests, the test results are displayed for the user.

All user interactions are handled through the console. The console redirector, in conjunction with underlying off-the-shelf communication stack, enables remote control of the user interface.

The tests support online help that is available on the local server and viewable through console redirection. The user interface is provided by the Build Your Own (BYO) and/or MTA diagnostics and will differ from the general look and feel of Direct Platform Control (DPC).

3. Test Descriptions

This section provides examples of the type of tests available for each FRU. In general, the subsections below relate to tests for a particular FRU, although in some cases tests apply to more than one FRU because of the organization of the test modules. Some tests may not be included because they are not appropriate for this test environment. These include tests such as those that require loop-back cables.

3.1 Processor FRU Tests

The following tests check the processor on the baseboard.

Table 6 - 1: Processor FRU Tests

Test	Description
Central Processing Unit (CPU) Tests	This test module ensures that the correct processor is installed in a board or system, and that the correct clock speed has been selected.
Floating-Point Unit (FPU) Tests	This test module verifies that the FPU is present on the board or the system and that the FPU is functional.
Processor Board Controller Tests	This test module checks the I ² C application command interface protocol between the baseboard I ² C Controller and the Processor Board Controller (PBC 8xC751).

3.2 Baseboard FRU Tests

The following tests check various parts of the baseboard.

Table 6 - 2: Baseboard FRU Tests

Test	Description
T82430 Tests	This test module is designed to verify the type of system controller on the Unit Under Test (UUT) and whether the Dual In-Line Memory Modules (DIMMs) plugged into the UUT are the expected size, type, and in the expected position. This also tests for the presence of the proper DIMM type to support Error Correction and Detection (ECC) feature of the chip set.
Cache Tests	This test module checks for the presence of caches in a board or system and verifies the functionality of the caches.
Chipset Tests	This test module ensures that the chipset is functioning properly, and looks at whether the DIMMs plugged into the UUT are the expected size, type, and in the expected position.
PCI Tests	This test module is designed to test the functionality of the Peripheral Component Interconnect (PCI) bus.
PCI/ISA/IDE Accelerator Tests	This MTA module is designed to verify functionality of the PCI / Industry Standard Architecture (ISA) / Integrated Drive Electronics (IDE) Xcelerator (PIIX4) device.
Snooping Tests	The purpose of this module is to validate the functionality of the snoop phase by testing system cache coherency.
POST Results Test	The purpose of this test module is to report any errors that occurred during Power on Self-Test (POST), and compare the memory size reported by POST

Test	Description
	with expected values. All POST information is read from Complementary Metal-Oxide Semi-Conductor (CMOS) Random Access Memory (RAM).
Serial I/O Tests	This test module is designed to test the functionality of the serial ports.
Keyboard Tests	This test module is designed to check the keyboard controller, mouse port and keyboard Light Emitting Diodes (LEDs).
Parallel Port Tests	This module is designed to test parallel port presence and functionality.
Mouse Tests	This test module is designed to check the Mouse Interface.
Programmable Interval Timer (PIT) Tests	PIT tests are designed to work with systems that have one or two timers. The parameter found in pit.cfg, pit.first, should be set to either one or two depending on how many timers are in the system.
Real-Time Clock (RTC) Tests	This test module was designed to test the Real Time Clock logic of a PC based system. It tests the CMOS RAM, clock and battery.
Direct Memory Access (DMA) Controller Tests	This test module is designed to check the DMA Controller.
Platform Instrumentation Control (PIC) Tests	This test module was designed to test the Interrupt logic on a PC based system.
Server Management Interrupt (SMI) and Non-Maskable Interrupt (NMI) Tests	This test module was designed to test the SMI and NMI interrupts. smi_nmi.exe is the test program for this module. It provides tests for the SMI, and Event Logging. It also has a test that fails on any error in the SMI Error Log. It provides two utilities for looking at the Event Log area of flash. The first lists the system configuration data, and the second lists all errors in the SMI Error Log.
Super I/O Tests (sio308.exe)	
Baseboard Management Controller (BMC) Tests	This module checks the command interface protocol for the Baseboard Management Controller.
Cirrus Logic* Video Controller Tests	This test module checks the functionality's of the Super Video Graphic Array (SVGA) Cirrus Logic CL GD542X/GD543X/GD544X video controllers. These controllers provide integrated RAM Digital-To-Analog Converter (RAMDAC), oscillator circuitry and video controller in one component.
VGA-Compatible Video Controller Test	This test module checks the functionality's of the VGA-compatible video controller, the video RAM (256 K), and video DAC. The operations of the video controller at low and high-resolution displays (character and graphics) are also verified.
Small Computer Systems Interface (SCSI) Controllers Test	This MTA module is designed to verify the functionality of the SCSI Controllers.
LED Tests	The purpose of this test module is to ensure that various LEDs on the UUT are connected and functioning properly. All tests in this module are interactive.
82440 PCI Bridge and Memory Controller Tests	The purpose of this module is to ensure that the PCI bridge and memory controller, is functioning properly, and whether the SIMMs plugged into the UUT are the expected size, type, and in the expected position. The PCI module and MSDRAM module may be used in addition to this module for further PCI bus and memory address lines testing.
Video Controller Tests (vid_wd.exe)	This test module checks the functionality's of the video controller, the video RAM, video DAC, video oscillator and supportive circuitry's. The operations of the video controller at low and high-resolution displays are also verified.
Universal Serial Bus (USB) Controller Tests	This test module verifies the functionality of the Universal Serial Bus (USB) host controller.
Server Management Bus (SMB) EEPROM Tests	This MTA module is designed to verify functionality of EEPROM devices with SMB (I ² C) interface.
Super I/O (SIO) Tests	The purpose of this module is to test the functionality of the Super I/O. The RTC, Universal Asynchronous Receiver/Transmitter (UART), Parallel Port, Floppy Disk Controller (FDC) and keyboard modules may be used in addition to this module for further testing in those areas.
PCI / IDE / ISA Accelerator	This module contains tests the registers and some general functionality of the

Test	Description
Tests	PIIX device.
PCI to Xpress Bus Bridge (PCXB) Tests	This test module is designed to test the functionality of the PCI to Xpress Bus Bridge (PCXB). This chipset consists of one control Application Specific Integrated Circuit (ASIC) X Performance Characterization (XPC) and one or two data ASICs (XPDs).
PCI Bridge Tests	The purpose of this module is to ensure that the PCI bridges are functioning properly, and to check for the correct number of bridges in a system.
Memory controller Tests	This module makes sure that the memory controllers are functioning properly, and checks for the correct number of memory controllers in a system.
I ² C Multiplexer (MUX) Tests	This module tests the DMI interface protocol for the I ² C MUX chip.
Advanced SCSI Programming Interface (ASPI) Tests	This module tests SCSI devices at the ASPI interface. ASPI is a software interface used by SCSI host adapter (controller card) drivers. By using an interface common to most (if not all) SCSI controllers, this test can be run on any machine that has the proper ASPI driver installed.
Advanced Integrated Peripheral (AIP) Controller Tests	This module tests features of the Advanced Integrated Peripheral (AIP) I/O controller.

3.3 Memory FRU Tests

These tests verify the functionality of the DRAM and cache memory on the board or system under test.

Table 6 - 3: Memory FRU Tests

Test	Description
Memory Tests	This test module is designed to verify the functionality of the DRAM and cache memory on the board or system under test.
Memory Stress Tests	This test module stresses the memory by performing random operations with random data to simulate system OS operation.

3.4 Hard Disk Drive FRU Tests

These tests check access to hard disk drives. Included are tests for hard disks that are attached to the baseboard via the IDE bus and disks that are used with RAID software.

Table 6 - 4: Hard Disk Drive FRU Tests

Test	Description
Hard Drive BIOS Tests	HDBIOS.EXE is a series of tests designed to test hard disks at the BIOS level of compatibility. The tests use only the documented BIOS INT 13H Fixed Disk Service functions.
IDE Tests	This test checks certain commands of IDE hard drives that HDBIOS cannot check.

3.5 Floppy Disk Drive FRU Tests

These tests check the Floppy Disk Drive units.

Table 6 - 5: Floppy Disk Drive FRU Tests

Test	Description
ISA Floppy	This test checks the Floppy drives on a PC based system.

3.6 SCSI CD-ROM Drive FRU Tests

These tests check the CD-ROM Drive Unit board.

Table 6 - 6: SCSI CD-ROM Drive FRU Tests

Test	Description
SCSI CD-ROM	This module tests the functionality of CD-ROM drives. The INTELPCDIAG companion disk provides audio and data tracks for use during the test.

3.7 Hot-Swap SCSI Backplane FRU Tests

These tests check the Hot-Swap Backplane.

Table 6 - 7: Hot-Swap SCSI Backplane FRU Tests

Test	Description
I2CHSPCA Tests	This module checks the I ² C Application Command Interface Protocol between the baseboard I ² C controller and the I ² C-compatible microcontroller on the hot-swap backplanes.
Hot Swap Backplane Controller Tests	This module checks the I ² C Application Command Interface Protocol between the baseboard I ² C controller and the I ² C-compatible microcontroller on the hot-swap backplanes.

3.8 Front Panel Enclosure FRU Tests

These tests check the Front Panel in the enclosure.

Table 6 - 8: Front Panel Enclosure FRU Tests

Test	Description
I2CFPPCA tests	This module checks the I ² C Application Command Interface Protocol between the baseboard I ² C Controller and the I ² C-compatible Microcontroller on the POCA front-panel controller.
Front Panel Port Tests	FPANEL.EXE consists of a single test designed to test the front panel port. The test assumes that the hardware attached to the port is an Liquid Crystal Display (LCD) controller chip.
Front Panel Controller Tests	This module checks the I ² C Application Command Interface Protocol between the baseboard I ² C Controller and the I ² C-compatible Microcontroller on the front-panel controller.

3.9 Power Share Backplane FRU Tests

These tests check the Power Share Backplane.

Table 6 - 9: Power Share Backplane FRU Tests

Test	Description
Power Share Controller Tests	This module checks the I ² C application command interface protocol between the baseboard I ² C Controller and the I ² C-compatible microcontroller on the Power Share Controller (PSC 8xC751).
Advanced Power Management (APM) Tests	The purpose of this module is to test Advanced Power Management (APM) functionality in APM compliant systems.

4. Test Selection Menu Display

Runtest is called from the testmenu.bat file and displays a list of test packages to be run. The selection is made by using the UP/DOWN Cursor controls and pressing the ENTER key:

```
L440GX Version 1.0 ©Copyright 1999 Intel Corp. All Rights Reserved.  
  Server Diagnostics Options  
    Quick Test  
    Comprehensive Tests  
    Comprehensive Test with Continuous looping  
  Highlight selection-using Cursor UP/DOWN and press ENTER
```

Figure 6 - 2. Execution of the Testmenu.bat File

Runtest issues a system call to execute T.exe, the diagnostics controller, and places the package selected on the command line. The TEST.SUM file is deleted before each test package is called to assure that only the results of the current test run are reported. After each test selection is made, a check of the bios_id.out file is made to determine if the system is appropriate for the test package. The bios_id string is compared with the BIOS_ID in the test package. If they do not match, the following error message is displayed and runtest ends.

```
This Baseboard is not supported by this test.
```

```
Press any key to exit.
```

5. DiagWiz Hardware Configuration (dwizcfg.exe)

The Hardware Configuration Utility displays a list of the hardware components that the test modules detected during the self-sense probe. The display consists of the hardware component and its size or status. This helps the BYO determine the hardware configuration to test. The user is asked to respond with ENTER if the configuration is correct or CTRL+BREAK if it is not correct.

Dwizcfg opens the display.cfg file created by T during self-sense operation. Key words are filtered out to prevent information from being displayed that is not useful or is confusing. The result is a list of hardware components and the size or status. A sample of the display follows:

```
DiagWiz Test Configuration (v0.3)

Base Memory Size: 640 KB
Cpu Type: A Pentium ® II Processor
Cpu Speed: 450 MHz
CPU SMP #0: Present
CPU SMP #1: Present
Keyboard-type: 101-Key
Mouse Enabled
RTC RAM SIZE 128
Number of SCSI channels: 2
COM2 at Port Address: 2F8 is enabled
LPT1 0x378
Floppy cfg.drive A: 1.4Mb (3.5 Inch)
Hard Drive 0 Cylinders:531 Heads:255 Sectors:63 Total Size":4157MB
Video Subsystem: Curris 5446 controller, 1024 K video RAM
External Cache Size: 512 KB
Memory Size: 96 Meg

If Configuration is correct press ENTER to continue or CTRL+BREAK to quit
```

Figure 6 - 3. DiagWiz Test Configuration Screen Display

If CTRL+BREAK is pressed dwizcfg exits and control is returned to the test selection menu (runtest.exe) after displaying a message instructing the user to check all hardware and cable connections. If ENTER was pressed, indicating that the configuration is correct, the test is started. Upon completion of testing, dwizstat.exe is executed to display the test results indicating pass or fail status of each FRU and its associated test modules.

5.1 DiagWiz Display FRU Status

The Display FRU Status Utility displays a list of the pass or fail status for the FRUs tested and the corresponding test modules. The name of a FRU in which all the sub-tests have passed is displayed in green with PASSED displayed to the right. If a FRU failed, the FRU name and failing test module name will be displayed in red, along with a FAILED string.

The dwizstat utility opens the test.sum file. Test.sum is created by T or Testview and contains a list of all tests run and the pass or fail status of each test. Many tests are run for each test module. Dwizstat reads a line from test.sum to determine the test module name and then scans subsequent lines to determine if any of the associated tests failed. If failures are encountered, a flag is set for later use. This operation continues until the end of the file when the results are displayed on the screen.

The display consists of each FRU name with each test module name listed under it. If all of the test modules in a FRU passed, the FRU name is displayed in green color as are all of the associated test module names. If any test module associated with a FRU failed, the FRU name is displayed in red, as is the failed test module name. The passing test module names are displayed in green. This allows the BYO to know which sub-unit of the FRU failed.

Sample screen display:

```

CPU MODULE FRU          PASSED
MATH_COPROCESSOR       PASSED
CPU                    PASSED
SMP_PROCESSOR_0        PASSED
MEMORY FRU             PASSED
MEMORY                 PASSED
STRESS                 PASSED
HARD DISK FRU          PASSED
Hard Disk 0            PASSED
Hard Disk 1            PASSED
    
```

Figure 6 - 4. DiagWiz FRU Status Display

6. Server Test Package

This section describes the diagnostics for server product. The diagnostics uses the MTA 'T' diagnostic controller to execute tests. The test package consists of:

- Quick Test package
- Comprehensive Test package
- Comprehensive Test with Continuous Looping package

The Diagnostic Wizard utilities are included to display configuration information and test results. The runttest utility prompts the user to select the test to be run. Once a test package is selected, the diagnostics self-sense operation executes to determine the hardware configuration. Self-sensing enables or disables tests according to the hardware found.

6.1 Test Packages

Runttest.exe is invoked by entering TESTMENU at the DOS prompt after the diskette is booted. The user is then prompted to select a test package from the following choices:

- Quick Test
- Comprehensive Tests
- Comprehensive Tests with Continuous Looping

After the selection is made, the self-sensing operation is executed, which invokes dwizcfg.exe to display the hardware configuration found. The user is prompted to press ENTER if the configuration is correct or to press CTRL/BREAK if the configuration is incorrect.

If CTRL/BREAK is selected, the tests are aborted and a screen is displayed instructing the user to check the hardware and cable connections. Control is returned to the test selection menu. If ENTER was pressed, indicating that the configuration is correct, the test is started. Upon completion of testing, dwizstat.exe is executed to display the test results indicating pass or fail status of each FRU and it's associated test modules.

6.1.1 Quick Test

The Quick Test package performs only minimal tests. They include:

- Power On Self tests
- CPU test
- Cache test
- Memory tests
- Hard Disk tests

The floppy drive and video monitor are tested by accessing the devices.

6.1.2 Comprehensive Tests

The Comprehensive Tests include all tests listed in the test list. Tests are performed to check the entire system. These tests take approximately 15 to 20 minutes, depending upon the hardware configuration.

6.1.3 Comprehensive Tests with Continuous Looping

The Comprehensive Tests with continuous looping include all the tests listed in the test list. The tests run continuously, until they are stopped by the user pressing the CTRL/BREAK keys. Dwizstat is then executed to display the test results after CTRL/BREAK is pressed.

7. Test List

A typical test package may include the following tests. This list is subject to future adjustments to address coverage enhancements and other requirements:

Table 6 - 10: Diagnostics Test List

CPU Support	Test Module	System Test
Primary Slot 1	cpu.exe: Tests for processor type, floating point unit, clock speed, checks processor information and MMX instructions. cache.exe: Tests cache read/writes dualpent.exe: Tests communication between multiple processors	cpu.exe: Tests for processor type, floating point unit, clock speed, checks processor information and MMX instructions. cache.exe: Tests cache read/writes dualpent.exe: Tests communication between multiple processors
Secondary Slot 1	Same as Primary Slot 1 tests	Same as Primary Slot 1 tests
Chipset	Test Module	System Test
82440BX	82440.exe: Verifies the type of 82450 system controller on the UUT, whether the DIMMs plugged into the UUT are the expected size, type, and in the expected position.	82440.exe: Verifies the type of 82450 system controller on the UUT, whether the DIMMs plugged into the UUT are the expected size, type, and in the expected position.
PIIX4	piix4.exe: Tests all the registers and timers on the device.	piix4.exe: Tests all the registers and timers on the device.
Video	Test Module	System Test
CL-GD5480 Graphics Controller	vid_cl.exe: Tests Cirrus specific registers and functions vid_vga.exe: Tests standard VGA functions of video vid_vmu.exe: Non-interactive testing of video modes	vid_cl.exe: Tests Cirrus specific registers and functions vid_vga.exe: Tests standard VGA functions of video vid_vmu.exe: Non-interactive testing of video modes
SGRAM	Same as GD5480 tests	Same as GD5480 tests
SM Video Blanking	Not tested	Not tested
Hardware Management	Test Module	System Test
5-V Standby	Power on of system	Power on of system
Server Management Controller (BMC)	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
Server Management Memory	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
Temperature Sensors	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
Conn/Jumpers	Test Module	System Test
ATX PWR	Not tested	Not tested
PWR Conn	Power on	Power on
Aux Power	Power on	Power on

CPU Support	Test Module	System Test
BB Fan 0	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
BB Fan 1	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
CPU Fan 2	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
CPU Fan 3	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller	bmc.exe: Checks the command interface protocol for the Baseboard Management Controller
DIMM 1	msdram.exe: Verify the functionality of the DRAM and cache memory stress.exe: Stress memory by performing random operations with random data to simulate system OS operation post.exe: Report any errors that occurred during Power on Self Test	msdram.exe: Verify the functionality of the DRAM and cache memory stress.exe: Stress memory by performing random operations with random data to simulate system OS operation post.exe: Report any errors that occurred during Power on Self Test
DIMM 2	msdram.exe: Verify the functionality of the DRAM and cache memory stress.exe: Stress memory by performing random operations with random data to simulate system OS operation post.exe: Report any errors that occurred during Power on Self Test	Not tested
DIMM 3	msdram.exe: Verify the functionality of the DRAM and cache memory stress.exe: Stress memory by performing random operations with random data to simulate system OS operation post.exe: Report any errors that occurred during Power on Self Test	Not tested
DIMM 4	msdram.exe: Verify the functionality of the DRAM and cache memory stress.exe: Stress memory by performing random operations with random data to simulate system OS operation post.exe: Report any errors that occurred during Power on Self Test	Not tested
USB	usb.exe: Tests functionality of USB feature on board by verifying presence and resources for USB. A stress test is performed to verify the connections in and out of the board. Note: Connect the baseboard to USB test cards via USB cables	TBD
PCI Slot #1	pro100b.exe: Tests functions of the Intel® EtherExpress™ Pro100B hardware or PCI slot	pro100b.exe: tests functions of Pro100B hardware or PCI slot
PCI Slot #2	pro100b.exe: Tests functions of Pro100B hardware or PCI slot	Not tested

CPU Support	Test Module	System Test
PCI Slot #3	pro100b.exe: Tests functions of Pro100B hardware or PCI slot	Not tested
Conn/Jumpers	Test Module	System Test
PCI Slot #4	pro100b.exe: Tests functions of Pro100B hardware or PCI slot	Not tested
ISA Slot #1	smmtest.exe: Uses Server Monitor Module to test SMM Feature connector	smmtest.exe: Uses Server Monitor Module to test SMM Feature connector
ISA Slot #2	Testhook card	Not tested
IDE Primary	hdbios.exe: Tests hard disks at the BIOS level of compatibly	Not tested
IDE Secondary	hdbios.exe: Tests hard disks at the BIOS level of compatibly	Not tested
Floppy	floppy.exe: Tests read/write capability of floppy	floppy.exe: Tests read/write capability of floppy
Keyboard	kb.exe: Tests keyboard controller and mouse port	kb.exe: Tests keyboard controller and mouse port
Mouse	mouse.exe: Tests mouse interface	mouse.exe: Tests mouse interface
Serial Com 1	serio.exe: Tests functionality of serial ports	serio.exe: Tests functionality of serial ports
Serial Com 2	serio.exe: Tests functionality of serial ports	serio.exe: Tests functionality of serial ports
Parallel Port	pario.exe: Test functionality of parallel port	pario.exe: Test functionality of parallel port
VGA	<p>vid_cl.exe: Tests the functionality of the SVGA Cirrus Logic GD542X/GD543X/GD544X video controllers</p> <p>vid_vga.exe: Tests the functionality's of the VGA-compatible video controller, the video RAM(256K), video DAC</p> <p>vid_vmu.exe: Test video modes non-interactively using the Visual Memory Unit (VMU)</p>	<p>vid_cl.exe: Tests the functionality's of the SVGA Cirrus Logic GD542X/GD543X/GD544X video controllers</p> <p>vid_vga.exe: Tests the functionality's of the VGA-compatible video controller, the video RAM(256K), video DAC</p>
NIC Connector	pro100b.exe: Tests functions of Pro100B hardware or PCI slot	pro100b.exe: Tests functions of Pro100B hardware or PCI slot
SCSI UW 68-pin	hdbios.exe: Tests hard disks at the BIOS level of compatibly	hdbios.exe: Tests hard disks at the BIOS level of compatibly
SCSI Narrow 50-pin	hdbios.exe: Tests hard disks at the BIOS level of compatibly	hdbios.exe: Tests hard disks at the BIOS level of compatibly
ITP Connector	Not tested	Not tested
SMM Feature Connector	smmtest.exe: Uses Server Monitor Module to test SMM Feature connector	smmtest.exe: Uses Server Monitor Module to test SMM Feature connector
Front Panel Connector	Not tested	led.exe: Tests functionality of LED
Override Jumper	Not tested	Not tested
Front-Side Bus (FSB) Speed Jumper	cpu.exe: Tests that FSB is operating at the correct frequency but does not test the alternate speed.	cpu.exe: Tests that FSB is operating at the correct frequency but does not test the alternate speed.
Wake-on-LAN Jumper	Not tested	Not tested
Boot Blk Write Enable (WE) Jumper	Not tested	Not tested

CPU Support	Test Module	System Test
Ext Intelligent Management Bus (IMB) Jumper	Not tested	Not tested
Ext Wake-On-LAN (WOL) Jumper	Not tested	Not tested
CMOS Jumper Block	If jumper is in wrong position, the system will not boot correctly.	If jumper is in wrong position, the system will not boot correctly.
FRB, Intrusion, BMC Update jumper block	If FRB jumper is in the wrong position, the system will not boot correctly. Intrusion/BMC not tested.	If FRB jumper is in the wrong position, the system will not boot correctly. Intrusion/BMC not tested.
Speaker	pit.exe: Tests functionality of speaker through the PIT	pit.exe: Tests functionality of speaker through the PIT
LED jumper Block	Not tested	Not tested
Clocks	Functional test	System Test
Clock Gen/drvr	Not directly tested	Not directly tested
Crystal 14.318-MHz	Not directly tested	Not directly tested
SM Cryst. 22.11-MHz	Not directly tested	Not directly tested
Miscellaneous	Functional test	System Test
PC87309 SIO	sio308.exe: Test the functionality of the PC87308 (SIO308) and PC87307 Super I/Os	sio308.exe: Test the functionality of the PC87308 (SIO308) and PC87307 Super I/Os
Pro100 (IN82558)	pro100b.exe: Tests functions of Pro100B hardware	pro100b.exe: Tests functions of Pro100B hardware
8-MB Flash	Not directly tested. Features of the BIOS are tested which are contained in the flash. If the UUT has an old version of BIOS, it will be flashed with the new version. Some DMI information is written into the flash.	Not directly tested. Features of the BIOS are tested which are contained in the flash. If the UUT has an old version of BIOS, it will be flashed with the new version. Some DMI information is written into the flash.
I/O APIC	Dualpent.exe: Tests symmetrical multiprocessing capabilities of multiprocessor boards	Dualpent.exe: Tests symmetrical multiprocessing capabilities of multiprocessor boards
Basic Util Router (Altera)	New test	New test
Primary Voltage Regulating Modules (VRMs)	Tested by powering on the system and recognizing both processors.	Tested by powering on the system and recognizing both processors.
Secondary VRM	Tested by powering on the system and recognizing both processors.	Tested by powering on the system and recognizing both processors.
Primary VRM Voltage ID (VID) Compare Logic	If VID is incorrect, the voltages supplied to the processor will be incorrect causing the processor to fail	If VID is incorrect, the voltages supplied to the processor will be incorrect causing the processor to fail
Secondary VRM VID Compare Logic	If VID is incorrect, the voltages supplied to the processor will be incorrect causing the processor to fail	If VID is incorrect, the voltages supplied to the processor will be incorrect causing the processor to fail
SCSI Sym53C876	symc8xx.exe: Verify the functionality of the SYMBIOS 53C8XX SCSI Controllers hdbios.exe: Tests hard disks at the BIOS level of compatibly	symc8xx.exe: Verify the functionality of the SYMBIOS 53C8XX SCSI Controllers hdbios.exe: Tests hard disks at the BIOS level of compatibly
SCSI Terminators	Not directly tested	Not directly tested

Intel® Server Control, Version 3.x TPS

Section 7: Client System Setup Utility (CSSU) Application

Table of Contents

1. Introduction to the Client System Setup Utility (CSSU) Application.....	1
2. Client Application Framework	3
2.1 Command Line Options.....	3
2.2 Initialization Files	3
3. CSSU Graphical User Interface.....	4
3.1 Main Menu Options	5
3.1.1 File Menu	5
3.1.2 Edit Menu	5
3.1.3 View Menu	5
3.1.4 Server Menu.....	6
3.1.5 Services Menu.....	6
3.1.6 Window Menu	7
3.1.7 Help Menu.....	7
3.1.8 Tool Bar	8
3.1.9 Status Bar	8
3.2 Phonebook Dialog Options.....	9
3.2.1 Add Phonebook Entry and Modify Phonebook Entry Dialogs	10
3.3 Connection Dialog Options.....	11
4. Console Redirection Feature	12
4.1 The SSU Console Redirection Window	12
5. Add-in Components.....	14
5.1 Resource Configuration Manager (RCM) Add-in	14
5.1.1 Device Window	15
5.1.2 System Resource Usage Window	16
5.2 Multiboot Manager (MBM) Add-in.....	18
5.2.1 User Interface / Operation	18
5.3 Password Manager (PWM) Add-in	19
5.3.1 Initialization Files	19
5.3.2 User Interface / Operation	19
5.4 System Event Log Add-In.....	22
5.4.1 Initialization Files	22

5.4.2	Internationalization	22
5.4.3	User Interface / Operation	22
5.5	Sensor Data Record Manager Add-In	22
5.5.1	Initialization and Customization Files.....	22
5.5.2	User Interface / Operation	22
5.6	Field Replaceable Unit Manager Add-In	22
5.6.1	Initialization Customization Files.....	22
5.6.2	User Interface / Operation	23
5.7	System Update Manager Add-in.....	23
5.8	Platform Event Manager Add-in	23
5.9	Configuration Save / Restore Manager Add-in	23
6.	System Update Manager Add-in Component.....	24
6.1	Initialization Files	24
6.2	Internationalization	24
6.3	User Interface / Operation	24
6.3.1	Confirmation Dialog.....	26
6.4	Recovery Agent.....	26
6.4.1	General Update Process	27
7.	Platform Event Manager Add-in Component	30
7.1	Initialization Files	30
7.2	Internationalization	30
7.3	User Interface / Operation	30
7.3.1	Platform Event Manager Window	30
7.3.2	Platform Event Paging Dialog.....	31
7.3.3	BMC LAN-Alert Dialog.....	32
7.3.4	Platform Event Action Dialogs	34
7.3.5	Emergency Management Port Dialog.....	35
8.	Configuration Save/Restore Manager Add-in Component.....	36
8.1	Initialization Files	36
8.2	Internationalization	36
8.3	User Interface / Operation	36
8.3.1	CSR Main Window	36
8.3.2	Configuration Data	37

List of Figures

Figure 7 - 1. System Setup Utility Framework	2
Figure 7 - 2. Client Main Window	4
Figure 7 - 3. Phonebook Dialog.....	9
Figure 7 - 4. Add Phonebook Entry Dialog	10
Figure 7 - 5. Connect Dialog	11
Figure 7 - 6. Console Redirection Window during Server Reboot.....	12
Figure 7 - 7. Console Redirection Window - MDI Child Window.....	13
Figure 7 - 8. Resource Configuration Main Window	14
Figure 7 - 9. Device Window	15
Figure 7 - 10. System Resource Usage Window.....	17
Figure 7 - 11. Multiboot Manager Main Window	18
Figure 7 - 12. Password Manager Main Window	20
Figure 7 - 13. System Update Manager Main Window	25
Figure 7 - 14. SUM Verify Operation Confirmation Dialog	26
Figure 7 - 15. Platform Event Manager Main Window	30
Figure 7 - 16. Platform Event Paging Dialog	31
Figure 7 - 17. BMC LAN-Alerting Dialog.....	32
Figure 7 - 18. Platform Event Action Dialogs.....	34
Figure 7 - 19. Emergency Management Port Dialog.....	35
Figure 7 - 20. CSR Manager Main Window	36

List of Tables

Table 7 - 1: Command Line Options.....	3
Table 7 - 2: CSSU Tool Bar Options	8
Table 7 - 3: Phonebook Dialog Options.....	9
Table 7 - 4: Add Phonebook Entry Dialog Options	10
Table 7 - 5: Connect Dialog Options	11
Table 7 - 6: Resource Configuration Manager Options	15
Table 7 - 7: Device Window Options	16
Table 7 - 8: System Resource Usage Window Options.....	17
Table 7 - 9: Multiboot Manager Main Window Options	19
Table 7 - 10: Password Manager Main Window Options	20
Table 7 - 11: System Update Manager Main Window Options	25
Table 7 - 12: Checkpoint File Format	29
Table 7 - 13: Platform Even Manager Main Window Options	31
Table 7 - 14: Platform Event Paging Options	32
Table 7 - 15: BMC LAN-Alert Dialog Options.....	33
Table 7 - 16: Platform Event Action Dialog Options.....	34
Table 7 - 17: Emergency Management Port Dialog Options.....	35
Table 7 - 18: CSR Manager Main Window Options	37

< This page intentionally left blank. >

1. Introduction to the Client System Setup Utility (CSSU) Application

This section describes the installation environment for ISC in those instances where Intel® Server Control (ISC), Desktop Management Interface (DMI) 2.0 SP, Explorer browser, and the Managed Object Toolkit (MOT) are installed.

The Client System Setup Utility (CSSU) provides a system-level view of the local server platform from a remote client workstation. The CSSU interface consists of a Win32* graphical user interface (GUI) resident on a console workstation. This communicates with the System Setup Utility (SSU) agents and framework resident on the Service Partition at the server. The GUI employs the common look-and-feel of Intel® Server Control (ISC) components and integrates into the ISC stand-alone console as well as into Enterprise System Management Consoles (ESMC) from Hewlett-Packard and Computer Associates.

To initiate a CSSU session, the client requests a service boot through the Emergency Management Port (EMP). As the service environment boots, a network stack and agent are started and communication between the server and client switches to a packet-based protocol. Using the new protocol, the client launches the SSU and begins communicating with the SSU through a socket interface. The application then allows the user to perform a variety of configuration tasks and setup tasks that normally would only be available at the local server platform.

Note: The SSU software can also be executed locally at the server by booting it from a floppy disk, CD-ROM, or the Service Partition and using the local monitor and keyboard. This is known as the Server SSU. It is not discussed in detail in this document.

The following figure illustrates the architecture of the server-resident portions of the SSU component of the ISC product. This architecture consists of an SSU framework and a collection of add-in modules that use the framework to access and control the server and to communicate to both local and remote user interfaces.

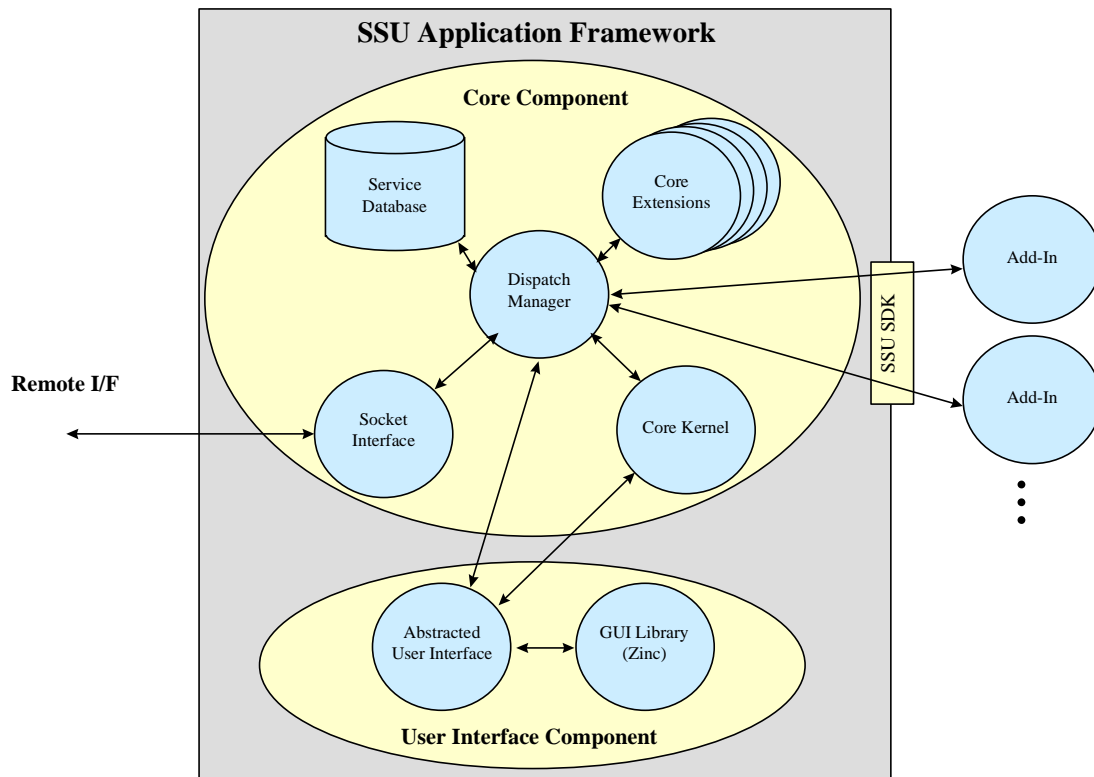


Figure 7 - 1. System Setup Utility Framework

The add-in modules to the right of the figure correspond to functions available through the SSU. Add-ins support management of:

- Field Replaceable Unit (FRU) information
- Sensor Data Records (SDR) information
- System Event Log (SEL) information
- System Update Manager (SUM)
- Platform Event Manager (PEM)
- Configuration Save/Restore (CSR)
- System boot order settings
- Security options
- Industry Standard Architecture (ISA) resource configurations

In addition, an add-in System Design Kit (SDK) is available to Original Equipment Manufacturers (OEMs) who want to supply their own add-in features.

2. Client Application Framework

The environment for remote (client) SSU operation is provided by the Client Application Framework (CAF). The CAF integrates SSU-based features through a set of management plug-ins called add-ins. The add-ins allow the user to perform remote system management tasks from the client workstation. Functionality provided by the add-in may vary by server platform.

The add-in modules may include support for configuring system resources, selecting boot options, specifying the password, and viewing system information (such as the system event log, the sensor data records, and the field replaceable unit information). Within this architecture, the CAF is implemented as a Multiple Document Interface (MDI) container application and each add-in component is implemented as an ActiveX* control.

2.1 Command Line Options

The CAF supports the following command-line options:

Table 7 - 1: Command Line Options

Option	Meaning
/I IP Address	Specifies the Internet Protocol (IP) address to be used to establish a connection with the SSU server.
/D DNS name	Specifies the Domain Name System (DNS) name to be used to establish a connection with the SSU server.
/P phone number	Specifies phone number to be used to establish a connection with the SSU server.

2.2 Initialization Files

The CAF does not include support for initialization files. Instead, all parameters required to configure the operation of the CAF are stored in the Windows* registry.

3. CSSU Graphical User Interface

Only a single instance of the CAF can be launched on the client platform. Launching multiple copies of the CAF to connect to multiple SSU Servers is not supported.

If the Client SSU is launched with a telephone number, IP address, or DNS name specified on the command line, it will attempt to establish a connection with the SSU Server at the given telephone number, address, or DNS name. If the Client SSU is launched without a any of this information specified on the command line, the Client SSU will display the main window and wait for user input.

While the connection is being established, the Client SSU will display connection information on the status bar of the main window. If a connection cannot be established with the remote server, the Client SSU will display an error message and return to the main window to wait for user input. Once a connection is initiated, the user will be prompted for an EMP password if a password has been configured in the server system BIOS.

If a single password is configured in the BIOS, all options within the Client SSU add-in modules will be available upon successful password entry. If both a system BIOS admin password and a user password have been set and the user provides only the user password, the functionality that is provided in the password add-in module is limited to the ability to change the user password. The password prompt cannot be selectively enabled or disabled within the CAF.

After the password has successfully been entered, the CAF will return to the main window to wait for user input. The main window consists of a Main Menu, Tool Bar, and Status Bar, as displayed in the following diagram.

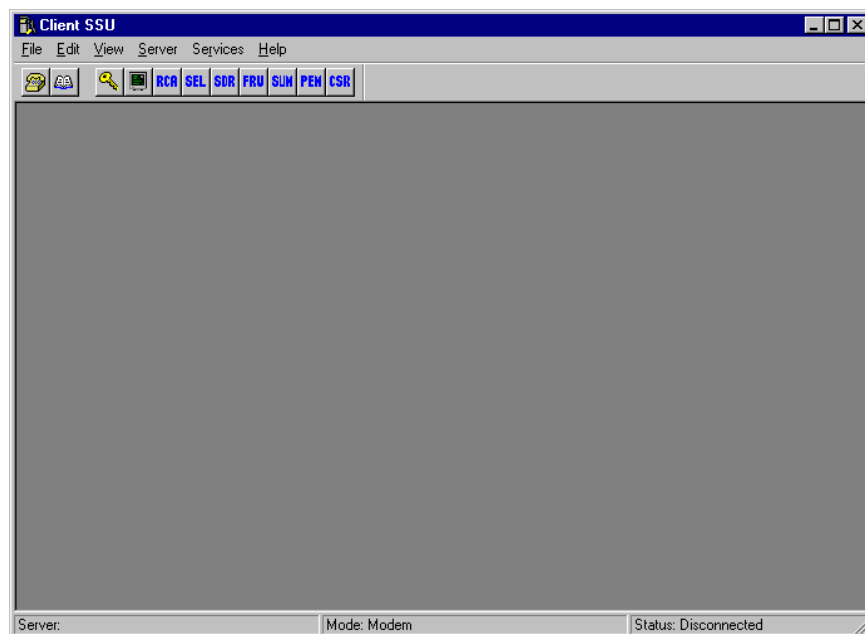


Figure 7 - 2. Client Main Window

3.1 Main Menu Options

The options in the following sections are available or viewable from the Main Menu.

3.1.1 File Menu

The 'File' menu provides the options:

- 'New'
- 'Open'
- 'Save'
- 'Save As'
- 'Close'
- 'Print'
- 'Print Preview'
- 'Recent File'
- 'Exit'

The availability of many of these options depends upon a manager being active and the level of support for the options within the active manager.

The 'Exit' option is always available and will terminate the SSU CAF and all manager components. If a connection with an SSU Server has previously been established, the 'Exit' selection will:

1. Confirm the exit action with the user.
2. Terminate the SSU Server application.
3. Terminate the connection between the Client SSU and SSU Server.
4. Reboot the server to its primary operating system.

The 'File' menu is not a dynamic menu and it may not include other options. The menu is always available, even if a manager is not currently active.

3.1.2 Edit Menu

The 'Edit' menu includes options to 'Undo', 'Cut', 'Copy', and 'Paste'. These options provide the standard functionality associated with a Windows application. The menu is always available, even if a manager is not currently active.

3.1.3 View Menu

The 'View' menu includes the 'Tool Bar' and 'Status Bar' options. These options provide the ability to selectively hide or show the toolbar and the status bar. This is not a dynamic menu and may not include other options. The menu is always available, even if manager is not currently active.

3.1.4 Server Menu

The 'Server' menu supports the options '(Re)Connect' or 'Disconnect', 'Phonebook', and a list of the five most recent connections. These options are used to manage the connection between the Client SSU and the SSU Server. The 'Phonebook' option is always available. It is used to manage the list of server connections and connection methods.

The availability of the other options depends on whether a connection has already been established. If a connection is established, the 'Disconnect' option is available, but the '(Re)Connect' option and the list of the five most recent connections are not available. If no connection is established, the '(Re)Connect' option can be selected, or a connection choice can be made from the list of the five most recent connections to re-establish that connection, but the 'Disconnect' option is not available.

The 'Disconnect' option confirms the user's intentions and then terminates the SSU Server application, closes the connection between the Client SSU and SSU Server, and reboots the server to its primary operating system. The 'Disconnect' option does not terminate the Client SSU application.

The '(Re)Connect' option displays a dialog box that allows the user to establish a connection with the SSU Server.

The 'Server' menu is not a dynamic menu and may not include other options. The menu is always available, even if a manager is not currently active.

3.1.5 Services Menu

The 'Services' menu is populated with manager options that can be accessed remotely by the Client SSU, including:

- 'Password Manager'
- 'Multiboot Manager'
- 'Resource Configuration Manager'
- 'SEL Manager'
- 'SDR Manager'
- 'FRU Manager'
- 'System Update Manager'
- 'Platform Event Manager'
- 'CSR Manager'

Additional managers may be integrated into the Client SSU and will appear as menu options in the 'Services' menu.

All manager options are displayed, regardless of whether the Client SSU is currently connected to the SSU Server platform. If a connection is not established, a connection dialog will be presented to the user when an option is selected.

After establishing the connection, the manager service will be launched within the CAF container. If the SSU Server does not support the desired manager, an informational message will be displayed. However, the connection between the Client SSU and the SSU Server will be maintained. The Client SSU cannot identify the services supported by the SSU Server until a connection is established.

All manager options are displayed if the Client SSU is currently connected to the SSU Server platform. However, some options may be “grayed-out” if the connected SSU Server does not support the manager feature.

The ‘Services’ menu is a dynamic menu and may include other options. The menu is always available, even if a manager is not currently active.

3.1.6 Window Menu

The Client SSU is a Multiple Document Interface (MDI) application, includes a ‘Window’ menu, which is available only when at least one manager component is instantiated in the CAF. The ‘Window’ menu includes options to ‘Cascade’ and ‘Arrange Icons’. Each of these options acts upon the manager module windows that can be invoked from the ‘Services’ menu. The options provide the standard functionality associated with a MDI application.

The ‘Window’ menu is not a dynamic menu and may not include other options. The menu is available only if a manager is currently active.

3.1.7 Help Menu

The ‘Help’ menu is always available in the CAF. This menu supports options for the CAF, including ‘Client SSU Help Topics’ and ‘About Client SSU’, when the CAF is the active window. If one of the managers is active, then the ‘Help’ menu displays help topics and “About” information for that active manager.













The ‘Help’ menu is a dynamic menu and may include other options when other managers are active.

3.1.8 Tool Bar

The CAF main window includes a ‘Tool Bar’ that has buttons to support frequent operations. Each button on the tool bar supports tool-tip help. Although additional managers may be integrated into the Client SSU and appear as menu options in the ‘Services’ menu, additional buttons on the ‘Tool Bar’ are not supported.

Options included on the ‘Tool Bar’ include those in the table below:

Table 7 - 2: CSSU Tool Bar Options

Bitmap	Description
	(Re)Connect – Launches the ‘Connection’ dialog
	Disconnect – Disconnects from the connected server with confirmation
	Phonebook - Launches the ‘Phonebook’ dialog. The phonebook allow the user to associate telephone (modem) numbers, IP addresses, or DNS names with a server to facilitate connections.
	RCM – Launches the Resource Configuration Manager module
	MBM – Launches the Multiboot Manager module
	PWM – Launches the Password Manager module
	SEL – Launches the SEL Manager module
	SDR – Launches the SDR Manager module
	FRU – Launches the FRU Manager module
	SUM – Launches the System Update Manager module
	PEM – Launches the Platform Event Manager module
	CSR – Launches the Configuration Save/Restore Manager module

3.1.9 Status Bar

The Status Bar displays information about the current connection. For modem-based connections, the ‘Status Bar’ includes the server name (if the connection was launched from the Client SSU), telephone number, the connection mode, and the connection status. These areas of the Status Bar include information only if an active connection exists.

3.2 Phonebook Dialog Options

The Client SSU includes support for a phonebook that organizes information needed to establish connections with SSU Server platforms. The phonebook is shared with other ISC components. The dialog box used to maintain existing or edit new phonebook entries is shown below.

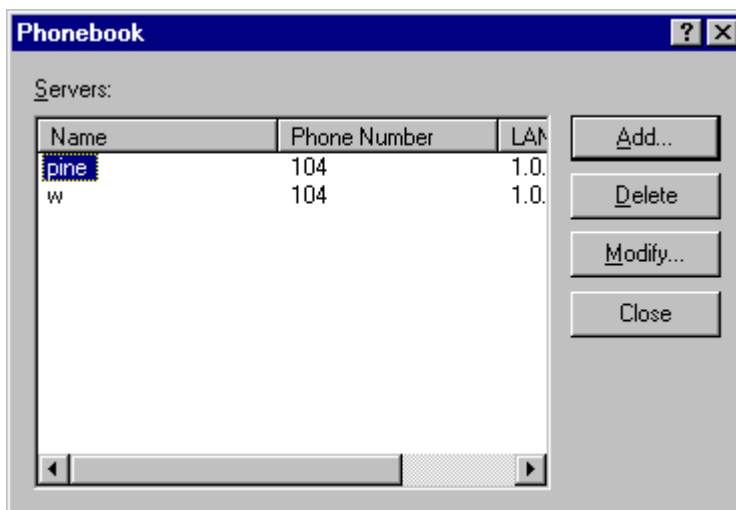


Figure 7 - 3. Phonebook Dialog

Table 7 - 3: Phonebook Dialog Options

Option	Function
Servers	The 'Servers' list box encompasses the majority of the screen. This provides a list of server platform names maintained in the phonebook. In addition to each server name, the list box also displays the telephone number and IP address or DNS name associated with the server. The list does not include any server information provided on the command line, which must be manually added to the phonebook.
Add	The 'Add' button is used to add an entry to the phonebook. Selection of this option opens an empty 'Add Phonebook Entry' dialog.
Delete	The 'Delete' button allows users to select an entry from the phonebook for deletion. Prior to selecting this option, the user must choose the desired entry to be deleted by selecting the server name from the 'Servers' list box.
Modify	The 'Modify' button allows users to select an entry from the phonebook for modification with the 'Modify Phonebook Entry' dialog box. Prior to selecting this option, the user must choose the desired entry to be modified by selecting the server name from the 'Servers' list box.
Close	The 'Close' button saves any changes and returns the user to the main window.

3.2.1 Add Phonebook Entry and Modify Phonebook Entry Dialogs

This dialog is shown when the user pushes the Add button in the Phonebook dialog. All entries are defaulted to blank. The server name and, either a phone number or the IP address / DNS name needs to be provided for the entry to be valid. If the user so desires, both a telephone number and IP address / DNS name can be entered. The Modify Phonebook Entry dialog has the same format as the Add Phonebook Entry dialog, so is not described separately in this document.

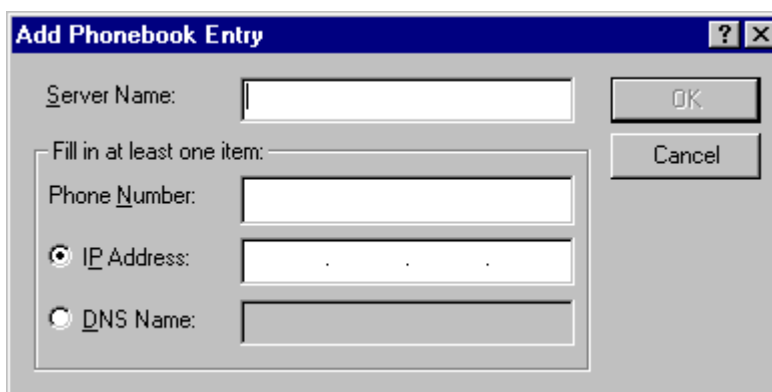


Figure 7 - 4. Add Phonebook Entry Dialog

Table 7 - 4: Add Phonebook Entry Dialog Options

Option	Function
Server Name	The name of the server to be managed is entered in this field. The server name must be filled in and must be unique.
Phone Number	If the server can be connected to by a modem, enter the telephone number for the server here.
IP Address	Select this radio button if the server has an IP Address. Enter the IP Address of the server in the edit control. Only one item (IP Address or DNS Name) will be saved in the phonebook.
DNS Name	Select this radio button if the server you are connecting to have a DNS Name. Enter the DNS Name of the server in the edit control. Only one item (IP Address or DNS Name) will be saved in the phonebook.
OK	Press this button to indicate all the information is correctly filled in. This closes the dialog, adds the entry to the phonebook, and returns the user to the 'Phonebook' dialog.
Cancel	Press this button to close the dialog without saving any of the information. The user is returned to the 'Phonebook' dialog.

3.3 Connection Dialog Options

The Client SSU contains support for a 'Connection' dialog. The 'Connection' dialog is used to establish a connection between the Client SSU and the SSU Server.

The dialog is shown below, and the various controls in the dialog are described in the following sections.

Note: An alternative connection method is to pass the server phone number, IP address, or DNS name to the Client SSU on the command line.

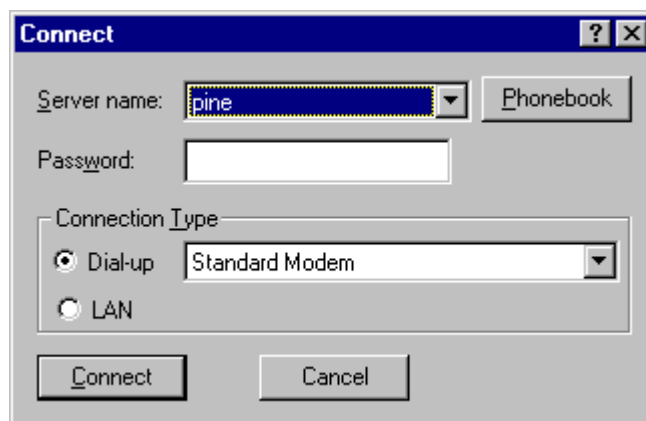


Figure 7 - 5. Connect Dialog

Table 7 - 5: Connect Dialog Options

Option	Function
Server Name	This pull-down option contains a list of servers that have been previously entered into the phonebook.
Phonebook	Pressing this button displays the Phonebook dialog to allow the user to view the phonebook. The user can then edit phonebook entries. When the user presses the Close button in the Phonebook dialog, control returns to the Connection dialog, and any changes made to the phonebook are reflected in the Server name combo-box.
Password	The Password edit box is used to enter the EMP password, if one exists. If one does not exist, this box can be left blank.
Connection Type	The radio buttons shown in Connection Type grouping allow the user to select the type of medium to use to connect to a server: Dial-up Connection: If the Dial-up radio button is selected, the user can choose a RAS device, such as a modem, to connect to the server. Local Area Network (LAN) Connection: If the LAN radio button is selected, the connection to the server will be done via LAN, using the IP address or DNS name associated with the selected server.
Connect	Press this button to initiate the chosen connection.

4. Console Redirection Feature

When the Client SSU attempts to establish a connection with a server, the socket connection to the server cannot be established until the server has rebooted to the service partition. During the reboot operation, the only information available to the user is the connection information on the status bar of the CAF main window. If a connection cannot be successfully established with the remote server, the Client SSU will display an error message and return to the main window to allow the user to select an operation.

In some cases, the error message displayed may not be sufficient for the user to identify the cause of the connection failure. To provide users with additional information during the server reboot, a Console Redirection window will appear within the CAF main window. This window shows the boot process on the server.

The Console Redirection window is implemented as a dialog window with an embedded ActiveX control. The Console Redirection Control is shared by the SSU and DPC. The window accepts user keyboard input, such as pressing the F2 key to access the server BIOS setup screens.

4.1 The SSU Console Redirection Window

When the Client SSU attempts to establish a connection, it sends an EMP command to the server. This command causes the server to reboot to the service partition. During the reboot, the server is switched to console redirection mode and a message to this effect is sent to the Client SSU. After this, the text output to the server's screen can be displayed in the Client SSU main window.

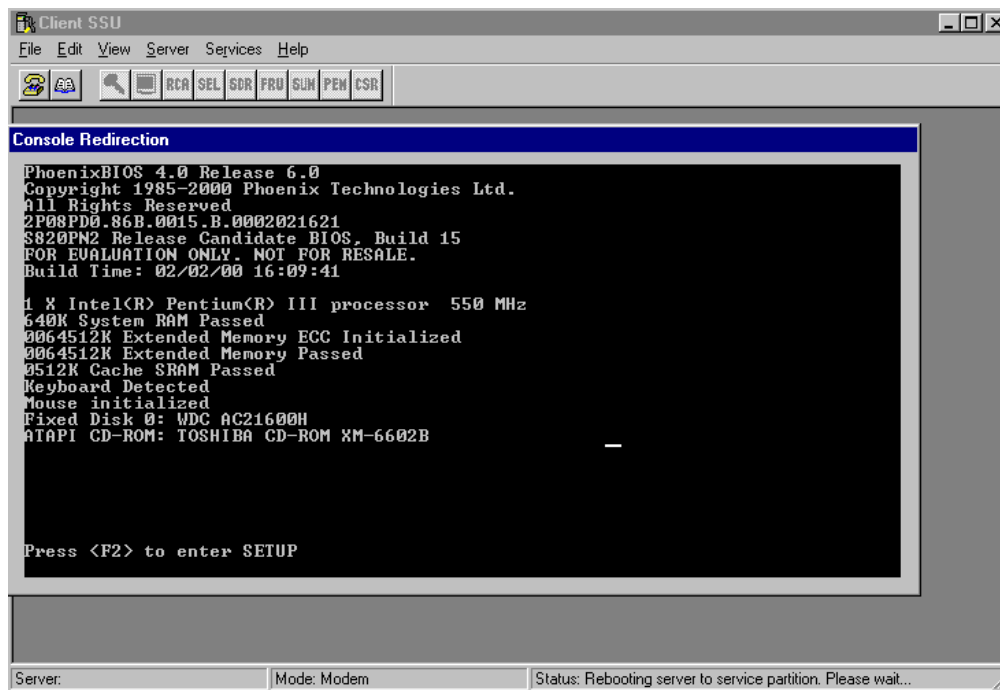


Figure 7 - 6. Console Redirection Window during Server Reboot

The SSU Console Redirection window is invoked whenever a connection is established. After a server reboot message is received, the MDI child window appears.

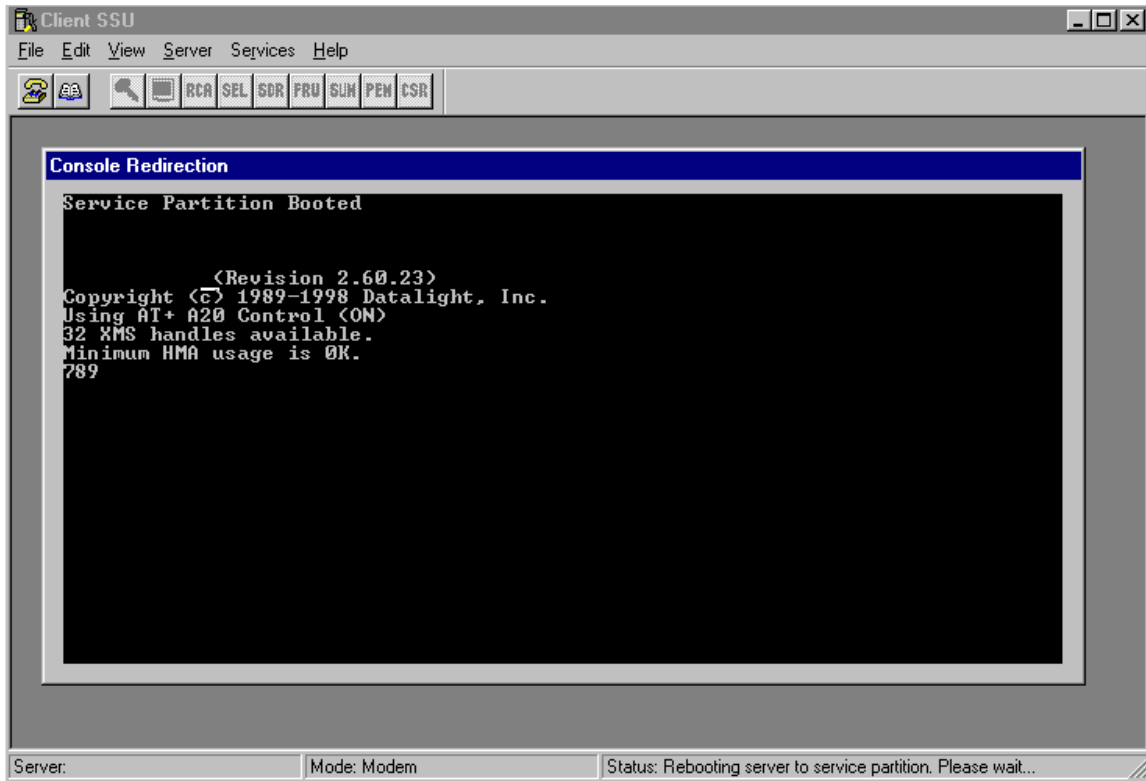


Figure 7 - 7. Console Redirection Window - MDI Child Window

After the server is booted to the service partition and the Remote Sensor Access (RSA) is started, another message is sent by the server indicating that it has switched to EMP mode. At this point, the Console Redirection window is closed.

5. Add-in Components

The add-in components described here do not include support for initialization files. Instead, all parameters required to configure the component are stored in the Windows registry. The add-in components are implemented as ActiveX controls within the MDI CAF application.

The following add-in components are discussed below:

- Resource Configuration Manager
- Multi-boot Manager
- Password Manager
- System Event Log
- Sensor Data Record
- Field Replaceable Unit
- System Update Manager
- Platform Event Manager
- Configuration Save/Restore Manager

5.1 Resource Configuration Manager (RCM) Add-in

The Resource Configuration Manager (RCM) provides resource conflict detection and resolution services. Its purpose is to facilitate the creation of a working configuration after the addition or removal of hardware from the system. The main window for this add-in is displayed in following figure.

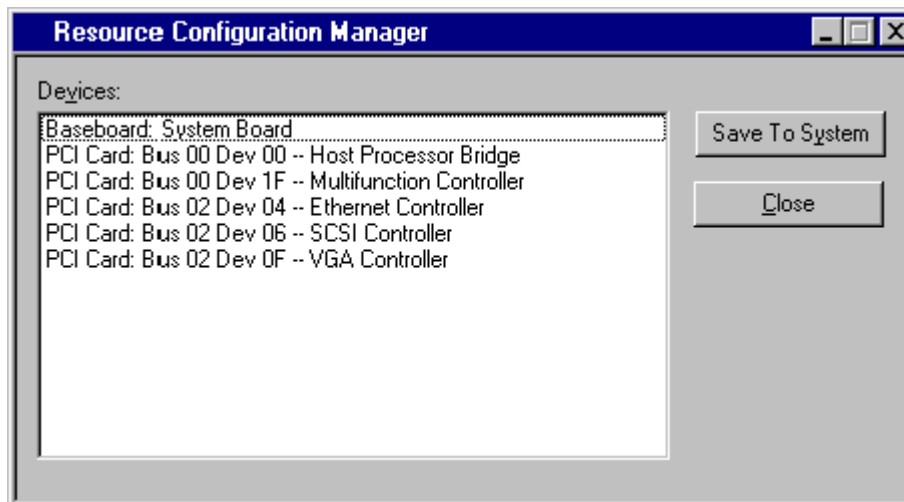


Figure 7 - 8. Resource Configuration Main Window

Table 7 - 6: Resource Configuration Manager Options

Option	Function
Devices List	Provides a list of specific items that can be accessed with a double-click and then modified in subsequent screens.
Save to System	Writes the current configuration to non-volatile storage on the server system. Once the configuration has been saved, the screen closes and may not be opened again for this server until the server system is rebooted. In addition to saving the configuration information to non-volatile storage, the user may choose to create a backup file containing all of the system configuration data that is included in the RCM. This binary file can be used to restore configuration information during a later SSU session and may be stored on either the client or server system. Restoration from a backup file is accomplished prior to complete initialization of the RCM. During the initialization of the RCM, the user will be prompted to restore from a backup file prior to loading the RCM. The file used for restoration may be stored on either the client or server system.
Close	Exits the RCM Add-in. If configuration changes have been made but not saved, the user is given the option of saving changes before exiting.

5.1.1 Device Window

It may be necessary to modify the resources of a device to accommodate certain operating systems, applications, and drivers. The 'Device Window' provides several features to aid in this process.

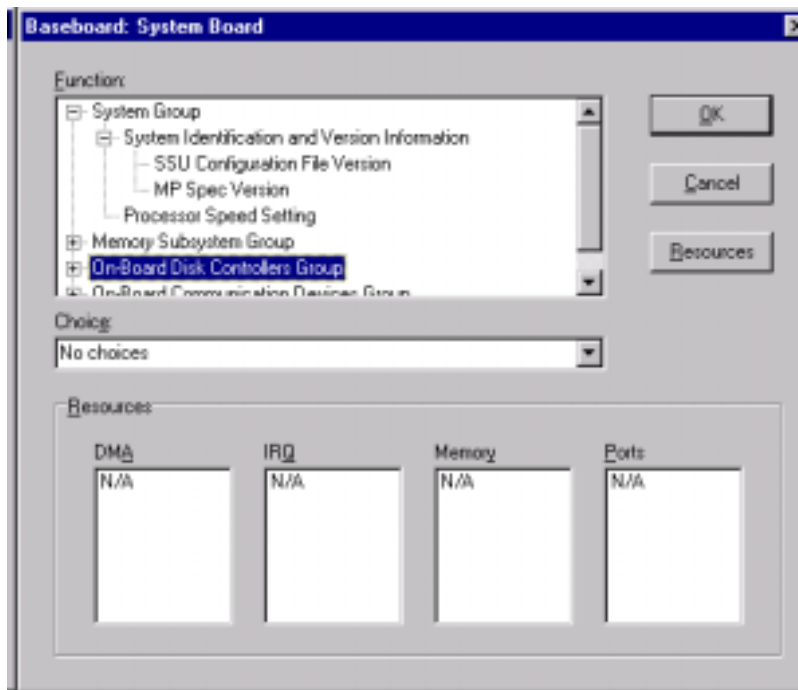


Figure 7 - 9. Device Window

Table 7 - 7: Device Window Options

Option	Function
Function List Box	The Function list box is used to select the device's function so that the configuration choices and resources associated with the function may be updated. Selection of a new function updates the Choice combo and the DMA, IRQ, Memory, and Ports list boxes as required. Some functions may not contain choices or resources but are instead used for grouping or organizational purposes.
Choice Combo Box	The Choice combo box is used to provide a list of configuration choices associated with the current function. Choices may be changed by selecting the desired choice from the combo box. Selection of a new choice updates the DMA, IRQ, Memory, and Ports list boxes.
DMA List Box	The DMA list box is used to change an existing setting of a DMA resource associated with the current function. DMA resources can be changed by double-clicking on the desired entry and updating the DMA entry in the Change DMA window. If a DMA resource is not required for the current choice, 'N/A' is displayed as the only item in the DMA list box.
IRQ List Box	The IRQ list box is used to change an existing setting of an IRQ resource associated with the current function. IRQ resources can be changed by double-clicking on the desired entry and updating the IRQ entry in the Change IRQ window. If an IRQ resource is not required for the current choice, 'N/A' is displayed as the only item in the IRQ list box.
Memory List Box	The Memory list box is used to change an existing setting of a memory resource associated with the current function. Memory resources can be changed by double clicking on the desired entry and updating the memory entry in the Change Memory window. If a memory resource is not required for the current choice, 'N/A' is displayed as the only item in the Memory list box.
Ports List Box	The Ports list box is used to change an existing setting of a ports resource associated with the current function. Port resources can be changed by double clicking on the desired entry and updating the port entry in the Change Port window. If a port resource is not required for the current choice, 'N/A' is displayed as the only item in the Ports list box.
OK Button	The OK button commits any resource changes made to the device to the internal resource database and returns the user to the RCM main window. Updated information is not stored in non-volatile storage until the Save button is selected on the RCM main window.
Cancel Button	The Cancel button discards any changes made to the device and returns the user to the RCM main window. After the RCM conflict detection and resolution algorithm is run, it is not possible to cancel changes to the selected device.
Resources Button	The Resources button invokes the Resource Usage window.

5.1.2 System Resource Usage Window

Viewing of system resources is useful to setup and debug system configurations. The System Resource window provides several sources to view this window.

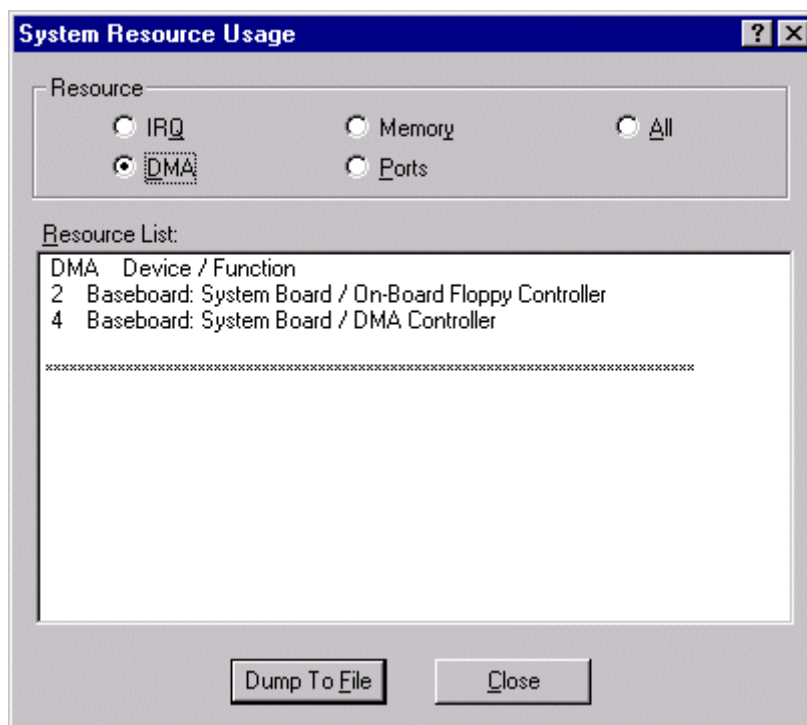


Figure 7 - 10. System Resource Usage Window

Table 7 - 8: System Resource Usage Window Options

Option	Function
Resource List Box	The 'Resource' list box provides a complete listing of the specified resources currently used in the system except for any re-locatable expansion ROM images. Re-locatable expansion ROM images are not included in the set of system resources because the address ranges occupied by these expansion ROM images should not be considered in the conflict detection and resolution algorithm provided in the RCM since they are fully re-locatable by the system BIOS.
IRQ Radio Button	The 'IRQ' radio button updates the 'Resource' list box to include only IRQ resources.
DMA Radio Button	The 'DMA' radio button updates the 'Resource' list box to include only DMA resources.
Ports Radio Button	The 'Ports' radio button updates the 'Resource' list box to include only port resources.
Memory Radio Button	The 'Memory' radio button updates the 'Resource' list box to include only memory resources.
All Radio Button	The 'All' radio button updates the 'Resource' list box to include all system resources. This includes IRQs, DMAs, ports, and memory resources.
Dump To File Button	The 'Dump To File' button writes the system resource usage information to the plain text file specified by the user. The system resource usage information file may be stored on either the client or server system.
Close Button	The 'Close' button exits the 'System Resource Usage' window.

5.2 Multiboot Manager (MBM) Add-in

The MBM does not include support for initialization files. Instead all parameters required to configure the operation of the MBM are stored in the Windows* registry.

5.2.1 User Interface / Operation

The MBM is implemented as an ActiveX control within the MDI CAF application.

The MBM presents a main window to the user that supports several features. These features are described in the following sections.

The IPL and Boot Connection Vector (BCV) priority in the 'Boot Device Priority' list shows that the first boot attempt will be on 'Removable Devices', followed by 'ATAPI CD-ROM drive', 'Hard Drive', and finally the 'LANDesk Service Agent'. The hard drive boot priority is determined by the 'Hard Drive' list, which shows the 'Other Bootable Device' will be booted first.

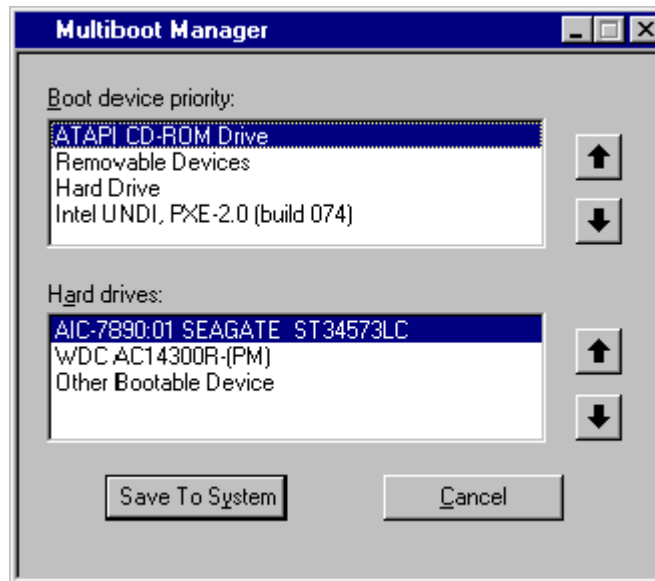


Figure 7 - 11. Multiboot Manager Main Window

Table 7 - 9: Multiboot Manager Main Window Options

Option	Function
Boot Device Priority List Box	The 'Boot Device Priority' list box contains the IPL devices in the system in descending boot priority.
Hard Drives List Box	The 'Hard Drives' list box contains the list of BCV devices in descending priority. Typically, the BCV device list contains hard disks installed in the system.
Move Up Buttons	The 'Move Up' buttons allows the user to move the selected IPL or BCV device up in the 'Boot Device Priority' or 'Hard Drives' list box respectively.
Move Down Buttons	The 'Move Down' buttons allows the user to move the selected IPL or BCV device down in the 'Boot Device Priority' or 'Hard Drives' list box respectively.
Save To System Button	The 'Save To System' button writes the updated boot priority information to non-volatile storage. Any changes made in the MBM re preserved by the MBM when it is re-invoked.
Cancel Button	The 'Cancel' button exits the MBM and returns the user to the AF. No configuration information is automatically written to non-volatile storage with this selection, and the user is not prompted to save any outstanding changes before exiting.

5.3 Password Manager (PWM) Add-in

The Password Manager (PWM) provides security and password support options. Within the PWM, the user can set or modify the current system passwords, or update various security options. Only a single instance of the PWM may be launched within the CAF.

5.3.1 Initialization Files

The PWM does not include support for initialization files. Instead, all parameters required to configure the operation of the PWM are stored in the Windows registry.

5.3.2 User Interface / Operation

The PWM is implemented as an ActiveX control within the MDI CAF application.

The PWM presents a main window to the user that supports several features broken into three sections relating to the 'Administrative Password', 'User Password', and the 'Security Options'.

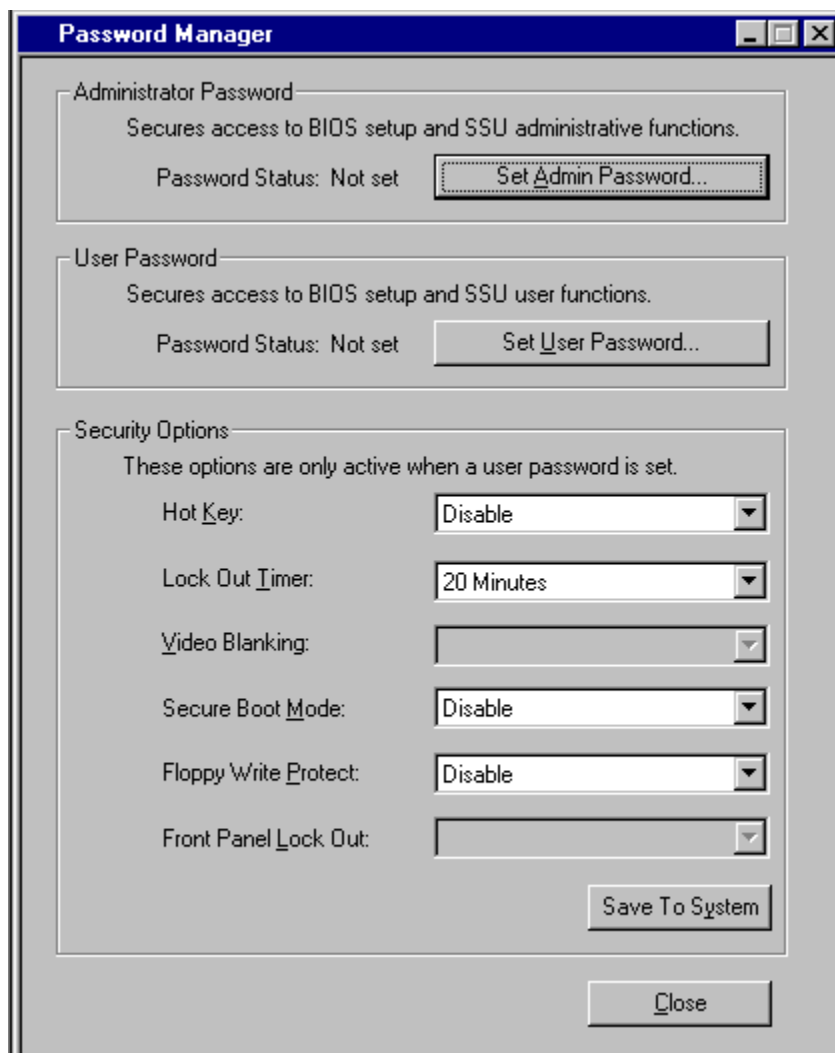


Figure 7 - 12. Password Manager Main Window

Table 7 - 10: Password Manager Main Window Options

Option	Function
Administrative Password Status Text	The administrative password support includes a text control used to display 'Password Status' information. The control displays either "Set" or "Not Set" depending on the current status of the administrative password.
Set Admin Password Button	The 'Set Admin Password Button' when clicked brings up the dialog that allows users to set the BIOS administrator password. Changes to a password take place immediately and do not require the "Save To System" button to be pressed. When a password is set, the text on this button changes to read "Change/Clear Admin Password".
Change/Clear Admin Password Button	The 'Change/Clear Admin Password' button allows the user to set or change the administrative password used by both the SSU and the system BIOS. All changes to the admin password take place immediately and do not require the 'Save To System' button to be pressed. Updates to the administration password are reflected in the 'Password Status' information as required.

Option	Function
Set User Password	This button should be clicked to bring up a dialog that allows the user to set the BIOS user password. Changes to a password take place immediately and do not require the "Save To System" button to be pressed. When a password is set, the text on this button changes to read "Change/Clear User Password".
Change/Clear User Password Button	The 'Change/Clear User Password' button allows the user to set or change the user password used by both the SSU and the system BIOS. All changes to the user password take place immediately and do not require the 'Save To System' button to be pressed. Updates to the administration password are reflected in the 'Password Status' information as required.
Hot Key Combo	The 'Hot Key' combo provides a list of valid secure mode hot keys, which may be selected. This option is only available when the user password is set; otherwise the option is "grayed out". The 'Hot Key' selection is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Lock Out Timer Combo	The 'Lock Out Timer' combo provides a list of valid secure mode timer values, which may be selected. The option is available only when the user password is set, otherwise it is "grayed out". The 'Lock Out Timer' option is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Secure Boot Mode	The 'Secure Boot Mode' combo allows the user to 'Enable' or 'Disable' secure boot mode. The option is available only when the user password is set, otherwise it is "grayed out". The 'Secure Boot Mode' option is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Video Blanking	The 'Video Blanking' combo allows the user to 'Enable' or 'Disable' secure boot mode. The option is available only when the user password is set, otherwise it is "grayed out". The 'Video Blanking' option is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Floppy Write Protect	The 'Floppy Write Protect' combo allows the user to 'Enable' or 'Disable' writing to the floppy drive when secure mode is active. The option is available only when the user password is set, otherwise it is "grayed out". The 'Floppy Write Protect' option is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Front Panel Lock Out	The 'Front Panel Lock Out' combo allows the user to 'Enable' or 'Disable' front panel support when secure mode is active. The option is available only when the user password is set, otherwise it is "grayed out". The "Front Panel Lock Out" option is saved to the platform via the 'Save To System' button. Support for this option may vary between platforms.
Save To System	The 'Save To System' button writes the updated security options to non-volatile storage. This button does not update either the administration or user password as they are updated immediately following a change. Any changes made in the PWM are preserved by the PWM when it is re-invoked.
Cancel Button	The 'Cancel' button exits the PWM and returns the user to the AF. No configuration information is automatically written to non-volatile storage with this selection, and the user is not prompted to save any outstanding changes before exiting.

5.4 System Event Log Add-In

The System Event Log Add-In (SEL) provides basic support for viewing and clearing the system event log on the server platform. Only a single instance of the SEL may be launched within the CAF.

5.4.1 Initialization Files

The SEL does not include support for initialization files. Instead, all parameters required to configure the operation of the SEL are stored in the Windows registry.

5.4.2 Internationalization

All strings and resources used within the SEL are stored in dynamic-link libraries. Each library contains the required strings and resources for a particular language/locale. The environment is extensible and extra dynamic link libraries supporting additional languages and locales can be added to the product at anytime.

5.4.3 User Interface / Operation

The SEL user interface and operation are described in the chapter on Common GUI for SEL, SDR, and FRU.

5.5 Sensor Data Record Manager Add-In

The Sensor Data Record Add-In (SDR) provides basic support for viewing sensor data record information on the server platform. Only a single instance of the SDR may be launched within the CAF.

5.5.1 Initialization and Customization Files

The SDR does not include support for initialization files. Instead, all parameters required to configure the operation of the SDR are stored in the Windows registry.

5.5.2 User Interface / Operation

The SDR user interface and operation are described in the chapter on Common GUI for SEL, SDR, and FRU.

5.6 Field Replaceable Unit Manager Add-In

The Field Replaceable Unit Add-In (FRU) provides basic support for viewing the FRU Inventory areas on the server platform.

Only a single instance of the FRU may be launched within the CAF.

5.6.1 Initialization Customization Files

The FRU does not include support for initialization files. Instead, all parameters required to configure the operation of the FRU are stored in the Windows registry.

5.6.2 User Interface / Operation

The FRU user interface and operation are described in the section titled Common GUI for SEL, SDR, and FRU.

5.7 System Update Manager Add-in

The System Update Manager (SUM) allows users to update the system BIOS or firmware code for various controllers (front panel controller, baseboard management controller, power share controller, etc.) on a server.

5.8 Platform Event Manager Add-in

The Platform Event Manager (PEM) provides an interface for configuring Platform Event Paging (PEP), BMC LAN-Alerts (BLA), and the Emergency Management Port (EMP).

5.9 Configuration Save / Restore Manager Add-in

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.

The Configuration Save/Restore Manager is explained in detail in chapter 7 of this section.

6. System Update Manager Add-in Component

The System Update Manager (SUM) is an add-in component that allows users to update the system BIOS or firmware code for various controllers on a server, such as the front panel controller, baseboard management controller, power share controller, etc. Only a single instance of the SUM may be launched within the CAF.

The SUM provides the following operations:

- Determines the current revision of BIOS and firmware on server controllers.
- Updates BIOS and/or firmware.
 - Updates the system BIOS with Intel BIOS files (.BIO file).
 - Updates operational code for controllers using files composed of Intel 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.
- Verifies the code currently loaded versus an external hex file.
 - BIOS cannot be verified (.BIO file).
 - Verifies the firmware for controllers using files composed of Intel Hex Format code (.HEX file).
 - Verifies the firmware of controllers by using a user-specified .UIF file.

6.1 Initialization Files

The SUM does not include initialization files. Instead, all parameters required to configure the operation of the SUM are stored in the Windows registry.

6.2 Internationalization

All strings and resources used within the SUM are stored in dynamic-link libraries. Each library contains the required strings and resources for a particular language and locale. The environment is extensible; dynamic-link libraries supporting additional languages and locales can be added to the product at any time.

6.3 User Interface / Operation

The SUM is implemented as an ActiveX control within the MDI CAF application. The main window of the SUM provides a table to display device, current revision, and status information. The Update, Verify, and Close buttons provide users corresponding actions. The SUM main window is shown below.

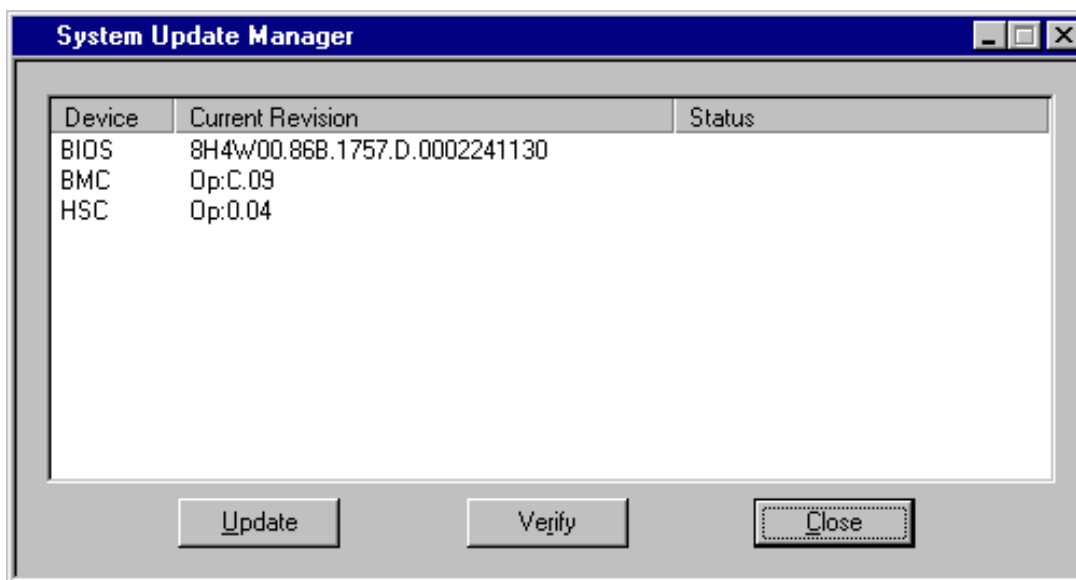


Figure 7 - 13. System Update Manager Main Window

Table 7 - 11: System Update Manager Main Window Options

Option	Function
Device	The name of the device
Current Revision	The version of the BIOS or firmware currently installed
Status	The status of an update or verify operation. For example, if a controller is to be updated to firmware version 2.1, during the update the status area will display "Updating"; when the update is complete, it will show "Updated". During a verify operation, the status area shows "Verifying"; and when the verification is complete, it will display "Verified"
Update Button	This button causes an update operation to occur. When this button is clicked, a file dialog appears so the user can select the file to be used for the update. The file selected can be on the client or the server, and can be a .UIF, .BIO, or .HEX file. If the file is on the client, it is first downloaded to the server and then the update operation takes place. During the update operation, the Status area in the table changes as indicated above.
Verify Button	This button causes a verify operation to occur. When this button is clicked, a file dialog appears so the user can select the file to be used for the update. The file selected can be on the client or the server, and can be a .UIF or .HEX file. Verify operations cannot be done with .bio files. If the file is on the client, it is first downloaded to the server and then the verify operation takes place. During the verify operation, the Status area in the table changes as indicated above.
Close Button	The close button exits the SUM. If an update or verify operation is taking place, an hourglass is displayed, so the Close button cannot be clicked during that time.

6.3.1 Confirmation Dialog

Before starting an update or verify operation, a confirmation dialog appears asking the user to verify that the version information for the update or verify is correct. This dialog shows the device, the current version of BIOS or firmware installed, and the version to be updated to. This dialog allows the user a chance to cancel the update or verify operation before it has started.

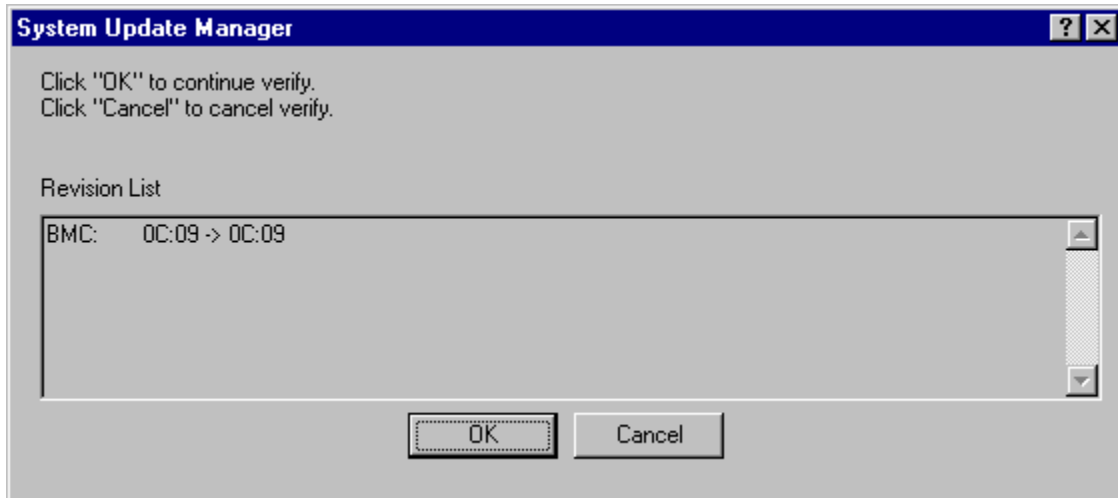


Figure 7 - 14. SUM Verify Operation Confirmation Dialog

6.4 Recovery Agent

The presence of correctly working BMC firmware is necessary for correct operation of a server. However, with the ability to perform remote BMC firmware updates to a server comes the possibility of an error occurring during an update. To help recover from BMC update errors, a recovery agent program is on the service partition of the server.

When a remote BMC firmware update is being done, a checkpoint file is written to the service partition by the System Update add-in on the server side that is handling the update request from the client. The checkpoint file is written at various times during the update to indicate the progress of the update because there are several points at which the recovery operation can begin.

If an error occurs during the update, the recovery agent is invoked. It reads the checkpoint file and starts a recovery process from that point. Up to three attempts are made to recover from BMC firmware update errors. If the update cannot be successfully completed after three attempts, the SUM will inform the user that the server cannot be updated.

Note: The recovery agent is an executable file named `recover.exe` (in the service partition). If a remote BMC update is attempted and for some reason this file does not exist, an error will be reported to the SUM and the update will not take place.

More details on the recovery agent and the BMC firmware update process are given in the following sections.

6.4.1 General Update Process

The following steps are performed to remotely update the BMC firmware on a server:

1. The new firmware image file is transferred to the service partition on the server.
2. Current firmware settings and SDRs are saved to files in the service partition.
3. The firmware on the server is put in update mode so the firmware can be updated.
4. The firmware is put in operational mode to run the new firmware.
5. The saved firmware settings and SDRs are restored.
6. The checkpoint file is removed.
7. The server is reset to bring the firmware and BIOS into alignment.

Each of these steps is described in more detail below.

6.4.1.1 Step 1: Transfer Firmware Image to Server

After the new firmware file is downloaded to the server, the SUA on the server writes to the checkpoint file on the service partition to indicate that the file firmware file is on the service partition.

If the recovery agent software is running, it updates the number of recovery attempts that have been made. This number is kept in a file on the service partition.

The SUA calls the BIOS with a Set BIOS Flags command. This flag forces a boot to the service partition. With this flag set, if an error occurs during the update, the server will reboot to the service partition, and the recovery agent software will run. The BIOS flag remains set until it is cleared by the SUA or recovery agent.

6.4.1.2 Step 2: Save Firmware Settings and Recovery Information

The SUA / recovery agent saves current firmware settings into a file on the service partition, so it can restore them after the update completes. Other data, such as SDRs, are also saved.

The operational mode watchdog timer in the BMC firmware is set to 'running'. This timer ensures that if a system hang occurs before entering update mode, then when the timer expires, a reboot to the service partition will occur so the recovery agent can run. This timer stops running when update mode is entered.

Remote connections (such as EMP and LAN) are disabled. This is done so that if a problem occurs and a reboot to the service partition takes place, the recovery agent can run without a connection being established from a remote console. At this point, the EMP does not own the serial port so that if a modem connection exists, it is between the CSSU and the SUA.

The checkpoint file is written to indicate that the update process reached the point of saving all configuration settings.

6.4.1.3 Step 3: Put Firmware in Update Mode

The SUA puts the firmware into update mode, writes the new code into the BMC firmware storage device, verifies the new contents, and writes the checkpoint file to indicate that the update process reached this point.

The BMC firmware (in the boot block) enables the boot block watchdog timer before beginning the update of the operational code. This timer watches firmware command activity. It assumes that commands occur occasionally when the firmware is in update mode. If no command activity is detected in a certain amount of time, the server will be rebooted to the service partition and the recovery agent will run. The SUA has the capability to set or modify the timer length.

6.4.1.4 Step 4: Put Firmware in Operational Mode

The SUA / recovery agent puts the firmware into operational mode and then writes to the checkpoint file indicating the update process reached this point.

The SUA / recovery agent again enables the operational mode watchdog timer in the firmware so that if a problem occurs at this point, a reboot to the service partition will occur and the recovery agent can perform the remaining update steps. The checkpoint file is again written to indicate that the operational mode watchdog timer has been enabled.

6.4.1.5 Step 5: Restore Firmware Settings

The SUA / recovery agent writes the saved firmware settings and SDRs from the files where they are stored back to the appropriate locations. The checkpoint file is written to indicate the settings have been restored.

Remote connection capability is restored and the operational mode timer in the firmware is disabled.

6.4.1.6 Step 6: Clear Checkpoint Information

The SUA/recovery agent removes the checkpoint file and other files created for use by the recovery agent from the service partition. A call is made to the BIOS with a Set BIOS Flags command to clear the flag that causes the server to reboot to the service partition.

6.4.1.7 Step 7: Reset Server

The SUM informs the user that the server is going to be reset. Any other managers open under the CSSU are closed and the server is reset. It is up to the user to reconnect to the server to perform any other management functions; no automatic reconnect is done.

6.4.1.8 Checkpoint File Format

This section describes the basic format of the checkpoint file that is used by the recovery agent in case of a failure during remote BMC firmware updates. The checkpoint file is a binary file that uses the filename `checkpnt.dat`. This file is only created when a remote BMC firmware update is attempted. It is removed following a successful update.

Table 7 - 12: Checkpoint File Format

File Component	Description
Header	"CheckPoint vNN" where NN is the version number of the checkpoint file format. (Header stored as 14 ASCII characters, followed by NULL terminator.)
Address of controller	Two byte field containing the IPMB address of the controller to perform the recovery on (one byte is sufficient, but making two for future expandability). This address should always be the BMC address.
Name of .HEX file in use when update failure occurred	15-byte filename in 8.3 format, such as HEMBMCC2.HEX
Name of file containing SDRs	SDRs are saved before a BMC update is started. 15 byte filename in 8.3 format, such as SDR.BAK
Name of saved firmware configuration settings file	15 byte filename in 8.3 format such as FWCONFIG.BAK
Location in update process	Two byte unsigned integer: 10: No actions taken 20: Configuration information saved 30: SDRs saved 40: Firmware written to flash 50: Firmware contents verified 60: Configuration settings restored 70: SDRs restored
Number of recovery attempts done	Two-byte unsigned integer

7. Platform Event Manager Add-in Component

The Platform Event Manager (PEM) provides an interface for configuring Platform Event Paging (PEP), BMC LAN-Alerts (BLA), and the Emergency Management Port (EMP).

7.1 Initialization Files

The PEM does not include support for initialization files. Instead, all parameters required to configure the operation of the PEM are stored in the Windows registry.

7.2 Internationalization

All strings and resources used within the PEM are stored in dynamic-link libraries. Each library contains the required strings and resources for a particular language/locale. The environment is extensible and has extra dynamic link libraries supporting additional languages and locales can be added to the product at anytime.

7.3 User Interface / Operation

The PEM is implemented as an ActiveX control within the MDI CAF application. The following sections describe the overall operation of the Platform Event Manager.

7.3.1 Platform Event Manager Window

The PEM presents a main window to the user that supports the features indicated by the following diagram. These features are described in additional detail in the following sections. Only a single instance of the PEM main window may be launched for a given SSU Client session.

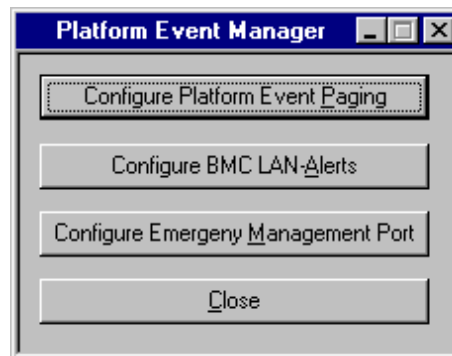


Figure 7 - 15. Platform Event Manager Main Window

Table 7 - 13: Platform Even Manager Main Window Options

Option	Function
Configure Platform Event Paging	The 'Configure Platform Event Paging' button allows the user to configure the Platform Event Paging features. All changes to must be saved before exiting the Platform Event Paging dialog.
Configure BMC LAN-Alerts	The 'Configure BMC LAN-Alerts' button opens a new dialog that allows the user to configure the BMC LAN-alert features. All changed must be save before exiting the BMC LAN-Alert dialog
Configure Emergency Management Port Button	The 'Configure Emergency Management Port' button allows the user to configure the Emergency Management Port features. All changes must be saved before exiting the Emergency Management Port dialog.
Close Button	The 'Close' button closed the Platform Event Manager.

7.3.2 Platform Event Paging Dialog

This window provides the ability to configure the Platform Event Paging features.

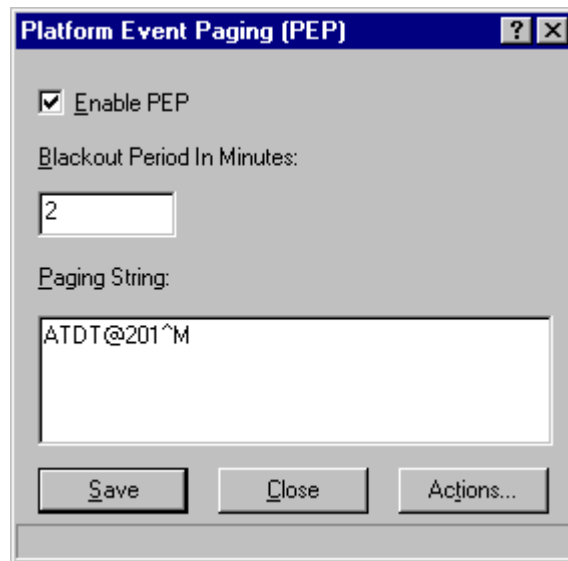


Figure 7 - 16. Platform Event Paging Dialog

Table 7 - 14: Platform Event Paging Options

Option	Function
Enable PEP checkbox	The 'Enable Platform Event Paging' checkbox is used to enable or disable the PEP feature entirely.
Blackout Period in Minutes Edit	The 'Blackout Period In Minutes' edit allows the user to set the time, in minutes, between successive pages. The valid range is [0 – 255] where 0 disables the blackout period.
Paging String Edit	The 'Paging String' edit field allows the user to enter the paging string that contains both the paging service number and the characters that are sent once the connection has been made. The length of the paging string is determined at run-time from firmware. The user will be notified if the string is truncated and the screen will be updated with the saved string
Close Button	The 'Close' button exits the PEP dialog without saving changed. If changes have been made, the user will be prompted with the option of saving changes before closing.
Actions Button	The 'Actions' button launched the PEP Actions Dialog (See figure 6-3) to allow the user to configure the event actions.
Save Button	The 'Save' button allows the user to save the configuration immediately.

7.3.3 BMC LAN-Alert Dialog

This dialog allows the user to configure the BMC LAN-Alert features.

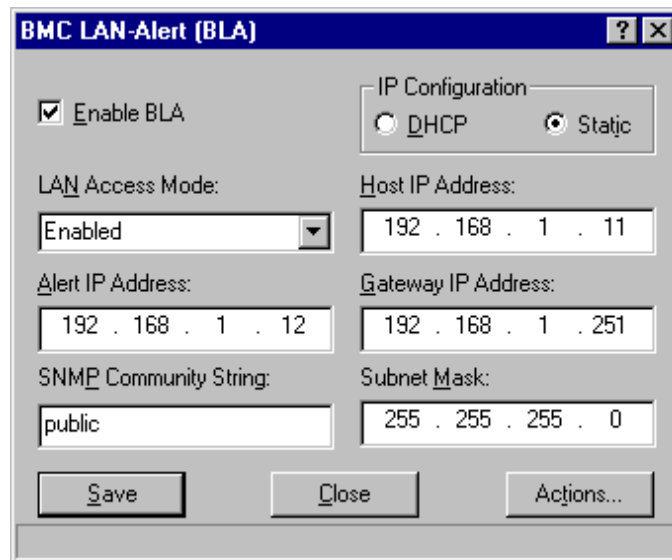


Figure 7 - 17. BMC LAN-Alerting Dialog

Table 7 - 15: BMC LAN-Alert Dialog Options

Option	Function
Enable BLA checkbox	The 'Enable BLA' checkbox allows the user to enable and disable BMC LAN-Alerting
LAN Access Mode combo	The 'LAN Access Mode' combo allows the user to set the remote access mode desired. The valid choices are Enable, Disabled and Restricted. In Enabled mode, a remote system can initiate a LAN session regardless of system state or health. In Disabled mode remote LAN sessions cannot be initiated. In Restricted mode control operations such as power down, front panel NMI, and reset cannot be performed.
Alert IP Address Edit	The 'Alert IP Address' is the logical or Internet address of the Alert-Destination. In case of single node destination this is the unicast or specific IP address. This is the IP Subnet address if the alert needs to be broadcast within a particular subnet. The 'Alert IP Address' is always saved when a user invokes the save action. The IP is entered as a dotted IP, e.g., 192.168.1.12.
SNMP Community String Edit	The 'SNMP Community String' can be configured for the community field in the Header section of the SNMP trap sent for a LAN alert. The default string is 'public'.The string must be from [5 – 16] characters long.
DHCP Radio Button	The 'DHCP' radio button enables the dynamic host configuration protocol to allow the server to automatically assign the host IP address, router IP address and subnet mask. If the 'DHCP' radio button is checked, the host IP address, router IP address and subnet mask will not be saved if the user invokes the save action. The current values will remain in effect.
Host IP Address Edit	The 'Host IP Address' is the Logical or Internet Address of the host. The 'Host IP Address' will only be saved when DHCP is disabled. The IP is entered as a dotted IP, e.g., 192.168.1.11.
Router IP Address Edit	The 'Router IP Address' is the Logical or Internet Address of the router. The 'Router IP Address' will only be saved when DHCP is disabled. The IP is entered as a dotted IP, e.g., 192.168.1.251.
Static Radio Button	The 'Static' radio button allows the user to set the server host IP address, router IP address and subnet mask. If the 'Static' radio button is checked, the host IP address, router IP address and subnet mask will be saved if the user invokes the save action. The values saved will take effect immediately.
Subnet Mask Edit	The 'Router IP Address' is the Logical or Internet Address of the router. The 'Router IP Address' will only be saved when DHCP is disabled. The IP is entered as a dotted IP, e.g., 192.168.1.251.
Actions Button	The 'Actions' button launches the Platform Event Paging Actions Dialog(see Figure 6-4) to allow the user to configure event actions.
Save Button	The 'Save Button Allows the user to save the configuration immediately.
Close Button	The 'Close' button allows the user to close the BMC LAN-Alert dialog without saving changes. If changes have been made, the user will be prompted with the option of saving changes before closing.

7.3.4 Platform Event Action Dialogs

This dialog allows the user to configure the Platform Event Action features.

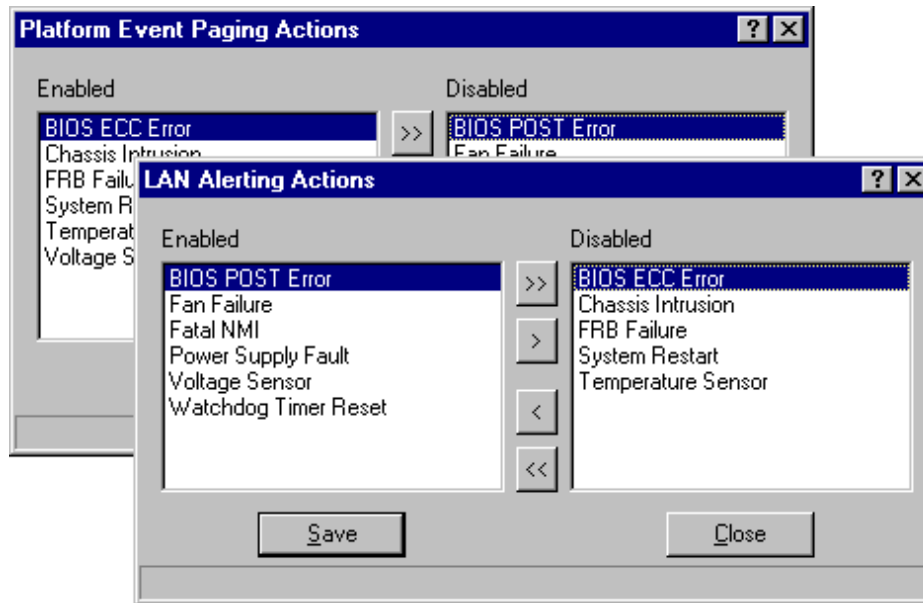


Figure 7 - 18. Platform Event Action Dialogs

Table 7 - 16: Platform Event Action Dialog Options

Option	Function
Enabled List box	The 'Enabled' list box contains the filters that are active.
Disabled List box	The 'Disabled' list box contains the filters that are not active.
>> Button	The '>>' button moves all the filters from the enabled list box to the disabled list box.
> Button	The '>' button moves the selected filter(s) from the enabled list box to the disabled list box.
< Button	The '<' button moves the selected filter(s) from the disabled list box to the enabled list box.
<< Button	The '<<' button moves all the filters from the disabled list box to the enabled list box.
Save Button	The 'Save Button Allows the user to save the configuration immediately.
Close Button	The 'Close' button allows the user to close the BMC LAN-Alert dialog without saving changes. If changes have been made, the user will be prompted with the option of saving changes before closing.

7.3.5 Emergency Management Port Dialog

This dialog allows the user to configure the Emergency Management Port features.

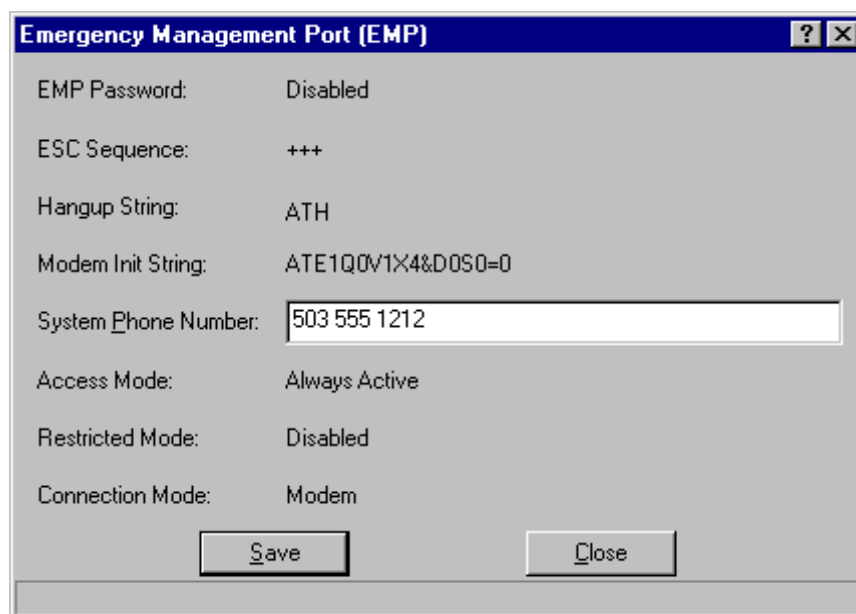


Figure 7 - 19. Emergency Management Port Dialog

Table 7 - 17: Emergency Management Port Dialog Options

Option	Function
EMP Password	The 'EMP Password' state will be listed here, Enabled or Disabled.
ESC Sequence	The 'ESC' sequence string is sent to the modem before sending a command string to the modem.
Hang up String	The 'Hangup Line' string is sent to the modem whenever the EMP wants to terminate the session. The EMP automatically sends an <ENTER> character after this string
Modem Init String	The 'Modem Init String' string is transmitted every time the EMP initializes.
System Phone Number Edit	The 'System Phone Number' is entered by a user and can be retrieved and reported via in-band management connections. The length of the system phone number is determined at run-time from firmware. The user will be notified if the string is truncated and the screen will be updated with the saved value.
Access Mode	The 'Access Mode' allows the user to set the points during system operation when the EMP can be activated. The current EMP access mode will be displayed here: Preboot, Always Active or Disabled.
Restricted Mode	The 'Restricted Mode' current setting will be displayed her: enabled or disabled.
Connection Mode Combo	The 'Connection Mode' current setting will be displayed her: modem or direct.
Save Button	The 'Save Button Allows the user to save the configuration immediately.
Close Button	The 'Close' button allows the user to close the BMC LAN-Alert dialog without saving changes. If changes have been made, the user will be prompted with the option of saving changes before closing.

8. Configuration Save/Restore Manager Add-in Component

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.

Only a single instance of the CSR may be launched within the CAF.

8.1 Initialization Files

The CSR does not include support for initialization files. Instead, all parameters required to configure the operation of the CSR are stored in the Windows registry.

8.2 Internationalization

All strings and resources used within the CSR are stored in dynamic-link libraries. Each library contains the required strings and resources for a particular language/locale. The environment is extensible and extra dynamic link libraries supporting additional languages and locales can be added to the product at anytime.

8.3 User Interface / Operation

The CSR is implemented as an ActiveX control within the MDI CAF application. The following sections briefly describe the overall operation of the Configuration Save/Restore Manager.

8.3.1 CSR Main Window

The CSR presents a main window that contains buttons to support saving and restoring configuration information. Configuration information can be saved to a file on the local client or the remote server. A configuration to be restored can be in a file on either the local or remote system.

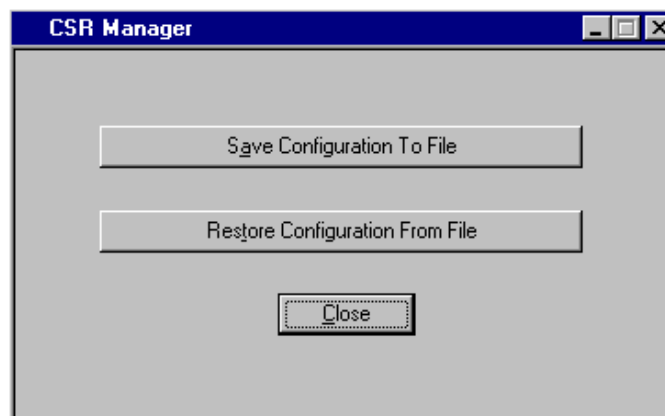


Figure 7 - 20. CSR Manager Main Window

Table 7 - 18: CSR Manager Main Window Options

Option	Function
Save Configuration to File	<p>When the "Save Configuration To File" button is clicked, the user is first asked whether the file is to be saved on the local or remote file system. The user is then shown a file dialog window that allows the location and name of the file to be specified. A save operation cannot be cancelled.</p> <p>The BIOS version string and the firmware version information for the BIOS and firmware currently installed on the system are saved in the backup file. This data is used during a restore operation to determine if a restore can be safely done or not (refer to section on Restore From File button).</p>
Restore Configuration From File	<p>When the "Restore Configuration From File" button is clicked, the user is first asked whether the file containing the data to be restored is located on the local or remote file system. The user is then shown a file dialog window that allows the location and name of the file to be specified. A valid configuration backup file contains data that identifies it as a backup file that the CSR Manager can interpret. If the file specified is not a valid backup file, an error message is displayed.</p> <p>A restore operation compares the BIOS and firmware version information on the server to which a configuration is to be restored with the version information in the selected backup file. If the version information does not match, the user is told of the mismatch and asked whether the restore operation should continue. Because of variations in bit assignments between BIOS or firmware revisions, restoring a configuration on a server for which the currently installed BIOS or firmware versions do not match those in the backup file can cause the server to operate incorrectly.</p>
Close	<p>The Close button closes the CSR Manager dialog window. Once a save or restore operation is begun, this button cannot be used to stop that operation.</p>

8.3.2 Configuration Data

During a Save operation, the CSR Manager saves the non-volatile data listed below to a file. Some data is not restored during a restore operation; exceptions are noted below.

- All data in all Complementary Metal-Oxide Semi-Conductor (CMOS) banks. During a restore operation, the first 16 bytes of bank 0 are not restored since these bytes contain information that cannot be altered.
- The entire Extended System Configuration (ESCD) area. The size of this area can vary from platform to platform.
- All PCI records (if not stored in ESCD; if the records are in ESCD, they are saved as part of the ESCD).
- EMP data: configuration data – one byte. This data contains settings for items such as
 - whether an EMP password is set
 - whether EMP is set up for direct connect or modem access
 - the EMP activation mode (for example, always active)

It also contains three modem strings and the system phone number. While EMP data is stored in the configuration file, it is not restored when doing a remote configuration restore. This is because if there are problems with any EMP settings, such as modem strings, the user will not be able to dial back in to the server.

- PEP data: page blackout interval; page string; page string length.
- PEF data: configuration data (two bytes, each with one non-volatile bit in it); PEF table entries. For the configuration data, the non-volatile bit in the first byte is bit 7, the enable PEF bit; in the second byte, the non-volatile bit is also bit 7, the PEF enable mask bit.

Intel® Server Control, Version 3.x TPS

Section 8: Platform Instrumentation Control (PIC)

Table of Contents

1. Introduction to Platform Instrumentation Control (PIC)	1
2. Platform Instrumentation	2
2.1 Local Response Agent	3
3. PIC Graphical User Interface	4
3.1 Main Menu	5
3.1.1 File Menu	6
3.1.2 View Menu	6
3.1.3 Configure Menu.....	7
3.1.4 ICMB Menu	7
3.1.5 Help Menu.....	8
3.2 Toolbar.....	8
3.3 Navigation Pane.....	10
3.3.1 Health.....	10
3.4 Presentation Pane.....	12
3.4.1 Group Information	12
3.5 LCD Display	16
3.6 Status Bar	17
3.7 Popup Menus	18
3.7.1 Presentation Pane Popup Menu.....	18
3.7.2 Toolbar Popup Menu.....	19
3.7.3 LCD Popup Menu.....	19
3.7.4 Status Bar Popup Menu	19
4. Individual Sensor / Server Information	20
4.1 Sensor Settings Tab Page	21
4.1.1 Threshold Values Rounded Off	22
4.1.2 Avoiding a Reboot-Fail Retry Loop.....	22
4.2 Sensor Status Tab Page	23
4.3 Alert Actions Tab Page.....	24
4.3.1 Avoiding a Power On/Off Loop.....	27
4.4 Sensor Information Tab Page	27
4.5 Inventory Information Tab Page	28

5. PIC Dialogs.....	30
5.1 Options Dialog.....	30
5.2 Restoring Factory Defaults Dialog.....	31
5.3 Watchdog Timer Dialog.....	31
5.4 Paging Configuration Dialog.....	32
5.5 ICMB Configuration Dialog.....	34
5.6 ICMB Remote Server(s) Dialog.....	35
6. Sensor Controls.....	37
6.1 Chassis.....	37
6.2 Fan.....	39
6.3 Memory Array.....	40
6.4 Memory Device.....	41
6.5 PCI Hot Plug Device.....	43
6.6 Power Supply.....	44
6.7 Power Unit.....	45
6.8 Processor.....	46
6.9 System Information.....	47
6.9.1 Field Replaceable Unit (FRU).....	48
6.9.2 Operating System.....	49
6.9.3 System BIOS.....	50
6.9.4 System Event Log (SEL).....	51
6.10 System Slots.....	52
6.11 Temperature.....	54
6.12 Third Party Instrumentation.....	56
6.13 Voltage.....	59

List of Figures

Figure 8 - 1: Platform Instrumentation Control and Platform Instrumentation	2
Figure 8 - 2: PIC Container	4
Figure 8 - 3: Main Menu	5
Figure 8 - 4: Toolbar.....	8
Figure 8 - 5: PIC Main Dialog, Toolbar Hidden	9
Figure 8 - 6: Navigation Pane.....	10
Figure 8 - 7: Health View in Main Dialog.....	11
Figure 8 - 8: Presentation Pane, Large Icon View	12
Figure 8 - 9: Presentation Pane, Small Icon View	13
Figure 8 - 10: Presentation Pane, List View	13
Figure 8 - 11: Presentation Pane, Detail View	14
Figure 8 - 12: Arrange Icons by Name, List Icon View.....	15
Figure 8 - 13: Arrange Icons by Status, List Icon View	16
Figure 8 - 14: LCD Display Pane.....	16
Figure 8 - 15: Managed Server without LCD, or LCD Hidden	17
Figure 8 - 16: Status Bar	17
Figure 8 - 17: PIC Main Dialog, Status Bar Hidden	18
Figure 8 - 18: Presentation Pane Popup Menu.....	18
Figure 8 - 19: Toolbar Popup Menu.....	19
Figure 8 - 20: LCD Popup Menu.....	19
Figure 8 - 21: Status Bar Popup Menu	19
Figure 8 - 22: Tab Pages in Presentation Pane.....	20
Figure 8 - 23: Sensor Settings Tab Page	21
Figure 8 - 24: Sensor Status Tab Page	23
Figure 8 - 25: Alert Actions Tab Page	25
Figure 8 - 26: Sensor Information Tab Page	28
Figure 8 - 27: Inventory Information Tab Page	29
Figure 8 - 28: Options Dialog	30
Figure 8 - 29: PIC Watchdog Timer Dialog.....	32
Figure 8 - 30: Paging Configuration.....	32
Figure 8 - 31: ICMB Configuration Dialog.....	34

Figure 8 - 32: ICMB Remote Server(s) Selection Dialog	35
Figure 8 - 33: PIC Main Dialog, Managing a Remote Server via ICMB.....	36
Figure 8 - 34: Chassis Sensor Status.....	38
Figure 8 - 35: Fan Sensor Settings.....	39
Figure 8 - 36: Memory Array Sensor Status	40
Figure 8 - 37: Memory Device Sensor Status	42
Figure 8 - 38: PCI Hot Plug Device Sensor Information	43
Figure 8 - 39: Power Supply Sensor Status.....	44
Figure 8 - 40: Power Unit Sensor Status	45
Figure 8 - 41: Processor Sensor Status	46
Figure 8 - 42: Field Replaceable Unit (FRU) Inventory Information	48
Figure 8 - 43: Operating System Information.....	49
Figure 8 - 44: System BIOS Information.....	50
Figure 8 - 45: System Event Log Information	51
Figure 8 - 46: PHP System Slots Sensor Information.....	52
Figure 8 - 47: Non-PHP System Slots Sensor Information	53
Figure 8 - 48: Temperature Sensor Settings	54
Figure 8 - 49: Third Party Alert Actions	56
Figure 8 - 50: Voltage Sensor Settings.....	59

List of Tables

Table 8 - 1: View Menu Options 6

Table 8 - 2: Toolbar Options..... 8

Table 8 - 3: Audio and Visual Notifications 26

Table 8 - 4: Shutdown and Power Control Actions 26

1. Introduction to Platform Instrumentation Control (PIC)

Platform Instrumentation Control (PIC) is a server management tool that provides real time monitoring and alerting for server hardware sensors. PIC consists of a Windows 32 graphical user interface (GUI) that communicates to the platform instrumentation (PI) resident on the server. PIC is designed to dynamically detect and display the management capabilities of Enterprise Server Group (ESG) platforms.

PIC allows system administrators to:

- Remotely monitor server hardware sensors
- Configure sensor thresholds
- Configure, receive, and act upon alert events
- Configure options to shutdown, reboot, or power-off the system automatically

As with the other Intel® Server Control (ISC) components, PIC uses a user-friendly graphical interface for monitoring and controlling the platform management features of the system. It is designed as a set of ActiveX controls that communicates to the server using the standard Desktop Management Interface Version 2.0 (DMI 2.0) remoting interfaces.

PIC integrates into the enterprise and workgroup management consoles, as well as into the ISC Standalone container. It relies on the management console or ISC Standalone for discovery of servers over the Local Area Network (LAN). Changes in the server state are propagated to the management consoles for appropriate alert handling.

2. Platform Instrumentation

Platform Instrumentation consists of the server-resident software required for monitoring and controlling the server when the operating system is on-line. The core instrumentation is implemented as platform instrumentation under the Desktop Management Interface 2.0 management framework.

A large set of the standard DMI 2.0 groups are used to make the instrumentation more manageable by management consoles that understand the semantics of the standard groups. All DMI standard groups that are required by 'Wired For Management' (WfM) 1.1a specifications are instrumented. The instrumentation retrieves data from the operating system as well as from the Platform Management Technology (hardware, firmware and BIOS).

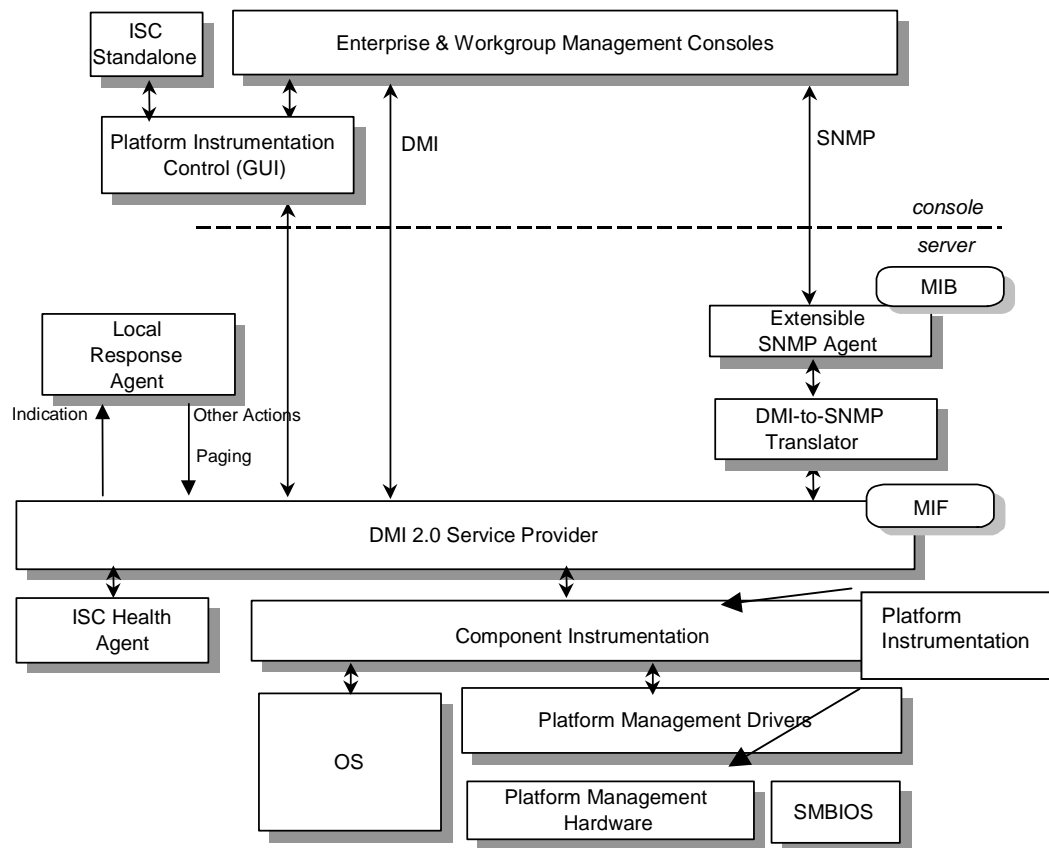


Figure 8 - 1: Platform Instrumentation Control and Platform Instrumentation

Platform Instrumentation also provides instrumentation data for the servers connected through the Intelligent Chassis Management Bus Bridge (ICMB). This allows PIC to use the Platform Instrumentation on one server to access the Platform Management Technology on another target server/chassis. This is useful when the target server is not fully operational and cannot be reached directly by the PIC, or when the target server is running an operating system (OS) that is not supported by the Platform Instrumentation.

2.1 Local Response Agent

Any change in the Server State generates a DMI indication. These indications are consumed by the Local Response Agent (LRA), which responds to the arrival of indications by taking actions such as:

- Power Off
- Reset
- Shutdown
- Non Maskable Interrupt (NMI)
- Beep the System Speaker
- Log to Disk
- Broadcast a message on the network and display a message on the system console

If the LANDesk Server Manager components are installed on the server and at the console, then the LRA also converts the DMI indication into an alert that is sent to the LANDesk Alert Management System (AMS-2).

A new paging capability has been added to the set of LRA actions. The Local Response Agent actions are programmable on a per-indication basis. Indications are also exported from the server directly to the interested DMI management applications.

A cross-mapper (SDLINK) is supported to allow access to the core DMI instrumentation on the servers from the SNMP consoles. The cross-mapper supports read and modify operations (gets and sets) from the SNMP consoles. The cross-mapper supports conversion of DMI indications into SNMP traps.

3. PIC Graphical User Interface

Note: Before launching the ISC GUI, a five-minute delay should be allowed after Windows 95* or Windows NT* loads. This will allow the OS sufficient time to start all services required for the ICMB discovery process.

As pictured below, PIC application uses a Windows Explorer*-like model, with a Navigation (tree view) Pane on the left and a Presentation (list view) Pane on the right.

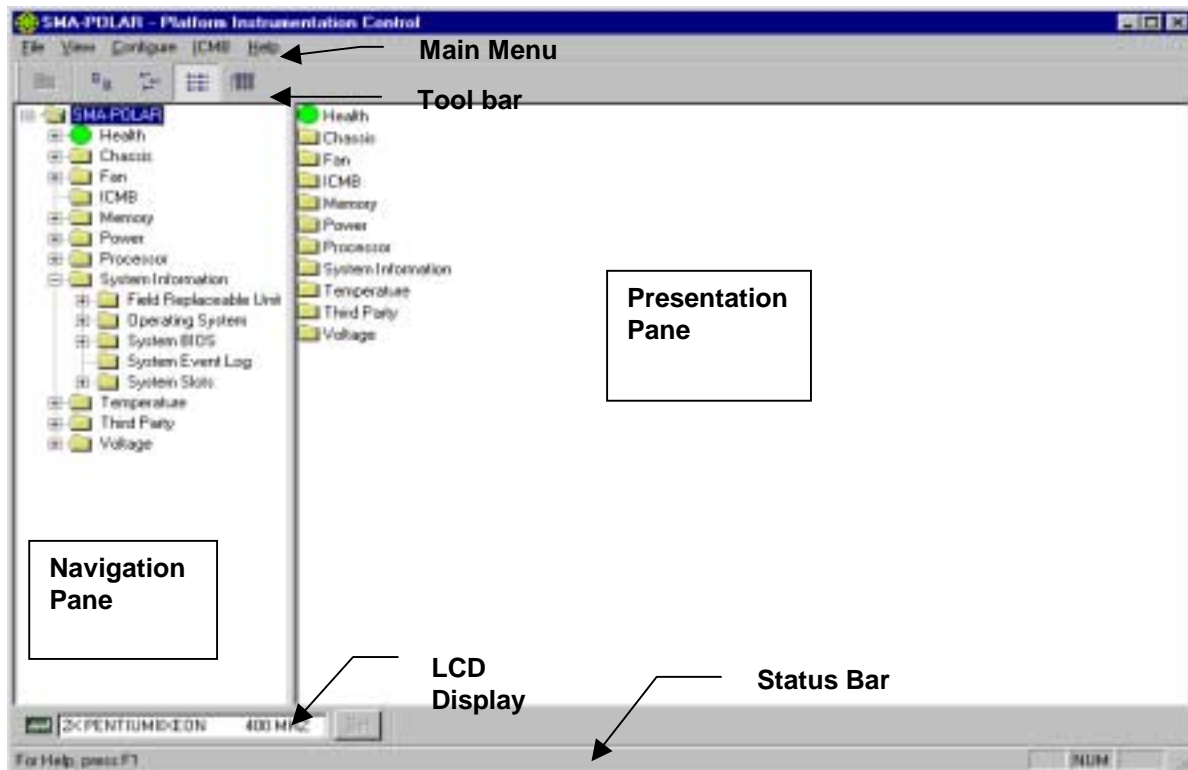


Figure 8 - 2: PIC Container

During initialization, PIC communicates with the managed server to determine which sensors are supported on the server. This information is used to build the navigation tree in the main window. PIC also determines the server health status and initializes the Health branch in the navigation tree.

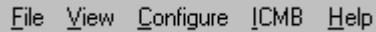
While initializing, the ISC bitmap is displayed in the Presentation Pane. The initialization progress is visible in the status bar as a series of vertical bars that are drawn from left to right until the initialization is complete and the status bar changes to “Ready”.

The Health branch provides the user with a quick and simple view of the current server health. All unhealthy sensors (status not OK) will be collected under the Health branch. If the server supports a Liquid Crystal Display (LCD), then the LCD display pane is also visible on the main window. When initialization is complete, the ISC bitmap is replaced with the list of managed sensors.

When the user navigates to a sensor in the tree view, a set of tabbed pages will appear in the Presentation Pane displaying sensor specific information. The administrator uses the Navigation Pane to select a sensor. Sensor information can be viewed, or sensor information updated, in the Presentation Pane.

The following sections provide a detailed overview of the screen components and activities that may be performed by using PIC.

3.1 Main Menu



The image shows a horizontal menu bar with five items: 'File', 'View', 'Configure', 'ICMB', and 'Help'. Each item has a small icon to its left. The menu is displayed in a light gray background with black text.

Figure 8 - 3: Main Menu

The Main Menu options may be outlined as follows. Details of the Main Menu options follow in the sections below.

File Menu

- Exit

View Menu

- Toolbar
- Status Bar
- LCD Display
- Large Icons
- Small Icons
- List
- Details
- Arrange Icons
- Refresh
- Options

Configure Menu

- Enable Front Panel Power and Reset
- Power off the server immediately
- Immediate Hardware Reset Server

- Enable Watchdog Timer
- Watchdog Timeout Value
- Paging Configuration
- Restore Factory Defaults

ICMB Menu

- View Managing Server
- View Managed Server(s)
- Reclaim Inactive Resources

Help Menu

- Help Topics
- About PIC

3.1.1 File Menu

The File Menu option contains only Exit. This command exits the application.

3.1.2 View Menu

The View Menu offers options to change options that are visible and to change the order in which options may be seen. The following menu options are available from the View Menu:

Table 8 - 1: View Menu Options

Option	Description
Toolbar	This command toggles the toolbar visibility. By default this option is checked and visible.
Status Bar	This command toggles the status bar visibility. By default this option is checked and visible.
LCD Display	This command toggles the LCD pane visibility. By default this option is checked and visible.
Large Icons	This command displays list view items using large icons. Large Icon view is the default choice.
Small Icons	This command displays list view items using small icons.
List	This command displays list view items in list format. This is the default view format.
Details	This command displays list view items in detail format.
Arrange Icons	This command allows the user to arrange the list view item icons by name or by status. Default value is by status.
Refresh	This command triggers an immediate screen and data refresh.
Options	This command displays the view options dialog, which allows the user to configure viewing preferences such as temperature display unit and GUI refresh interval.

3.1.3 Configure Menu

The Configure Menu provides selections to perform power-related functions at the server, and to perform select configuration functions at the server, such as Paging and changing the Watchdog timeout value. The available options are as follows:

- **Enable Front Panel Power and Reset**
This command toggles the server's front panel power and front panel reset buttons. By default, these features are enabled. If disabled, the server front panel buttons will not respond when pressed.
- **Power off the server immediately**
This command immediately powers down the server. This action is an immediate power-off without a shutdown of the OS; it might corrupt files. Use with caution.
- **Immediate Hardware Reset Server**
This command immediately resets the server via hardware. This action is an immediate hard reset without a shutdown of the OS; it might corrupt files. Use with caution.
- **Enable Watchdog Timer**
This command toggles the watchdog timer option. When the user enables the Watchdog Timer, the Watchdog Time-out configuration dialog will appear automatically for the user to configure its value. By default, the Watchdog Timer is disabled.
- **Watchdog Timeout Value**
Default value is two minutes. Its value range is from two minutes to 60 minutes.
- **Paging Configuration**
This command displays the paging Configuration dialog box. This configuration is not sensor specific; this is global to a server.
- **Restore Factory Defaults**
This command restores the sensor threshold values to its default values.

3.1.4 ICMB Menu

The ICMB Menu provides the following options:

- **View Managing Server**
This command enables the default local managing server view. The Navigation Pane and Presentation Pane are redrawn with information on the primary server. This is the same information displayed when PIC initialized.
- **View Managed Server(s)**
This submenu brings up the ICMB managed server view(s).
- **Reclaim Inactive Resources**
This command reclaims inactive ICMB resources.

3.1.5 Help Menu

The Help Menu displays detailed information about the procedures and the options to operate the PIC Console. This menu displays the following menu items:

- **Help Topics**
This command brings up the PIC help topics.
- **About PIC**
This command brings up the PIC version information.

3.2 Toolbar

The Toolbar is displayed on the main dialog directly under the Main Menu items. The Toolbar consists of five buttons described below. The Toolbar is displayed by default, but can be hidden by toggling the Toolbar option accessed under the Main Menu, View, Menu, and Toolbar. Right clicking with the mouse over the Toolbar and selecting the Hide menu option can also hide the Toolbar.



Figure 8 - 4: Toolbar

The Toolbar options can be described as follows:

Table 8 - 2: Toolbar Options

Icon	Command	Function
	Up One Level	This button brings the user up one level in the tree (navigation) view.
	Large Icons	This button displays list view items using large icons.
	Small Icons	This button displays list view items using small icons.
	List	This button displays list view items in list format.
	Details	This button displays list view items in detail format.

When the toolbar is hidden, the main dialog appears as follows:

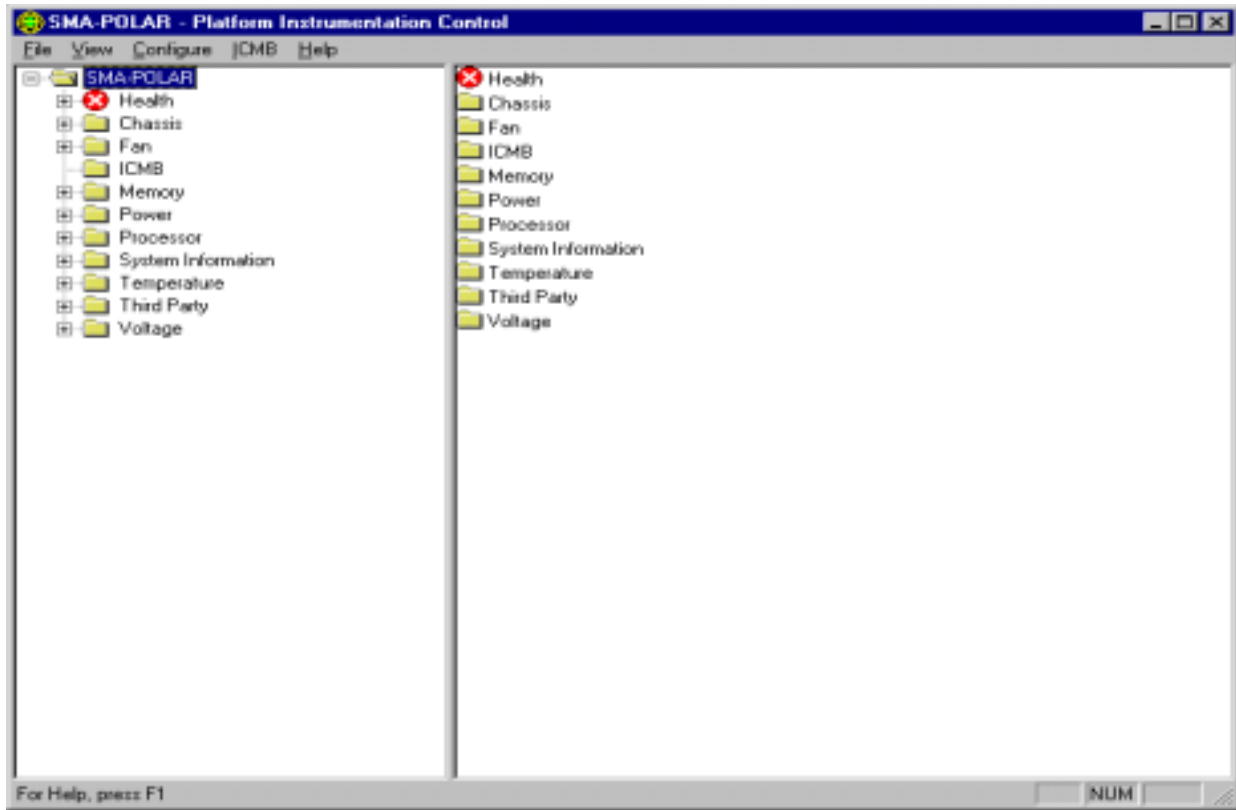


Figure 8 - 5: PIC Main Dialog, Toolbar Hidden

3.3 Navigation Pane

The Navigation Pane appears on the left side of the main dialog. It is used to organize the server information.

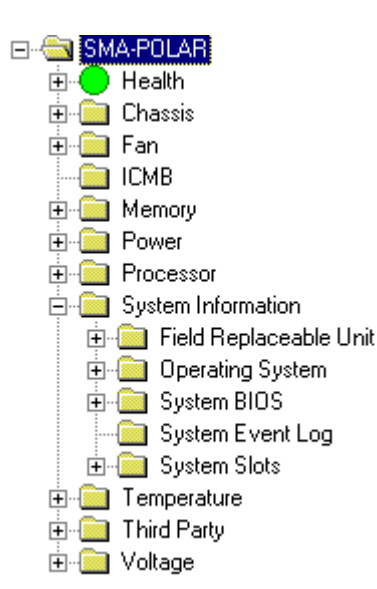




Figure 8 - 6: Navigation Pane

The Navigation Pane contains a tree view, which presents the server object hierarchy. The root of the tree is the server name or server IP address. Each “group” branch within the tree with a  symbol can be expanded to view additional tree information. Each “group branch with a  symbol can be collapsed to hide additional tree information. By default, the tree information is organized as follows:

- Health branch first
- Sensor group sorted alphabetically
- System Information groups sorted alphabetically within that branch

The tree view is also expanded by default to the group level.

3.3.1 Health

Health is always the first branch of the server tree. Health provides the user with a quick and simple view of the current server health. All unhealthy sensors (status not OK) will be collected and displayed under the Health branch. These sensors are the same sensors found in other branches of the Navigation tree. For example, an unhealthy 12-V sensor would be found under the Health branch and the Voltage branch of the tree.

Within the health branch, sensors are organized alphabetically. Colored icons in the Health branch of the server tree indicate individual sensor status and overall server status:

- **Green:** healthy server
- **Yellow:** non-critical conditions
- **Red:** critical failures
- **Blue:** unknown state or status

The color of the server health icon will display the state of the most severe sensor status. If any sensor is in a critical condition, the server health status will be shown as critical (red), even if other sensors are not in a critical state. If there are only non-critical sensors, the server health status will be shown as non-critical (yellow). Only if all sensors report normal conditions will the server health status be shown as OK (green).

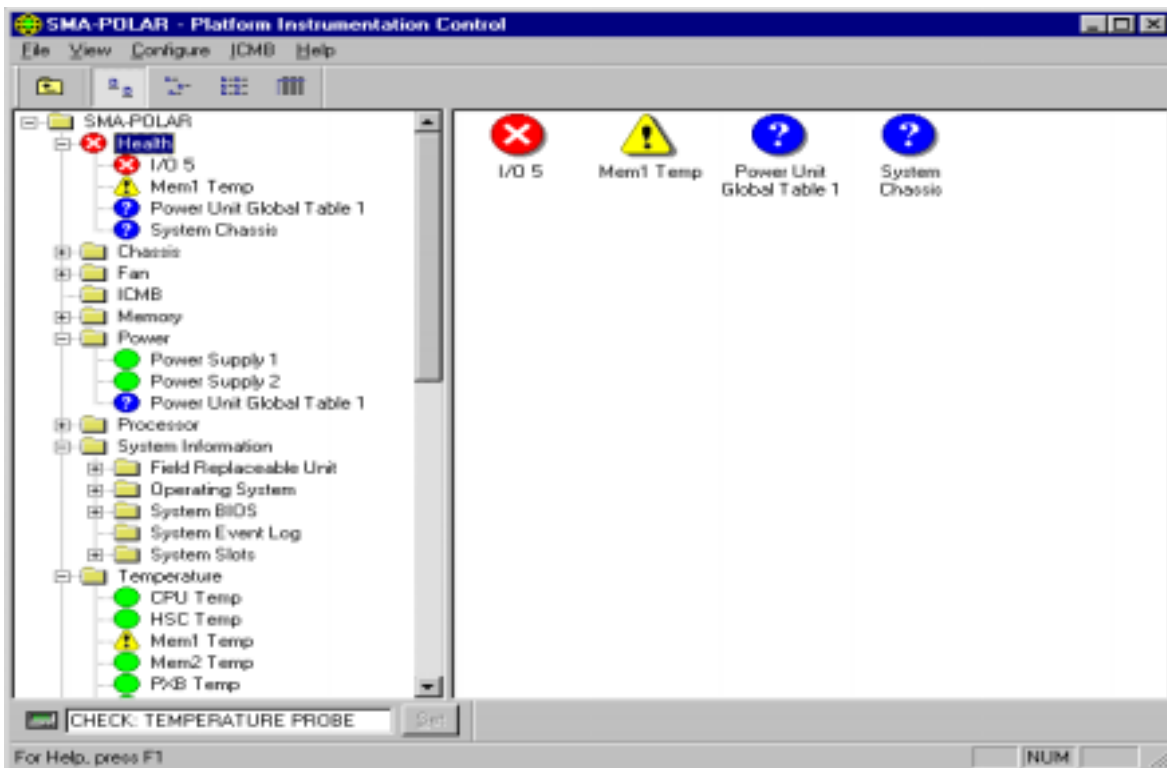


Figure 8 - 7: Health View in Main Dialog

3.4 Presentation Pane

The Presentation Pane appears on the right side of the main dialog. It is used to display server and sensor information for the sensor that is selected in the Navigation Pane.

3.4.1 Group Information

When browsing the tree in the Navigation Pane, information about groups – information related to a major heading, is displayed in the Presentation pane. An example of grouped information is if the user selects the major heading “Temperature” in the Navigation Pane, the available temperature sensors are displayed in the Presentation Pane.

3.4.1.1 Viewing Grouped Information – Icon Selection

Group information displayed in the Presentation Pane will appear in Large Icon, Small Icon, List or Detail view, depending on the View option selected from Main Menu / View. List View is the default view when the PIC GUI is initialized. See Figure 8 - 8, Figure 8 - 9, Figure 8 - 10, and Figure 8 - 11.

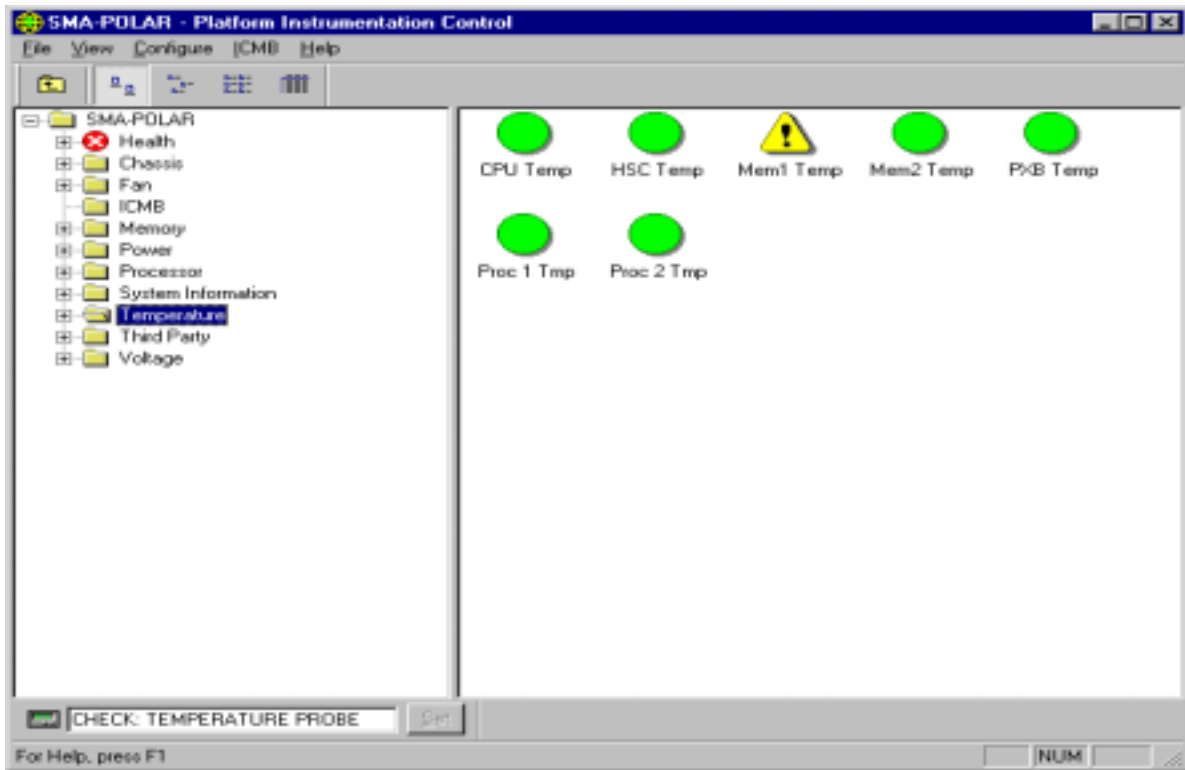


Figure 8 - 8: Presentation Pane, Large Icon View

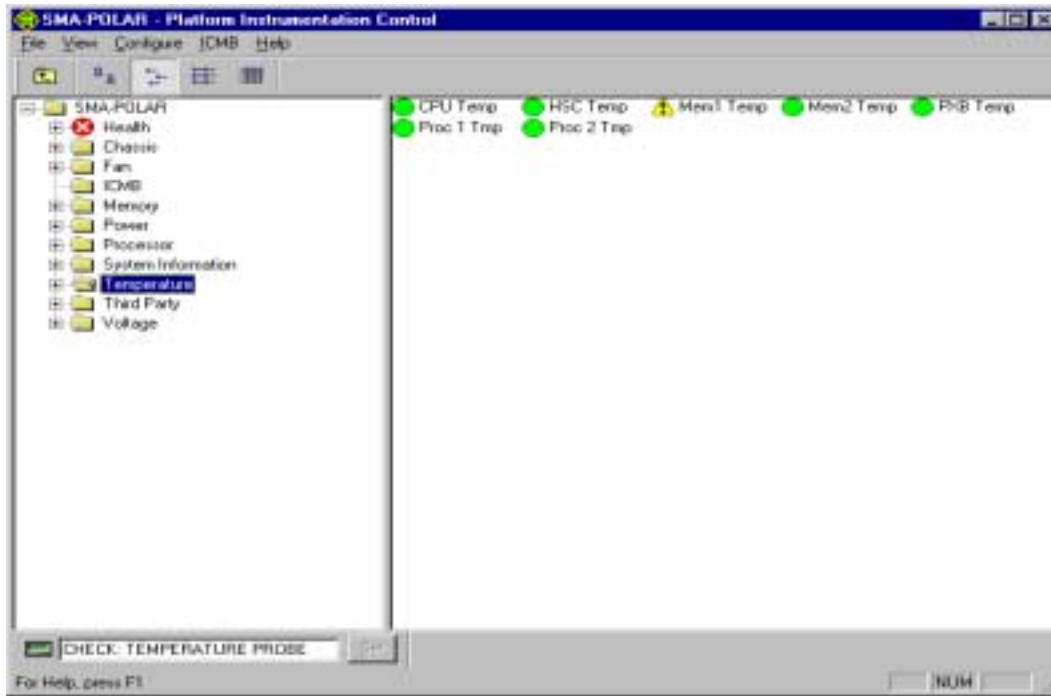


Figure 8 - 9: Presentation Pane, Small Icon View

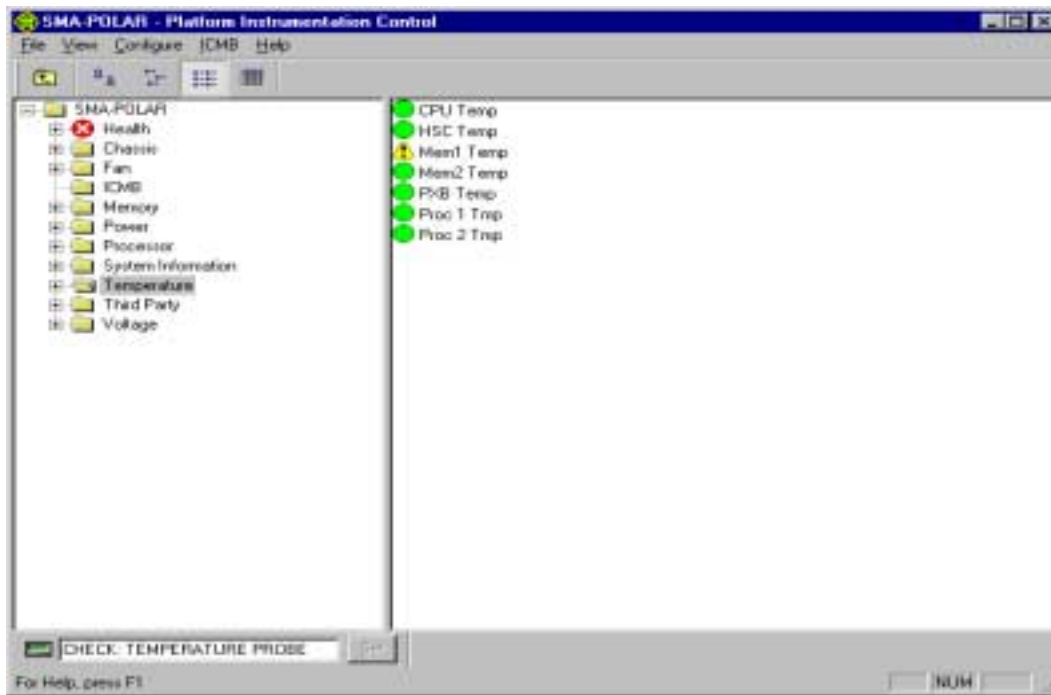


Figure 8 - 10: Presentation Pane, List View

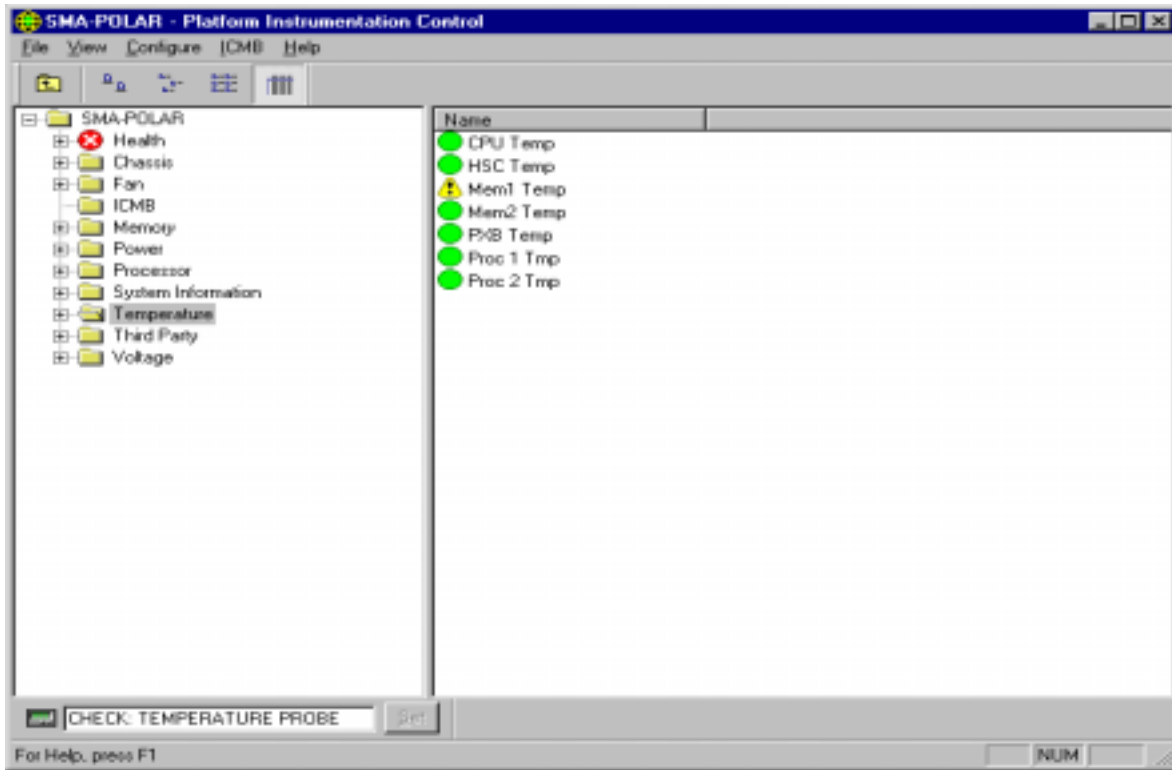


Figure 8 - 11: Presentation Pane, Detail View

3.4.1.2 Viewing Grouped Information – Name / Status Selection

Group information can also be arranged on the screen by name or by status, with the exception of Health views. Health is always arranged by status. The “Arrange by Name” and “Arrange by Status” options are available from the Main Menu / View.

“Arrange by Name” will sort the list of items alphabetically. “Arrange by Status” will sort these items by their status. The possible values of status are “Critical”, “Non-Critical”, and “OK”.

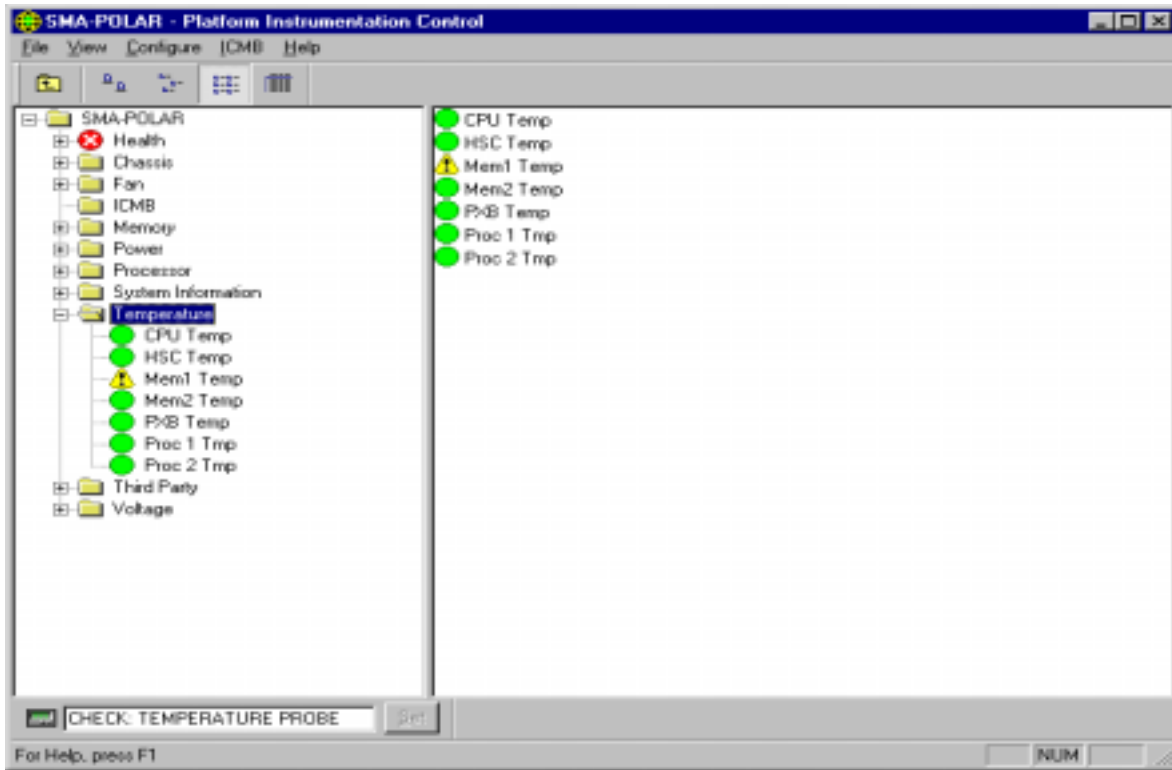


Figure 8 - 12: Arrange Icons by Name, List Icon View

When “Arrange by Status” is selected, the Navigation and Presentation Panes sort grouped sensor information by health status as follows: Critical sensors first, Non-critical sensors next, followed by Normal sensors. See Figure 8 - 13.

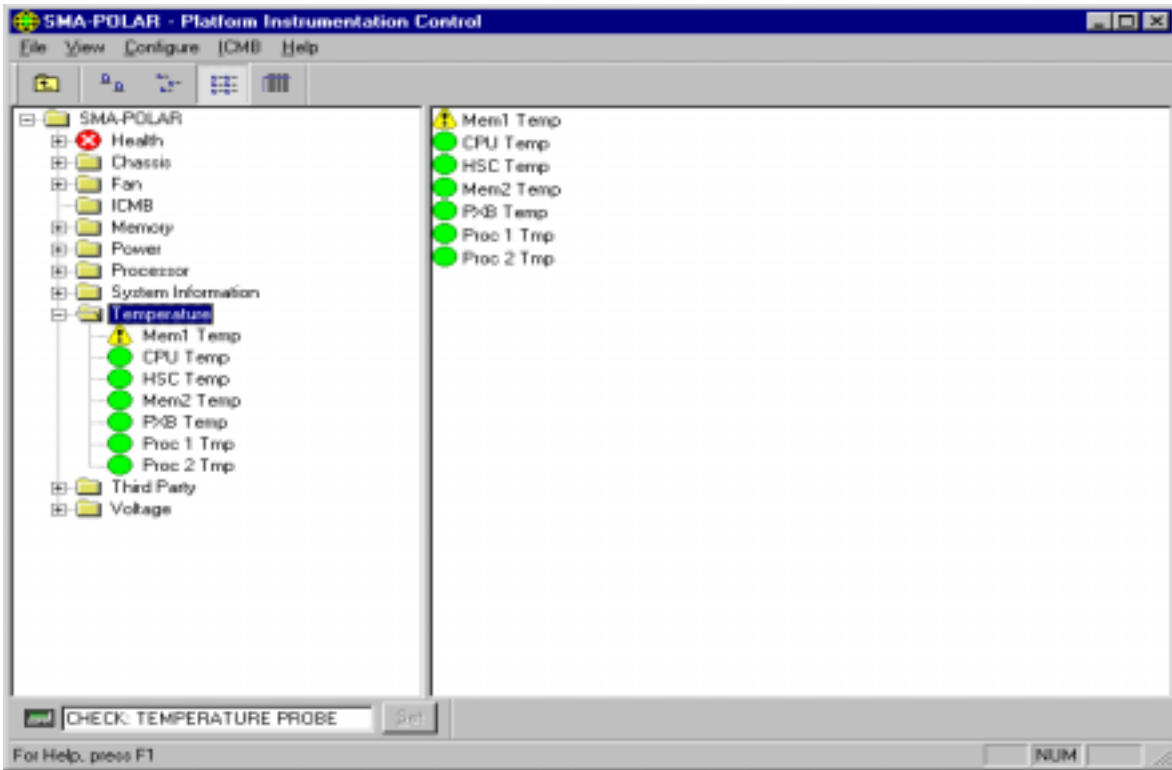


Figure 8 - 13: Arrange Icons by Status, List Icon View

3.5 LCD Display



Figure 8 - 14: LCD Display Pane

The LCD Display pane is displayed if the managed server supports an LCD. It may be seen at the bottom of the Navigation Pane, above the Status Bar. The LCD Display pane displays the server LCD contents. If the server hardware does not support an LCD, the corresponding LCD pane and will be disabled, as will the LCD Display option under Main Menu / View.

The LCD Display pane is displayed by default if the server supports an LCD. The pane can be hidden by toggling the LCD Display option accessed from Main Menu / View. Right clicking with the mouse over the LCD Display pane and selecting the Hide menu option can also hide it.

If the server does not support an LCD or the if LCD display is hidden, the main screen appears as follows:

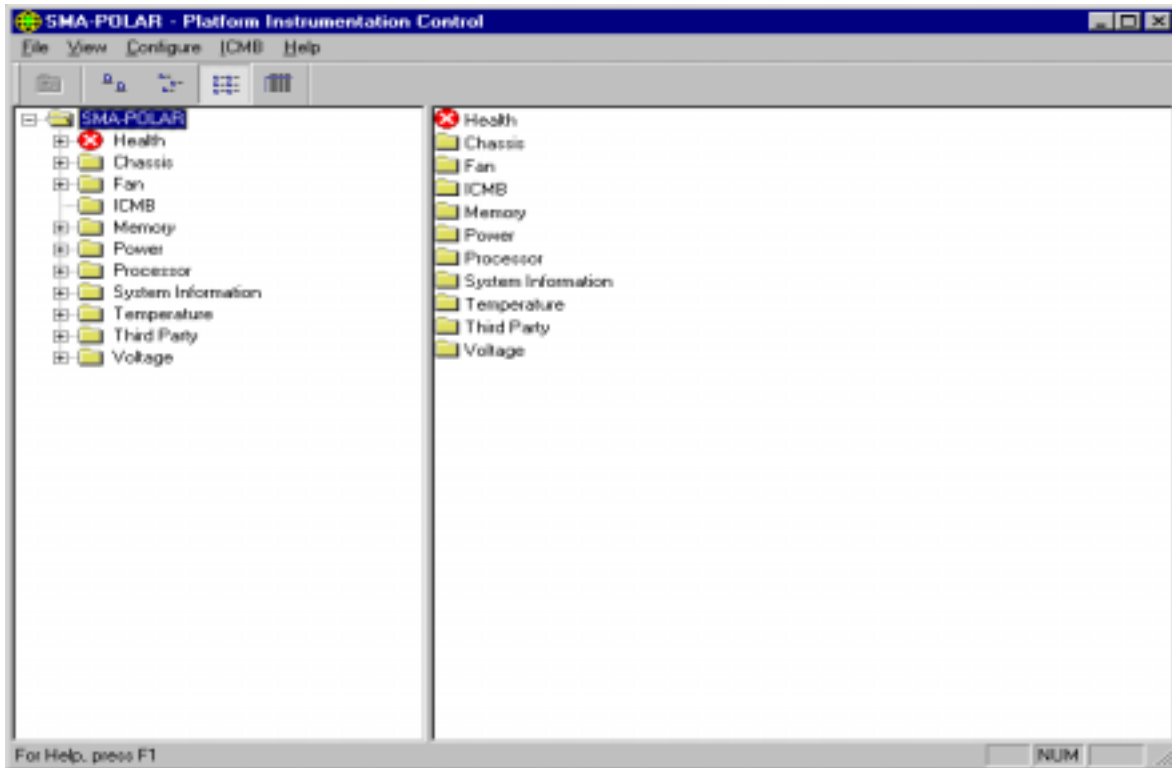


Figure 8 - 15: Managed Server without LCD, or LCD Hidden

3.6 Status Bar

Ready

Figure 8 - 16: Status Bar

The Status Bar is displayed at the bottom of the main screen and displays messages about system activity. The Status Bar is displayed by default, but can be hidden by toggling the Status Bar option, located under Main Menu / View. Right clicking with the mouse over the Status Bar and selecting the Hide menu option can also hide the Status Bar.

Initialization progress of the PIC GUI is visible in the status bar as multiple vertical bars that are displayed from left to right until initialization is complete. The status bar then changes to "Ready".

When the status bar is hidden, the main dialog appears as follows:

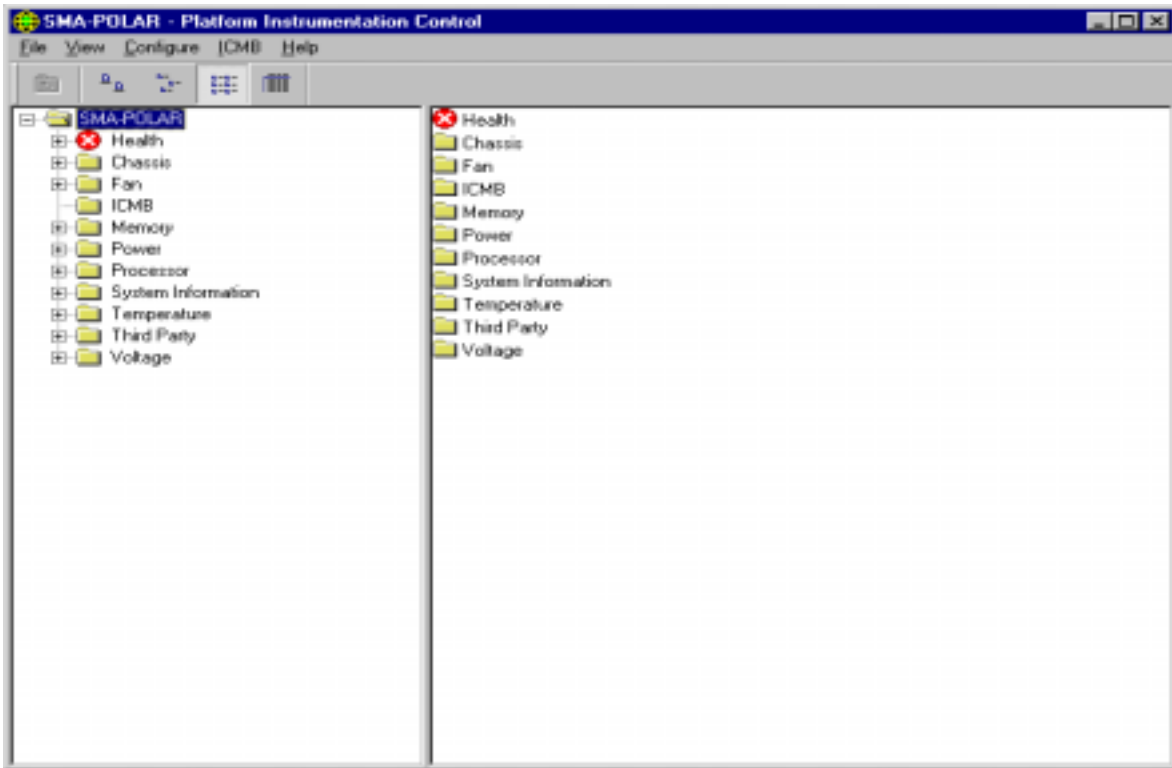


Figure 8 - 17: PIC Main Dialog, Status Bar Hidden

3.7 Popup Menus

Several popup menus are available within the PIC application. The sections below describe these popup menus in more detail.

3.7.1 Presentation Pane Popup Menu

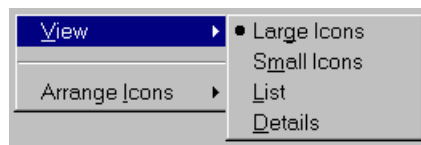


Figure 8 - 18: Presentation Pane Popup Menu

The Presentation Pane popup menu appears when the user right clicks in the Presentation Pane. The following options are available from this menu:

- **View**
View allows the user to change between large icons, small icons, list view, or detail view. This functionality is also available from Main Menu / View:

- **Arrange Icons**
Arrange Icons allows the user to arrange the list of item icons by name or by status. This functionality is also available from Main Menu / View.

3.7.2 Toolbar Popup Menu



Figure 8 - 19: Toolbar Popup Menu

The Toolbar popup menu appears when the user right clicks in the Toolbar. The **Hide** popup hides the toolbar. This functionality is also available from Main Menu / View.

Once hidden, the Toolbar can be restored by selecting the Toolbar option from Main Menu / View.

3.7.3 LCD Popup Menu

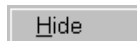


Figure 8 - 20: LCD Popup Menu

The LCD popup menu appears when the user right clicks on the LCD. The **Hide** popup hides the LCD display. This functionality is also available from Main Menu / View.

Once hidden, the LCD display can be restored by selecting the LCD Display option from Main Menu / View.

Note: The LCD options are only available on systems that support an LCD.

3.7.4 Status Bar Popup Menu

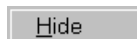


Figure 8 - 21: Status Bar Popup Menu

The Status Bar popup menu appears when the user right clicks on the Status Bar. The **Hide** popup hides the Status Bar. This functionality is also available from Main Menu / View.

Once hidden, the Status Bar can be restored by selecting the Status Bar option from Main Menu / View.

4. Individual Sensor / Server Information

When an individual sensor or server component is selected from the tree in the Navigation Pane, the data is displayed in one or more tab pages in the Presentation Pane.

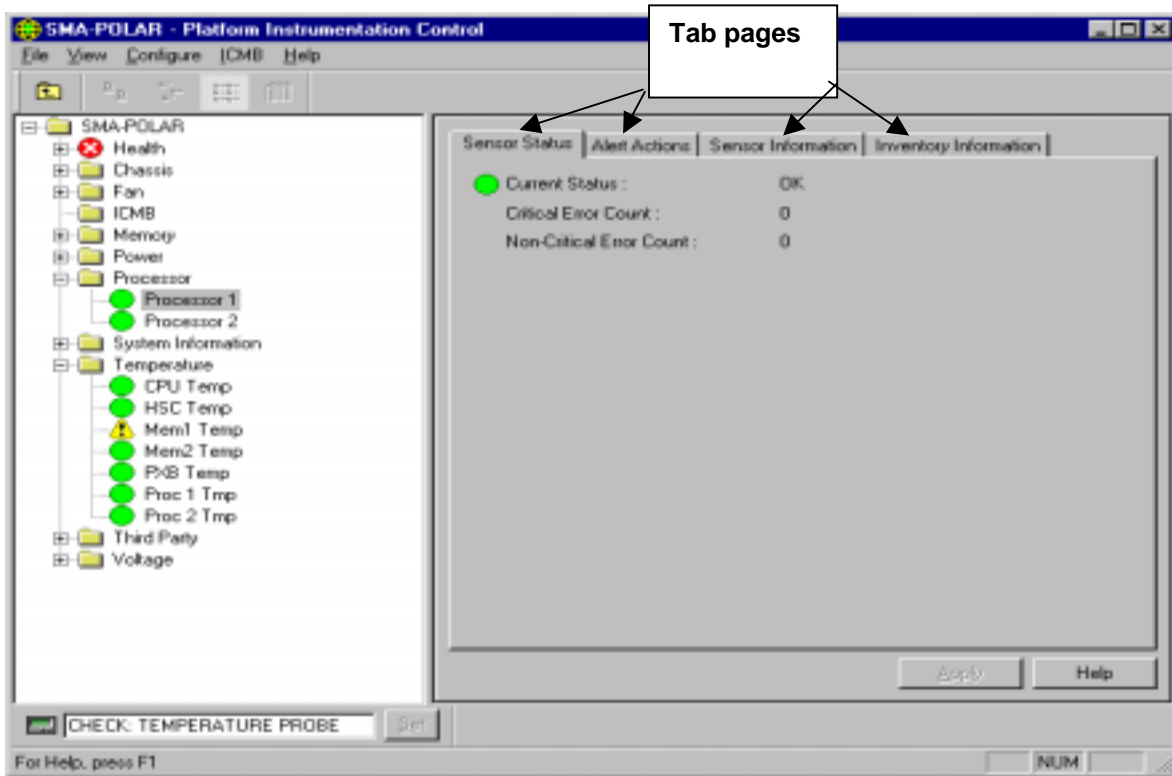


Figure 8 - 22: Tab Pages in Presentation Pane

For sensor objects selected in the Navigation Pane (e.g. Temperature, Fan, Voltage sensors), up to four tab pages are displayed:

- Sensor Settings or Sensor Status – displays health status, current readings, error counts and threshold values (if supported).
- Alert Actions – displays user configurable alert event actions. Includes audio/visual and power control actions. If LANDesk® Server Manager components are available on the managed console and server, then Alert Management System (AMS) events actions are also displayed.
- Sensor Information – displays static sensor information such as normal readings, tolerances, ranges, etc. **Note:** not all types of sensors support the Sensor Information tab page.
- Inventory Information – displays Field Replaceable Unit (FRU) information such as manufacturer, model, serial number, etc. **Note:** not all types of sensors support the Inventory Information tab page.

A user can change a threshold value and then switch between tab pages without pressing the Apply button to save the changes. The changes will be saved as long as the user presses Apply before selecting a different sensor. If the user attempts to select another sensor without pressing the Apply button, the user will be prompted to save the changes before PIC will display information about the newly selected sensor.

For server components, such as Operating System, System BIOS, and System Event Log, only one tab page is displayed. The data displayed is specific to the sensor component selected and the name of the tab page will match the component name.

The following sections provide an overview of the tab pages available.

4.1 Sensor Settings Tab Page

The Sensor Settings tab page displays the health of the sensor, the current value or state, any associated error counts, and lets the user modify any supported threshold values for that sensor. The Sensor Settings tab page is the default tab page displayed in the Presentation Pane for sensors that support this feature. The Sensor Settings tab page is displayed for the following sensor types:

- Fan
- Temperature
- Voltage

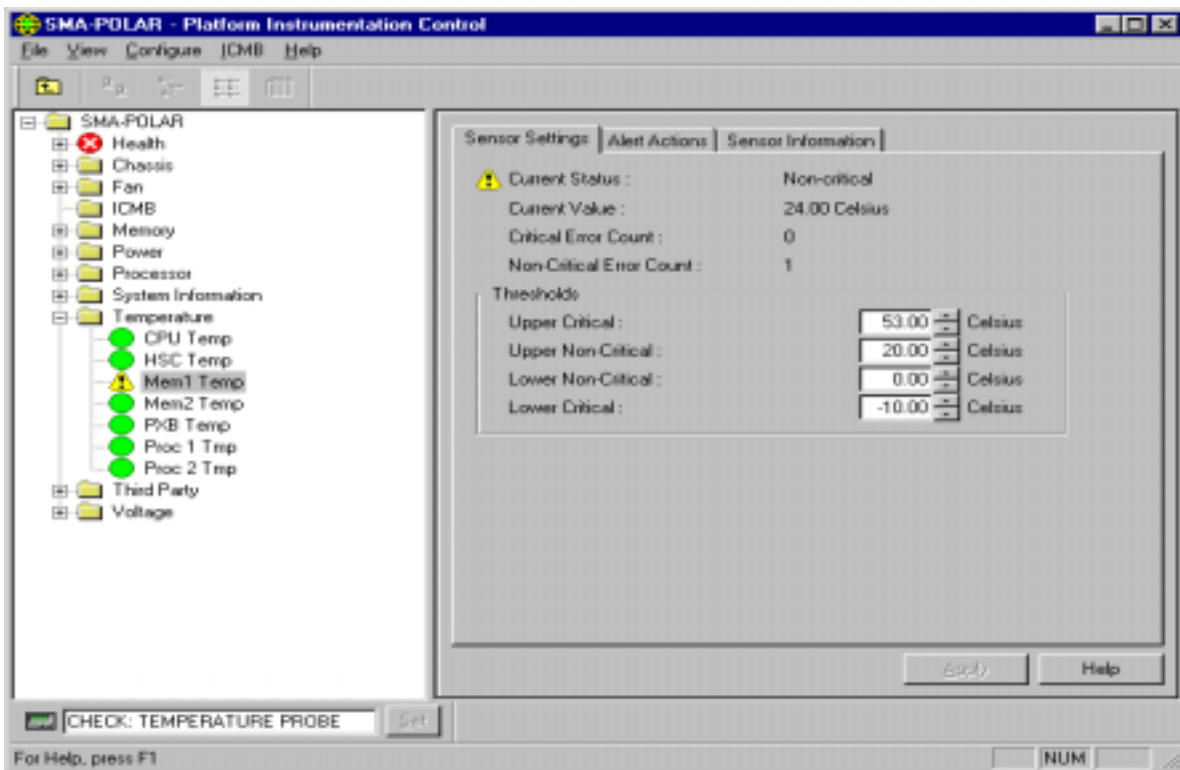


Figure 8 - 23: Sensor Settings Tab Page

Depending on the individual sensor displayed, some thresholds may be unsupported and appear as disabled (grayed out) in the control. The status bitmap on the upper left corner of the tab page provides a graphical view of the current sensor status. A red circle with a white X means “Critical”, a yellow caution sign means “Non-Critical”, a green circle means “OK”, and a blue question mark means “Unknown”.

The Apply button is enabled when a threshold value has been changed. PIC validates user entries for threshold values once the Apply button is pressed. Threshold values must conform to the following rule: $MIN \leq \text{Lower Critical} \leq \text{Lower Non Critical} < \text{Upper Non Critical} \leq \text{Upper Critical} \leq MAX$. For each sensor, there are minimum (MIN) and a maximum (MAX) threshold values. If a sensor does not have a MIN or a MAX value defined, MIN and MAX is taken as the range of a machine integer (which may vary from one server to another).

For Temperature sensors, the display unit can be changed from Celsius to Fahrenheit by using the Main Menu / View / Options.

Error counts on the Sensor Settings tab page are read-only fields. Users cannot modify them through PIC.

4.1.1 Threshold Values Rounded Off

When setting thresholds, the values entered might not be the exact values set by the software. Hardware rounding causes this behavior. The user must redisplay the Sensor Settings tab page to find the actual value set by the software.

4.1.2 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 the user changes a threshold value or an alert action in PIC, s/he can create an environment in which an event is immediately generated. An example is setting the Upper Non-critical 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 is valid immediately in the active instrumentation, but PIC waits five minutes before writing user changes to disk.
2. If the change causes the server to reboot, the previous value is restored from disk when the server reboots. PIC then uses and displays the previous value, thus avoiding the immediate reboot-fail-reboot-fail cycle.

Any change made will be successfully written to disk as long as the baseboard instrumentation continues running for five minutes after the change is saved.

4.2 Sensor Status Tab Page

The Sensor Status tab page displays the health of the sensor, the current value or state, and any associated error counts. The Sensor Status tab page is displayed for the following sensor types:

- Chassis
- Memory Array
- Memory Device
- Power Supply
- Power Unit
- Processor
- System Slots

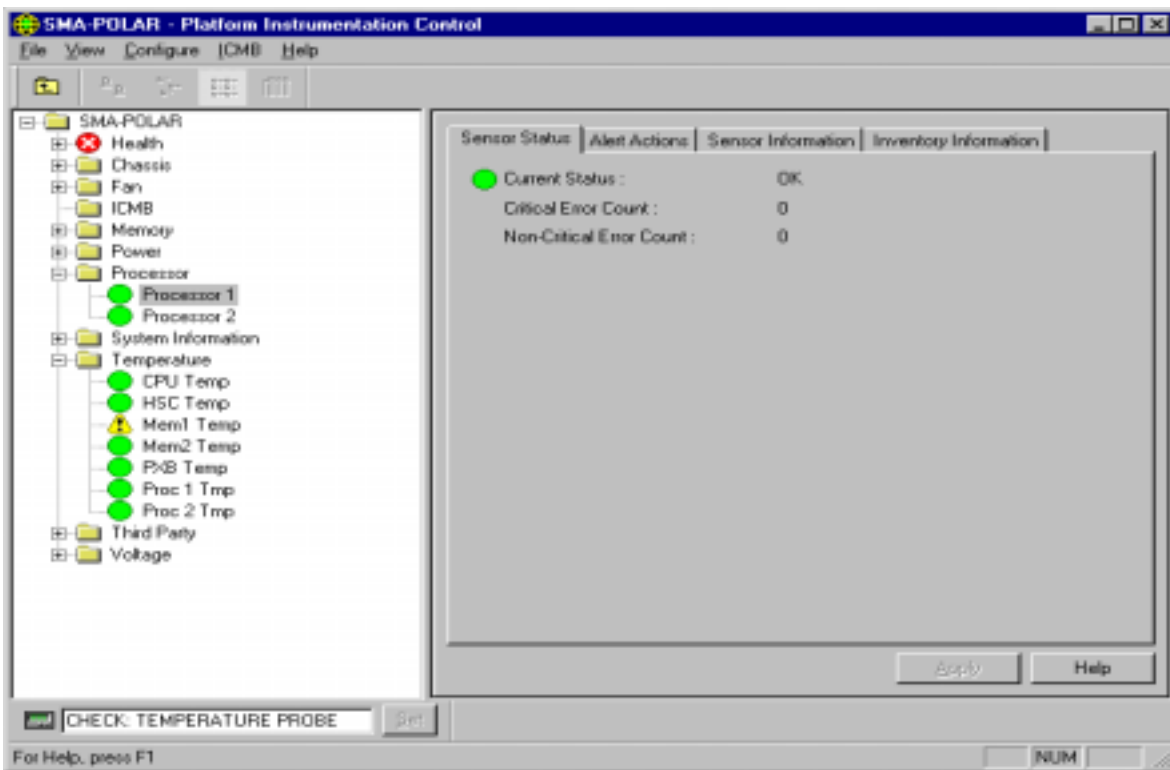


Figure 8 - 24: Sensor Status Tab Page

4.3 Alert Actions Tab Page

On the Alert Actions tab page, users can select actions that will take place when a sensor exceeds a threshold or changes state. Several options exist.

Local actions:

- Audio/visual notifications (more than one may be selected)
- Shutdown/power control actions (more than one may be selected)

Network actions:

- AMS2 actions (if LANDesk Server Manager is installed on the server and console).

Generally, audio/visual notifications and AMS2 alerts are for non-critical thresholds. Shutdown and power control actions are for critical thresholds. The Alert Actions tab page is displayed for the following sensor types:

- Chassis
- Fan
- Memory Array
- Power Supply
- Power Unit
- Processor
- System Slots
- Temperature
- Third Party Instrumentation
- Voltage

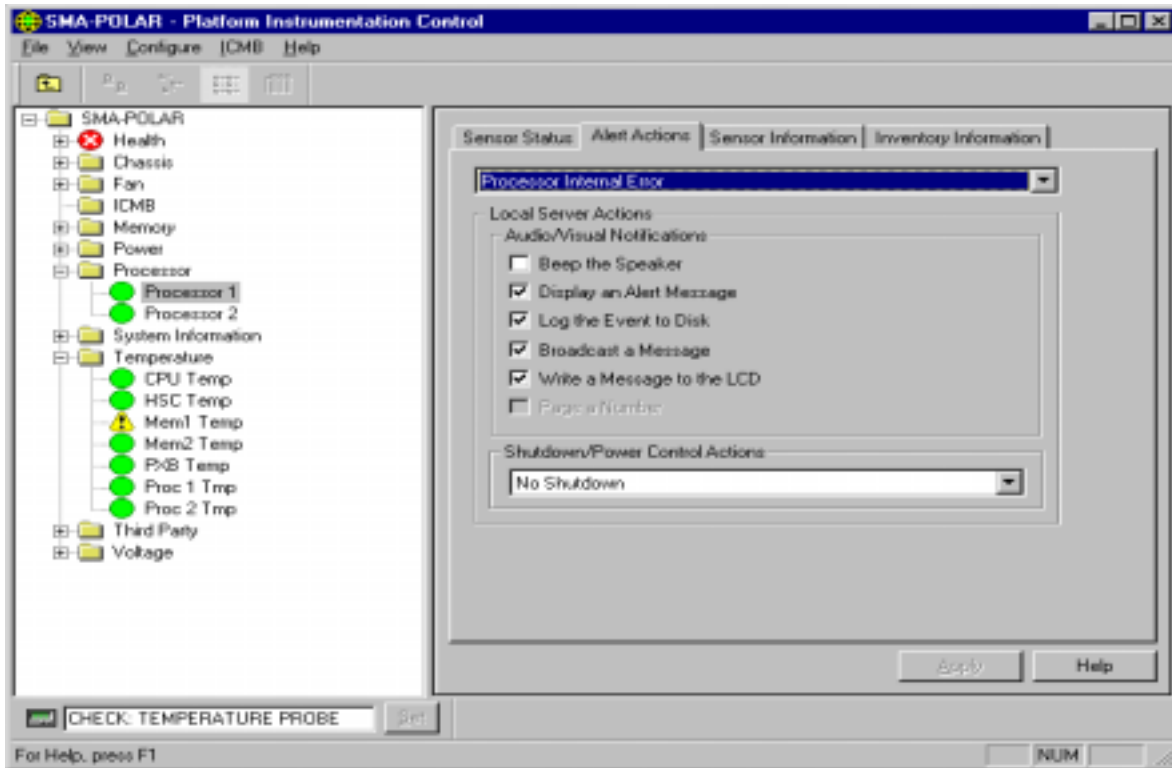


Figure 8 - 25: Alert Actions Tab Page

For more information on AMS2 and its alert actions, see “Configuring AMS2 Alert Actions” in the Intel LANDesk Server Manager Administrator’s Guide.

CAUTION: If the OS is disabled by a non-critical event action (such as configuring an OS shutdown action for a voltage surge), then 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 user configurable actions are defined in the tables below.

Table 8 - 3: Audio and Visual Notifications

Action	Description
Emit a beep from the managed server's speaker	Speaker emits a beep.
Display an alert message on the managed server	Default action for non-critical and critical indications. The message box stays up until acknowledged. On UnixWare and Solaris, the alert message is displayed as a text message on the server console.
Log the event to disk	Default action for all indications. This option records the event in the standard system error log. On NetWare, ISC records the event in the System Log, which you can view with NetWare's Syscon utility. On Windows NT, ISC records the event in the System Event Log, which you can view with the Windows NT Event Viewer. On UnixWare, events are logged in the system log file: /etc/osm. On Solaris the messages are logged to /var/adm/messages.
Broadcast a message	Default action for critical indications. On NetWare, the message goes to all users currently logged into the managed server with Administrator or Supervisor privileges. On Windows NT, the message goes to all the users currently logged into the managed server. Note: Windows 95/98 cannot receive network broadcast messages from Windows NT. If you configure a broadcast message and it is triggered on a Windows NT server, the message will not be received by any Windows 95/98 systems. On UnixWare and Solaris, a text message is sent to all users currently logged onto the UNIX server.
Write a message to the managed server's LCD	Default action for all indications. If the LCD is not available on the managed server, this option is grayed out and disabled.
Page a Number	A page is sent to a specified pager, with the telephone number of the server, an ID number, or other numerical information.

Table 8 - 4: Shutdown and Power Control Actions

Action	Description
No shutdown	Default action for all indications. Select this option if you do not want to shutdown or reset the server when an event occurs.
Shutdown the OS	The user should select this option to shut down the OS gracefully (controlled, closing files and applications). On NetWare, the server is returned to DOS. On Windows NT, the server is set to a state ready for manual power-off or reset. On UnixWare and Solaris, standard shutdown is completed and system prompts for reboot or power off.
Shutdown the OS and power off	The user should select this option to shutdown the OS gracefully and turn off the system power.
Shutdown the OS and hardware reset	The user should select this option to shutdown the OS gracefully and reset the server via hardware.
Immediate power off	The user should select this option 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	The user should select this option 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	The user should select this option to cause a hardware Non-Maskable Interrupt (NMI). If this feature is not supported on the managed server, this option is disabled / grayed out .

4.3.1 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. This can occur in the following scenario:

1. An event occurs. Example: a high-temperature threshold is exceeded.
2. While the condition causing the event still exists, the user sets 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 the user reboots the system and the event condition has not been corrected (in this example, the temperature is still over threshold), the system detects the temperature condition, triggers the event, and the corresponding action is taken. In this example action, Immediate Power Off, the system is automatically and immediately powered off.

When the system is powered up, an infinite loop of power-up and power-down begins. To break this cycle, the user has two options:

1. Clear the event condition (cool down the system in this example).
2. 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 will disable the software component that responds to the event. The contents of the file are not important. Booting DOS can create this file. The user must then delete this file after the problem is fixed to allow the software to operate normally. On UnixWare* systems, the user either creates a LRA.NOT file in the root directory or uses the diskette described above.

4.4 Sensor Information Tab Page

The Sensor Information tab page displays static sensor information such as normal readings, tolerances, ranges, etc. for the sensor. The values displayed in the Sensor Information tab page are read-only, and the user cannot modify them through PIC. The Sensor Information tab page is displayed for the following sensor types:

- Fan
- Memory Array
- Memory Device
- PCI Hot Plug Device
- Power Supply
- Processor
- System Slots
- Temperature
- Voltage

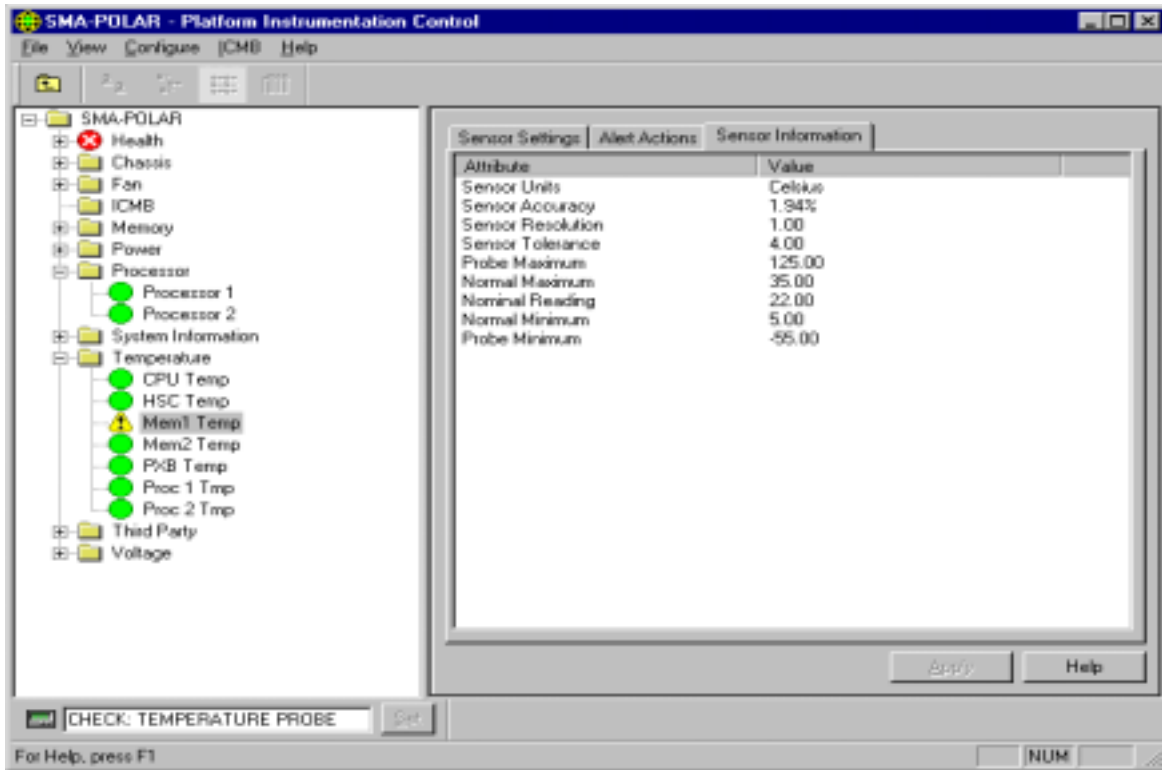


Figure 8 - 26: Sensor Information Tab Page

Note: For Temperature sensors, the display unit is either degrees Celsius or degrees Fahrenheit. For Voltage sensors, the display unit is Volts.

4.5 Inventory Information Tab Page

The Inventory Information tab page displays Field Replaceable Unit (FRU) information such as manufacturer, model, serial number, etc. for the sensor. The values displayed in the Inventory Information tab page are read-only, and you cannot modify them through PIC. The Inventory Information tab page is displayed for the following sensor types:

- Chassis
- Field Replaceable Unit
- Memory Array
- Processor

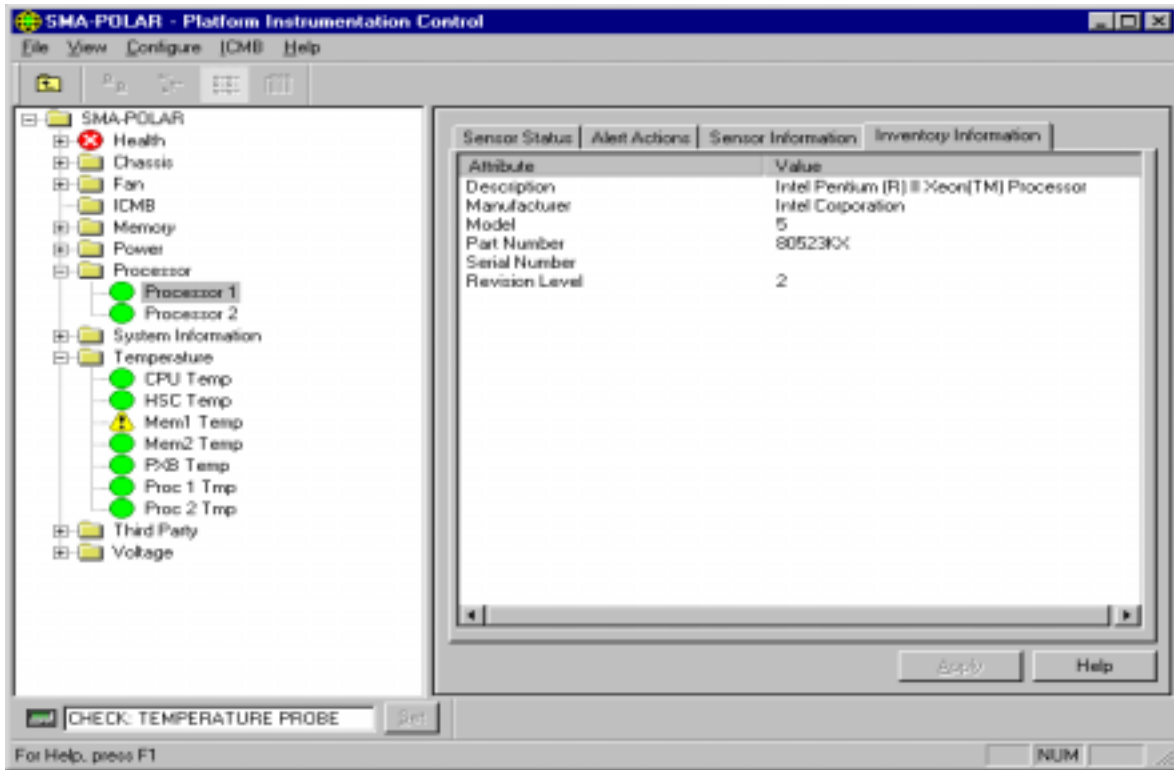


Figure 8 - 27: Inventory Information Tab Page

5. PIC Dialogs

From the Main Menu, users can display several customization/configuration dialogs or perform several different tasks while managing the server.

5.1 Options Dialog

The Options dialog is available from the Main Menu / View / Options menu selection.

PIC has several configurable options. The user can set the PIC console refresh rate, thus determining how frequently PIC is updated with current information for those sensors or servers where information is gathered through polling. The user can also enable or disable polling entirely and specify whether the temperature values display in degrees Celsius or degrees Fahrenheit.

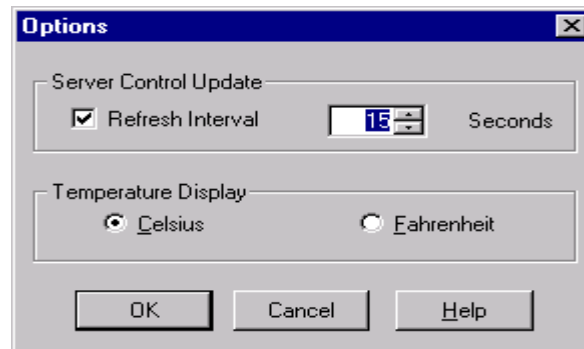


Figure 8 - 28: Options Dialog

PIC installs with the following defaults:

- PIC console refresh interval: 15 seconds
- Temperature display format: Celsius
- Watchdog feature: Off
- Watchdog timer: Two minutes
- Sensor threshold values as defined in the Sensor Data Records (SDR) file

The user should be aware when configuring the console refresh interval that a frequent refresh interval will impact system performance on both the console and the managed server. This is because on some servers PIC 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 the rate at which the server system responds to event notifications (e.g., threshold crossings), only how quickly PIC displays updates with server information. A value of 15 seconds or greater for console refresh value provides a reasonable compromise.

5.2 Restoring Factory Defaults Dialog

To restore default PIC settings for threshold values, console refresh interval, and the watchdog feature the following steps should be used:

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

Note: Event actions that have been configured and the temperature display format are not affected by the Restore Factory Default option.

Default threshold values are stored in SDR in nonvolatile storage on the server board. These values are determined and configured during manufacturing and are therefore not documented in this manual.

CAUTION: Indications may be generated if the restoration of 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 the user selects the Restore Default Settings action, threshold restore may cause a threshold crossing. In the above example, PIC would detect a threshold crossing and generate an indication. The actions associated with that indication would occur.

To avoid the possibility of unwanted indications when restoring default settings, Intel recommends the following: For each sensor where indications are not wanted, the user should adjust the user-defined threshold value. The current sensor value should NOT be between the user-defined threshold value and the default threshold value. Once this adjustment is made, the user can select the Restore Default Settings action.

5.3 Watchdog Timer Dialog

Each motherboard supported by PIC has a watchdog timer implemented in the hardware. This 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 PIC server instrumentation software will periodically reset the timer so it will not reach a value of zero. If the OS hangs, the timer will count down to zero.

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

The Watchdog Timer dialog is available from the Main Menu / Configure / Watchdog Timeout Value menu selection.

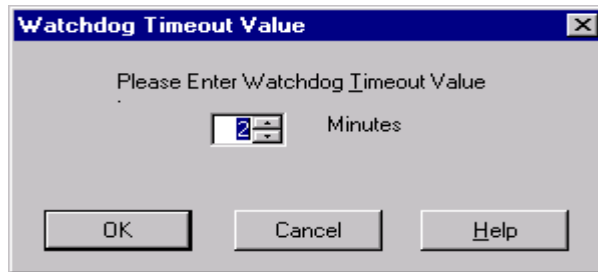


Figure 8 - 29: PIC Watchdog Timer Dialog

5.4 Paging Configuration Dialog

Sending a page is an alert action that can be configured for any sensor event if paging is supported on the managed server. The paging function is implemented by the Baseboard Management Controller (BMC) and uses a modem on the managed server. Although PIC supports paging as an event action, PIC does not provide a user interface to configure the system modem. PIC does provide a dialog to configure the pager number, repeat counts and other items relevant to the paging event action. This paging configuration is global to the server and is therefore not sensor specific.

The Paging Configuration dialog is available from the Main Menu / Configure / Paging Configuration menu selection. If paging is not supported on the managed server, this menu option will be grayed out.

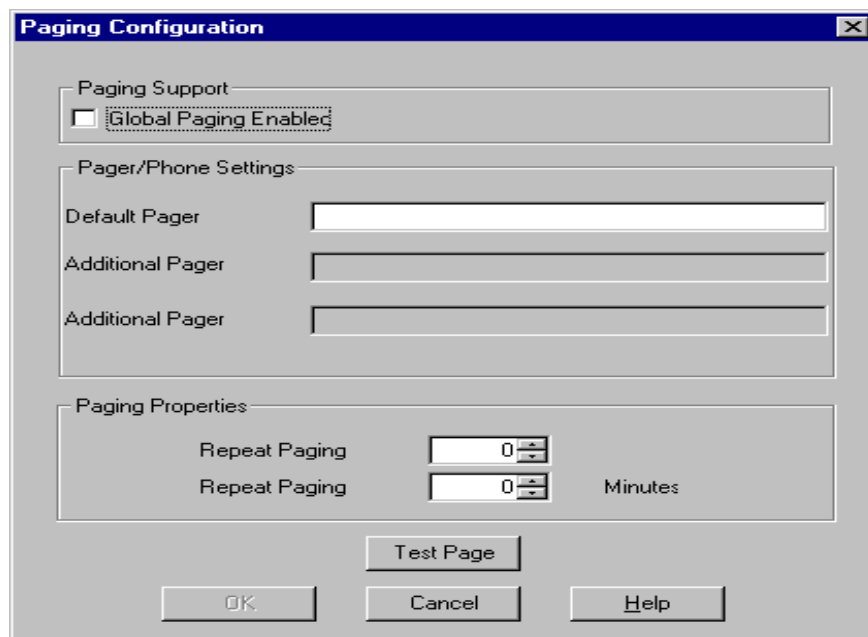


Figure 8 - 30: Paging Configuration

The Paging Configuration dialog allows the user to configure the following paging information :

- **Paging Support** — The Global Paging Enabled check box allows the user to enable or disable paging as a configurable event action for all PIC sensors. By default, global paging is enabled in PIC unless paging has been disabled on the managed server through the BMC. If global paging is enabled, then the user can configure paging as an event action for individual sensor events on the Alert Actions tab page.
- **Pager/Phone Settings** — The Default Pager Number is the default number used to issue any page request. The Additional Pager Numbers, if configured, will also be used for any paging event. These are free format edit fields. The user must enter the full pager number the way it would be dialed including:
 - Modem dial commands
 - Paging service phone number, including initial numbers to access an outside dial tone for inter-company dialing
 - Paging service passcode (if required)
 - System Identification Number
 - Termination characters

For example, the page string might be: ATDT18005551234,123456#,5031234567#

This includes, in order of appearance:

- Modem dial command
- Paging service phone number
- Pause (,)
- Passcode
- Pause (,)
- System identification phone number
- Closing # sign

Since the pager number information may vary on many factors (e.g. modem commands, service number, inter-company, local call, long distance call, international call, etc.), PIC does not provide any validation on the user input. The Test Page function should be used to validate the information entered.

Note: The Test Page function is supported only for the default pager number.

- **Paging Properties** — The Repeat Paging feature allows administrators to be notified multiple times for any paging event. The user can configure the number of times and at what frequently a page is generated. If more than one pager number is configured, then each pager number will be contacted the specified number of times. The paging interval is the time between when the pagers were last contacted and when the page is re-issued.

The default paging count is one with a maximum value of three. The default paging interval is ten minutes, with a maximum value of sixty minutes.

- Test Page — Allows the user to generate and validate a page request based on the Default Pager information. **Note:** This feature is not supported for the Additional Pager information.

5.5 ICMB Configuration Dialog

The Intelligent Chassis Management Bus (ICMB) dialog allows the user to configure ICMB options. The ICMB feature allows multiple remote devices to be interconnected and management information shared among them. For example, a managed server could be configured to be an ICMB primary server and report management information on other ICMB devices connected to it. With ICMB, PIC can manage the power state of remote ICMB devices, and view the SEL and FRU information about those devices.

Through the PIC software, the user can switch the 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. The user can also change the view back to the primary server or any other ICMB-managed device at any time.

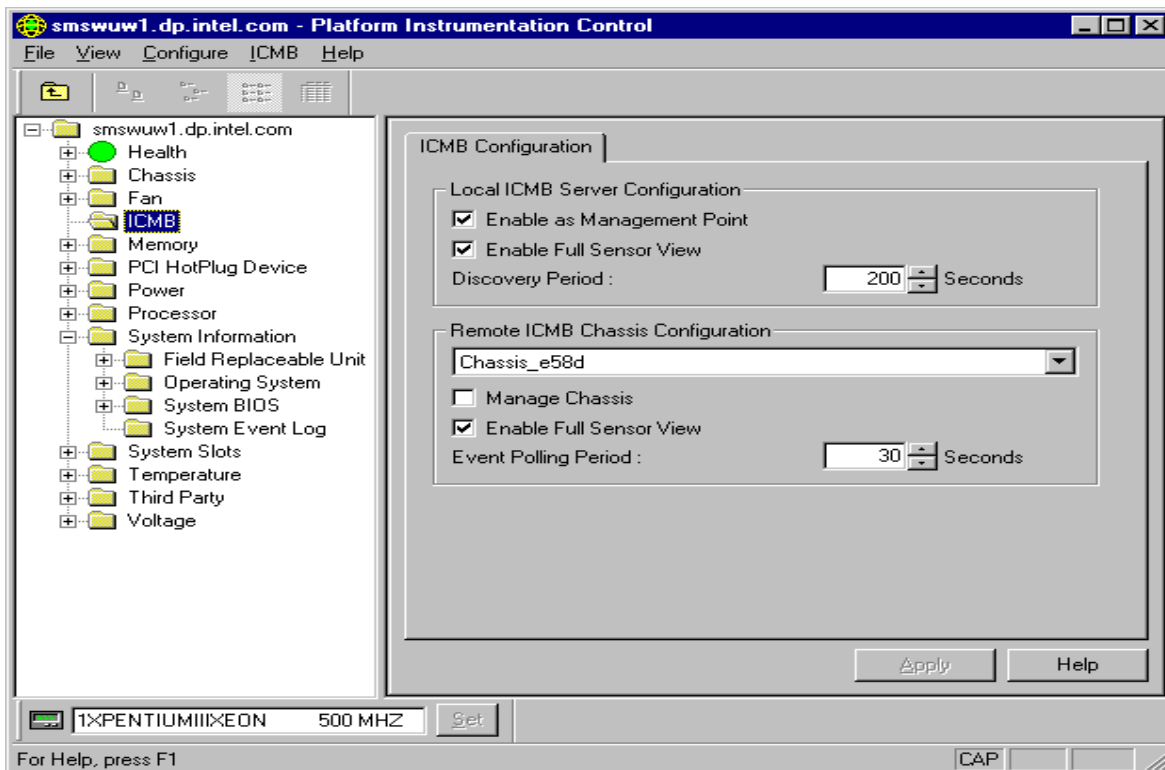


Figure 8 - 31: ICMB Configuration Dialog

Through the PIC software, the user can configure the ICMB management features of the primary managed server and the remote ICMB managed devices. An ICMB dialog let user configure local and remote ICMB servers as follows:

- Local ICMB Server Configuration — With this option it is possible to 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 it is possible to configure each remote device discovered via ICMB. The user can decide whether to manage the remote device, enable full sensor view for the remote device, and set the event-polling rate for the remote device.

5.6 ICMB Remote Server(s) Dialog

Once the primary server has been configured to be the management point via ICMB, the user can switch the PIC view from the primary managed server to one of the ICMB managed servers.

The ICMB Remote Server(s) dialog is available from the Main Menu / ICMB / View Managed Server(s) menu selection. If ICMB is not enabled on the managed server, this menu option will be grayed out.

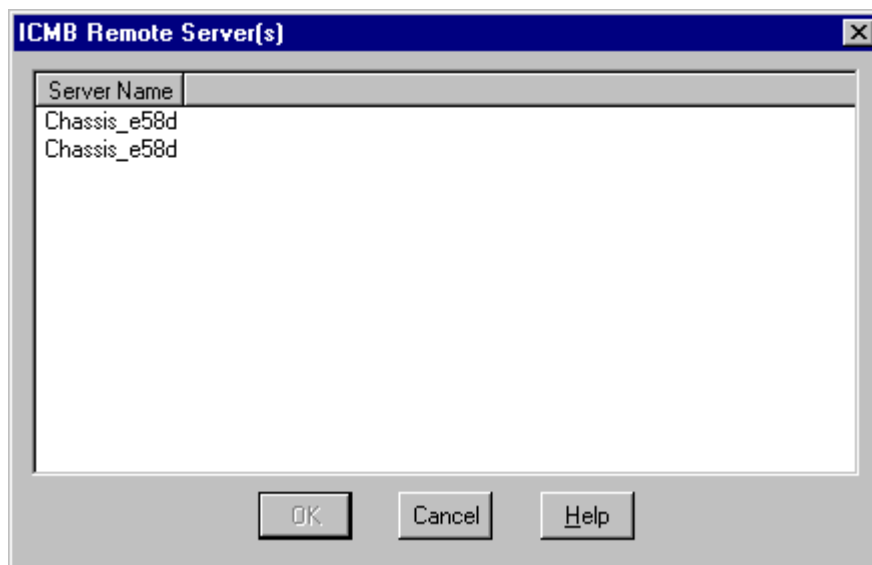


Figure 8 - 32: ICMB Remote Server(s) Selection Dialog

This dialog will display a list of all the servers currently being managed via ICMB. The user can change the PIC view to one of the ICMB managed servers by double-clicking on the server name or by selecting the name and pressing the OK button.

When an ICMB managed server is selected, the PIC main dialog is redrawn with the selected server information. The available information via ICMB is a subset of the information available when managing the server directly via PIC. Through ICMB, the following server information is available:

- Health Information
- Chassis Information
- Field Replaceable Unit (FRU) Information
- System Event Log (SEL)

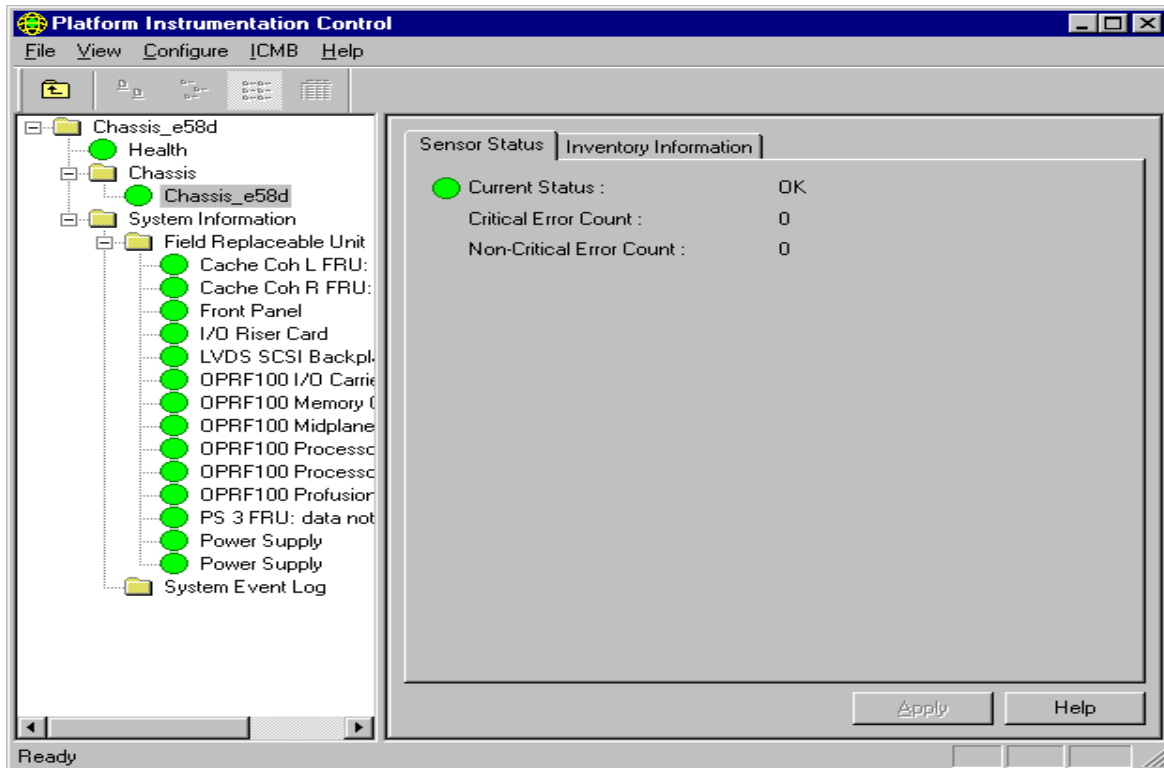


Figure 8 - 33: PIC Main Dialog, Managing a Remote Server via ICMB

The user can switch between ICMB managed servers and the primary managed server using the Main Menu / ICMB / View Managing Server and the Main Menu / ICMB / View Managed Server(s) menu selections.

6. Sensor Controls

The sensor controls are ActiveX* controls that plug into the PIC container in the Presentation Pane.

Each sensor has one or more tab pages representing the sensor information. The Sensor Settings, Sensor Status or Sensor Information tab pages vary based on the type of sensor or information displayed. The Sensor Settings and Sensor Status tab pages have the most variances for the following reasons:

- Some sensors include only critical error counts, not non-critical
- Some sensors support only one threshold value
- Some sensors support two threshold values
- Some sensors support all four threshold values
- Some sensors have non-editable threshold values
- Some sensors have Range-based thresholds for which a variety of values can be set. Example uses: for temperatures, voltages, and RPM-sensing fans.
- Some sensors have State-based thresholds that have fixed values like OK, Critical, Secure, Redundant. Example uses: for rotation-sensing fan, chassis door, and power unit.

Note: The number of sensors and sensor types vary based on the managed server type.

The user can see individual sensor information in the Presentation Pane by selecting the corresponding sensor node from the navigation tree.

6.1 Chassis

The Chassis control displays intrusion and inventory information for the system chassis on the managed server. For chassis sensors, three tab pages are available in the Presentation Pane:

- Sensor Status
- Alert Actions
- Inventory Information.

Note: Not all servers support the Chassis sensors.

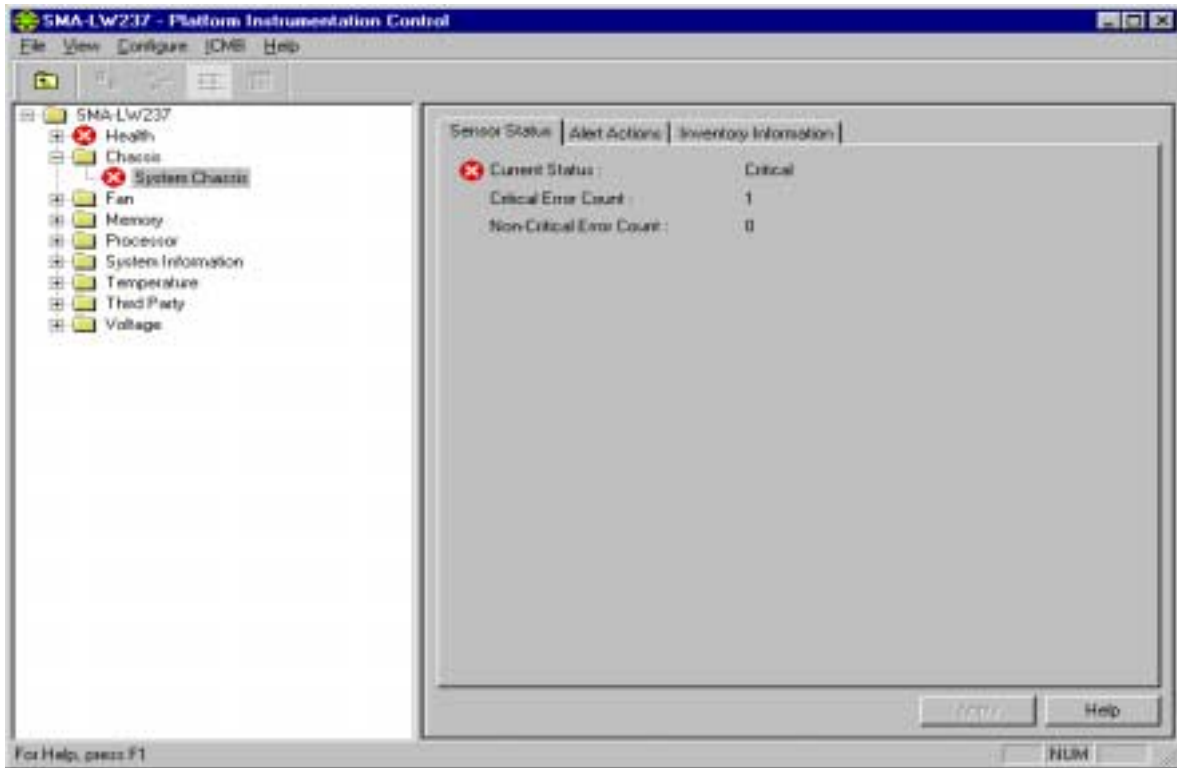


Figure 8 - 34: Chassis Sensor Status

On the Sensor Status tab page, the Current Status can have the following values:

- OK
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following state changes:

- Chassis Vulnerable
- Chassis Secured

The Sensor Information tab page displays the following chassis sensor attributes:

- Description – A description of this chassis.
- Manufacturer – The name of the company manufacturing or providing this chassis.
- Model – The manufacturer's model number for this chassis.
- Part Number – A part number by which a replacement part can be ordered.
- Serial Number – The manufacturer's serial number for this chassis.
- Revision Level – The revision level of this chassis.

6.2 Fan

The Fan control displays information for all fan sensors on the managed server. For fan sensors, three tab pages are available in the Presentation Pane:

- Sensor Settings
- Alert Actions
- Sensor Information.

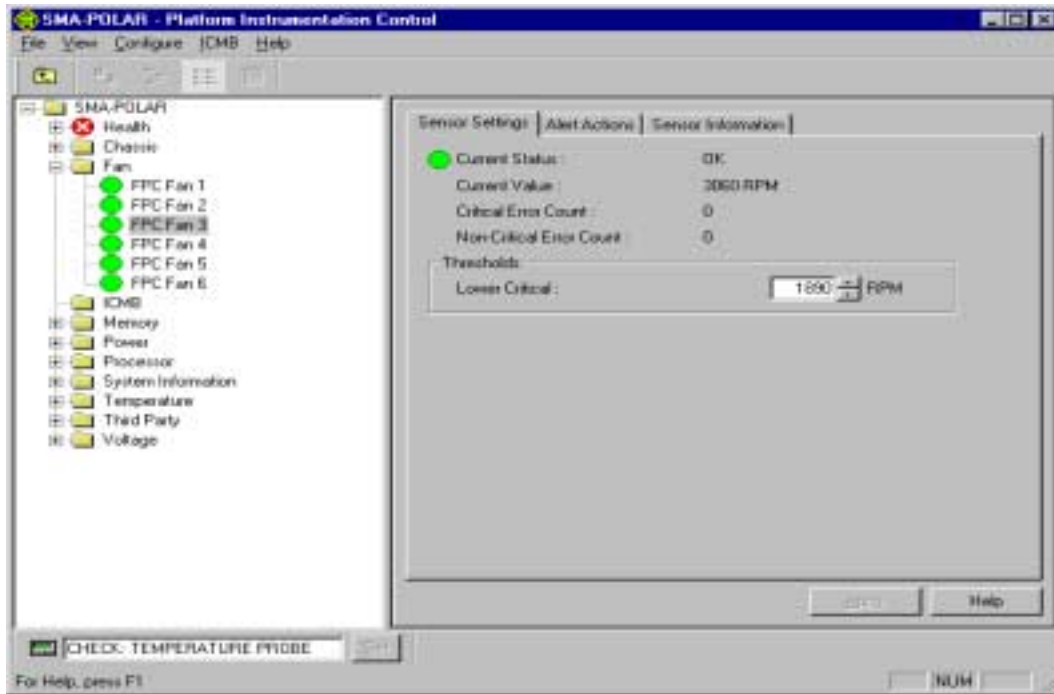


Figure 8 - 35: Fan Sensor Settings

On the Sensor Settings tab page, the Current Status can have the following values:

- OK
- Critical
- Unknown

Sensor values are displayed in Revolutions per Minute (RPM). The fan control will display the actual fan RPM value for systems that support this feature. For the systems that support non-RPM sensing fans, the threshold setting has a value of zero and is read-only.

On the Alert Action tab page, the user can configure event actions for the following threshold state changes:

- Cooling Device Failure
- Cooling Device OK

The Sensor Information tab page displays the following fan sensor attributes:

- Sensor Units – the fan display unit, which is RPM, CFM or OK/Fatal. OK/Fatal is only supported on non-RPM sensing Fans.
- Sensor Accuracy – The accuracy for the reading from this fan probe, in plus/minus hundredths of a percent.
- Sensor Tolerance – The tolerance for the reading from this fan probe, in plus/minus Sensor Units.
- Probe Maximum – The maximum reading supported by this probe.
- Normal Maximum – The normal maximum reading monitored by this probe.
- Nominal Reading – The nominal reading monitored by this probe.
- Normal Minimum – The normal minimum reading monitored by this probe.
- Probe Minimum – The minimum reading supported by this probe.

6.3 Memory Array

The Memory Array control displays information for all memory array sensors on the managed server. A memory array is a group or bank of memory devices. For memory array sensors, four tab pages are available in the Presentation Pane:

- Sensor Status
- Alert Actions
- Sensor Information
- Inventory Information

Note: Not all servers support the Memory Array sensors.

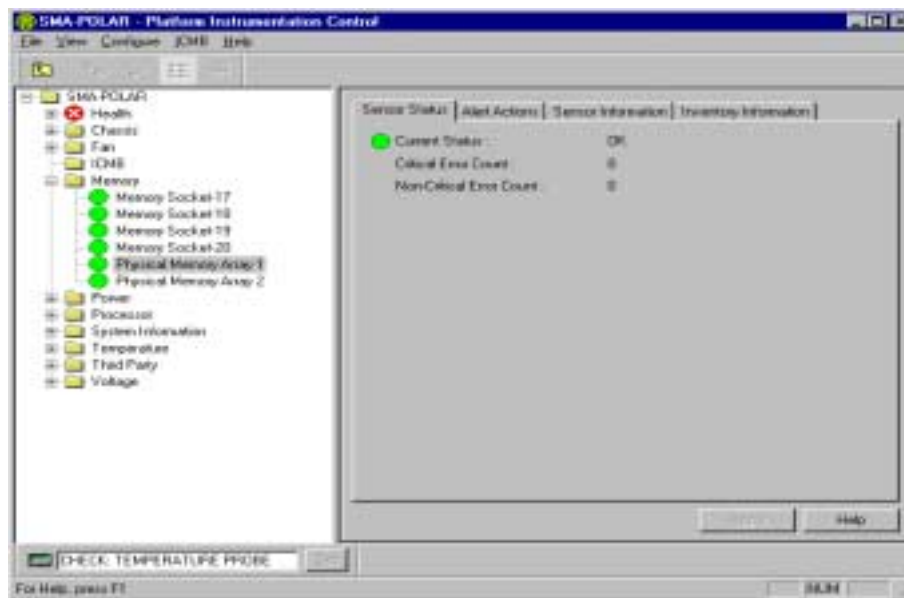


Figure 8 - 36: Memory Array Sensor Status

On the Sensor Status tab page, Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following state changes:

- Single Bit Memory Error
- Multi Bit Memory Error (from previous boot)

The Sensor Information tab page displays the following memory array sensor attributes:

- Memory Array Location – The physical location of the Memory Array, whether on the system board or an add-on board.
- Memory Array Usage – What this memory array is used for.
- Number of Sockets – The number of slots or sockets available for memory devices in this memory array.
- Number of Sockets Used – The number of slots or sockets in use by memory devices in this memory array.
- Memory Error Correction – The main hardware error correction or detection method supported by this memory array.
- Memory Array Error Type – The type of error that is associated with the current status value.
- Last Error Update – System state during which the last error status was collected.

The Inventory Information tab page displays the following memory array sensor attributes:

- Description – A description of this memory array.
- Manufacturer – The name of the company manufacturing or providing this memory array.
- Model – The manufacturer's model number for this memory array.
- Part Number – A part number by which a replacement part can be ordered.
- Serial Number – The manufacturer's serial number for this memory array.
- Revision Level – The revision level of this memory array.

6.4 Memory Device

The Memory Device control displays information for all memory device sensors on the managed server. A memory device is a SIMM or DIMM. For memory device sensors, two tab pages are available in the Presentation Pane:

- Sensor Status
- Sensor Information

Note: Not all servers support the Memory Device sensors.

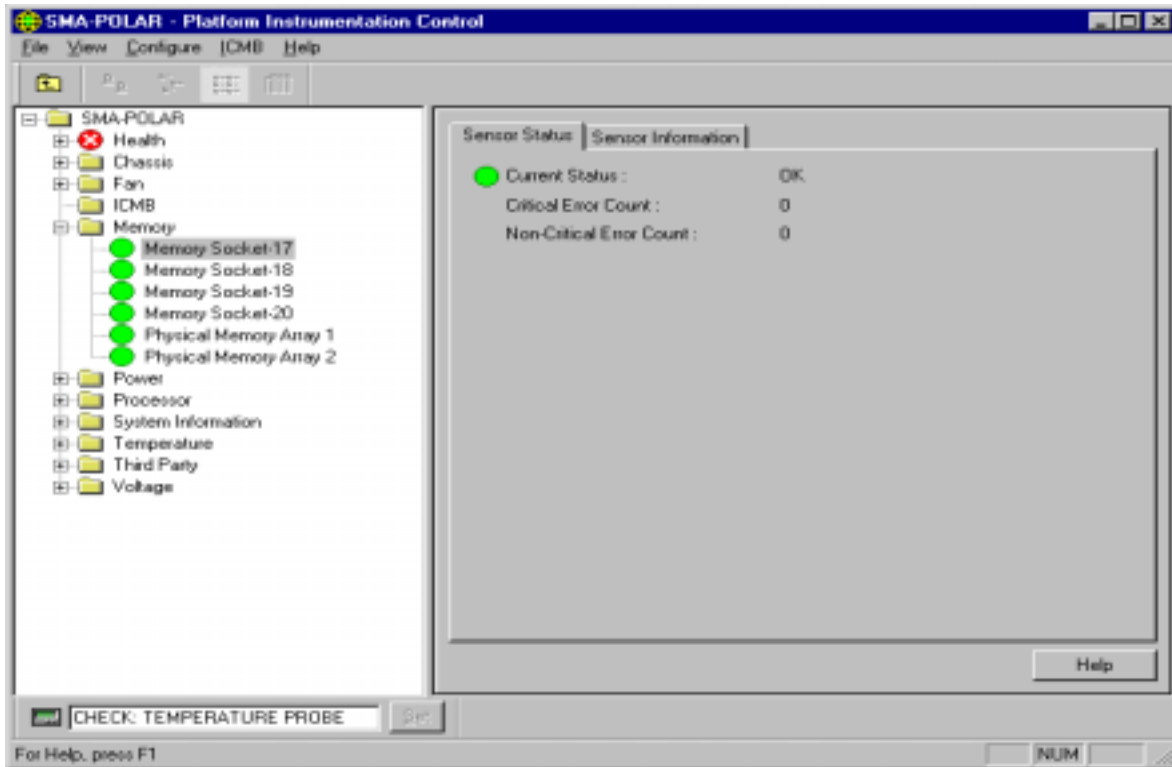


Figure 8 - 37: Memory Device Sensor Status

On the Sensor Status tab page, Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

The Sensor Information tab page displays the following memory array sensor attributes:

- Memory Device Size – The size of the memory device, in Bytes.
- Memory Device Form Factor – Implementation form factor for this memory device.
- Memory Device Total Width – Total width of this memory device, including check or error correction bits, in bits. If there are no error correction bits, the value in this attribute should match that specified in Memory Device Data Width.
- Memory Device Data Width – Data width of this memory device, in bits. A data width of 0 and a Total Width of 8 would indicate that the device is solely being used to provide eight error correction bits.
- Memory Type – Type of memory used in this memory device.

- Memory Type Detail – Additional detail on the memory device type.
- Memory Device Error Type – The type of error that is associated with the current status value.
- Last Error Update – System state during which the last error status was collected.

6.5 PCI Hot Plug Device

The PCI Hot Plug Device control displays information for each PCI Hot Plug device that is plugged into one of the PHP slots on the managed system.

Note: When a PCI device does not exist in the slot or when the power to a given slot is off, the corresponding device entry is still shown in the tree under the PCI Hot Plug Device group in the Navigation Pane. The corresponding Sensor Information tab page displays the information for Manufacturer, Device Type and Device Revision as “unknown”.

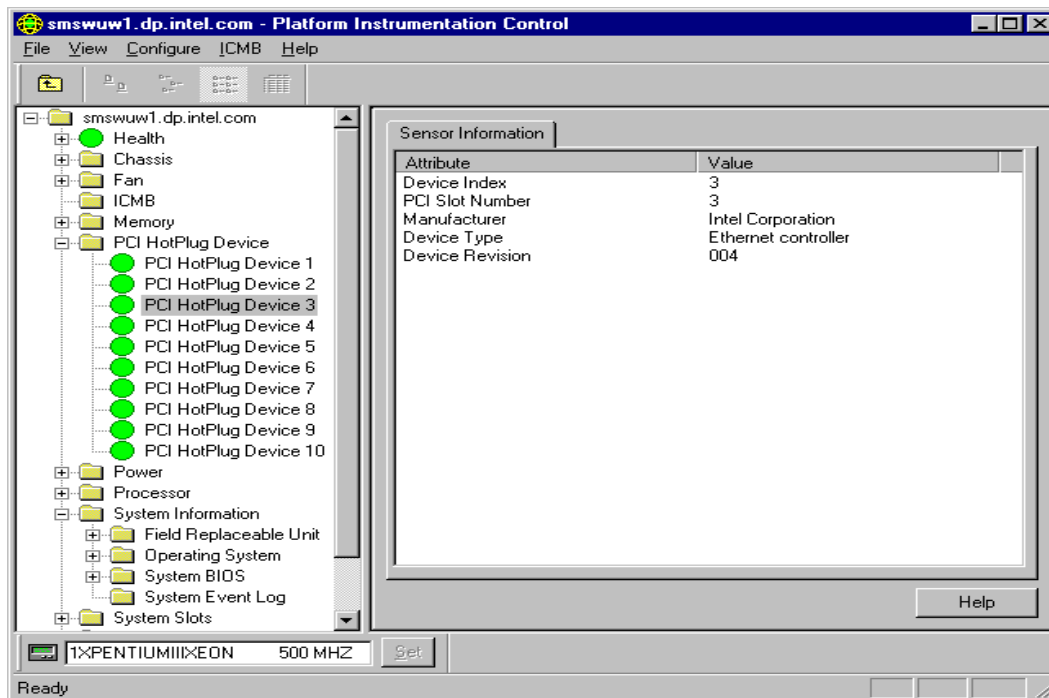


Figure 8 - 38: PCI Hot Plug Device Sensor Information

The Sensor Information tab page displays the following information:

- Device Index – An index into the devices for PHP system slots.
- PCI Slot Number – The PHP slot number in which this device is occupying.
- Manufacturer – Manufacturer of the device that is currently occupying the PHP slot.
- Device Type – Displays what type of device is currently occupying the PHP slot.
- Device Revision – Revision ID of the device that is currently occupying the PHP slot.

6.6 Power Supply

The Power Supply control displays information for all power supply sensors on the managed server. For power supply sensors, three tab pages are available in the Presentation Pane:

- Sensor Status
- Alert Actions
- Sensor Information

Note: Not all servers support the Power Supply sensors.

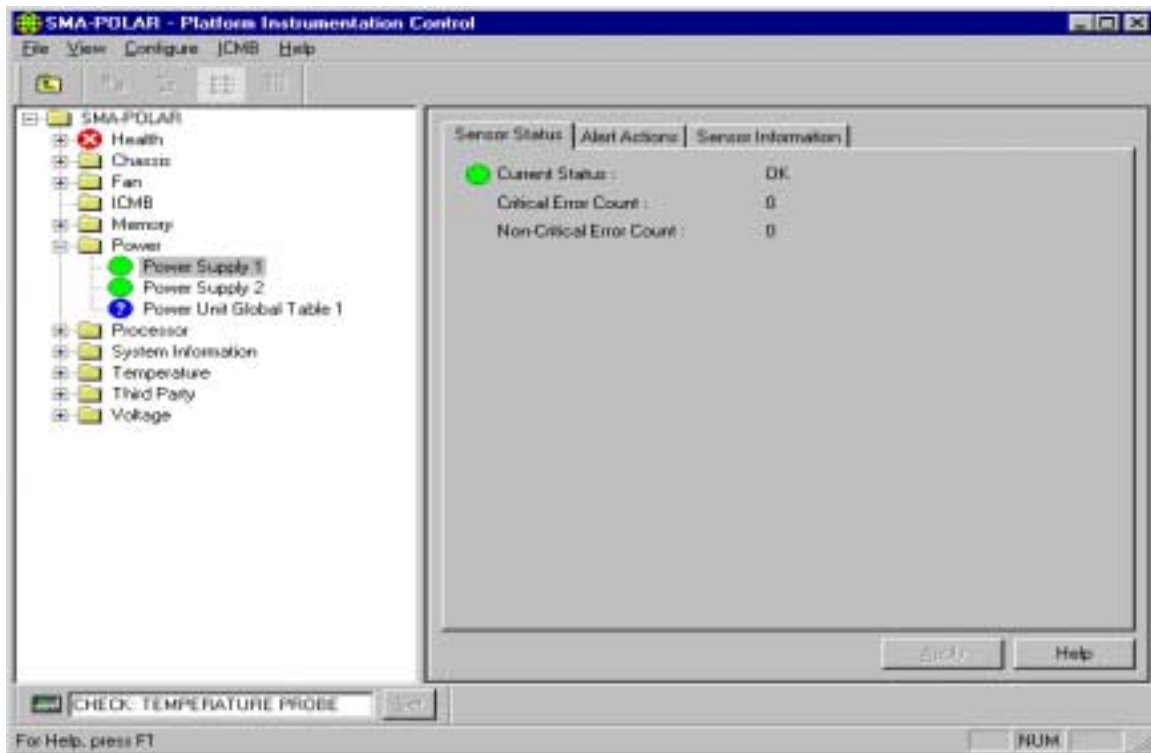


Figure 8 - 39: Power Supply Sensor Status

On the Sensor Status tab page, Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following state changes:

- Power Supply Failed
- Power Supply OK
- Power Supply Likely to Fail

The Sensor Information tab page displays the following power supply sensor attributes:

- Power Supply Type – This attribute describes the type of power supply, e.g. Linear, Switching, and Battery.
- Total Output Power – The total output power of this power supply.

6.7 Power Unit

The Power Unit control displays the power redundancy status on the managed server. For power unit sensors, two tab pages are available in the Presentation Pane:

- Sensor Status
- Alert Actions

Note: Not all servers support the Power Unit sensors.

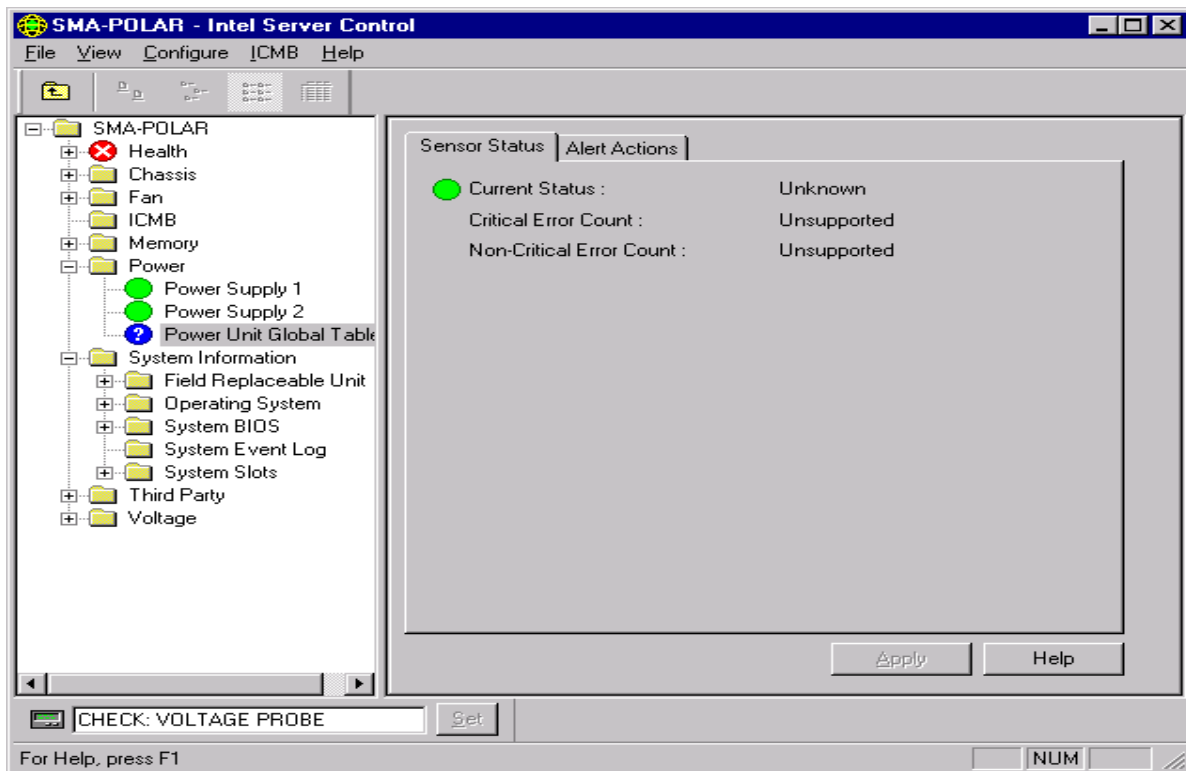


Figure 8 - 40: Power Unit Sensor Status

On the Sensor Status tab page, Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following state changes:

- Power Unit Redundancy Lost
- Power Unit Fully Redundant
- Power Unit Redundancy Degraded
- Power Unit VA Shutdown Condition Cleared
- Power Unit VA Shutdown Limit Exceeded

6.8 Processor

The Processor control displays information for all processor sensors on the managed server. For processor sensors, four tab pages are available in the Presentation Pane:

- Sensor Status
- Alert Actions
- Sensor Information
- Inventory Information

Note: Not all servers support the Processor sensors.

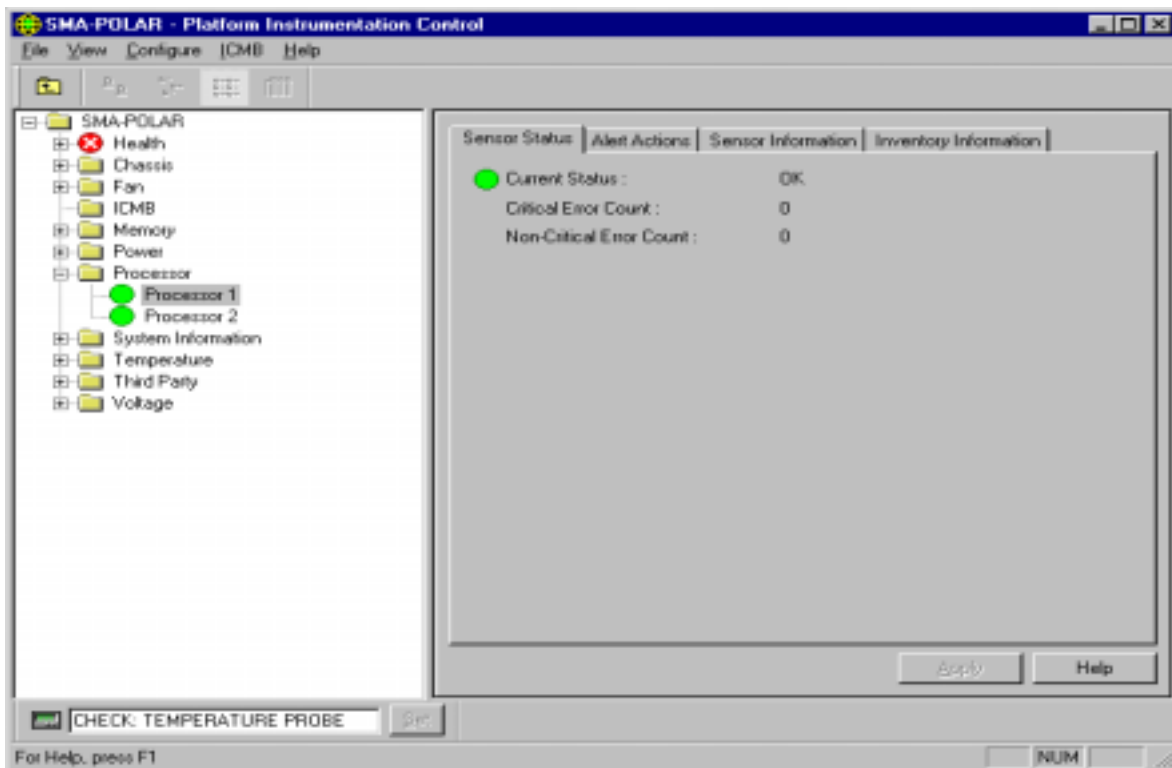


Figure 8 - 41: Processor Sensor Status

On the Sensor Status tab page, Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following state changes:

- Processor Internal Error
- Processor Thermal Trip
- Processor FRB-3 Error
- Processor Disabled Error

The Sensor Information tab page displays the following processor sensor attributes:

- Processor Type – The type of processor currently in the system.
- Processor Family – The family of processors to which this processor belongs.
- Processor Upgrade – The method by which this processor can be upgraded, if upgrades are supported.
- Processor Maximum Speed – The maximum speed (in MHz) of this processor.
- Processor Current Speed – The current speed (in MHz) of this processor.

The Inventory Information tab page displays the following processor sensor attributes:

- Description – A description of this processor.
- Manufacturer – The name of the company manufacturing or providing this processor.
- Model – The manufacturer's model number for this processor.
- Part Number – A part number by which a replacement part can be ordered.
- Serial Number – The manufacturer's serial number for this processor.
- Revision Level – The revision level of this processor.

6.9 System Information

System Information is a logical grouping of system related components. It includes:

- Field Replaceable Unit (FRU) information
- Operating System information
- System BIOS information
- System Event Log information
- System Slot information

This information is discussed in the following sections.

6.9.1 Field Replaceable Unit (FRU)

The FRU control displays a list of FRU attributes for all FRU devices on the managed system.

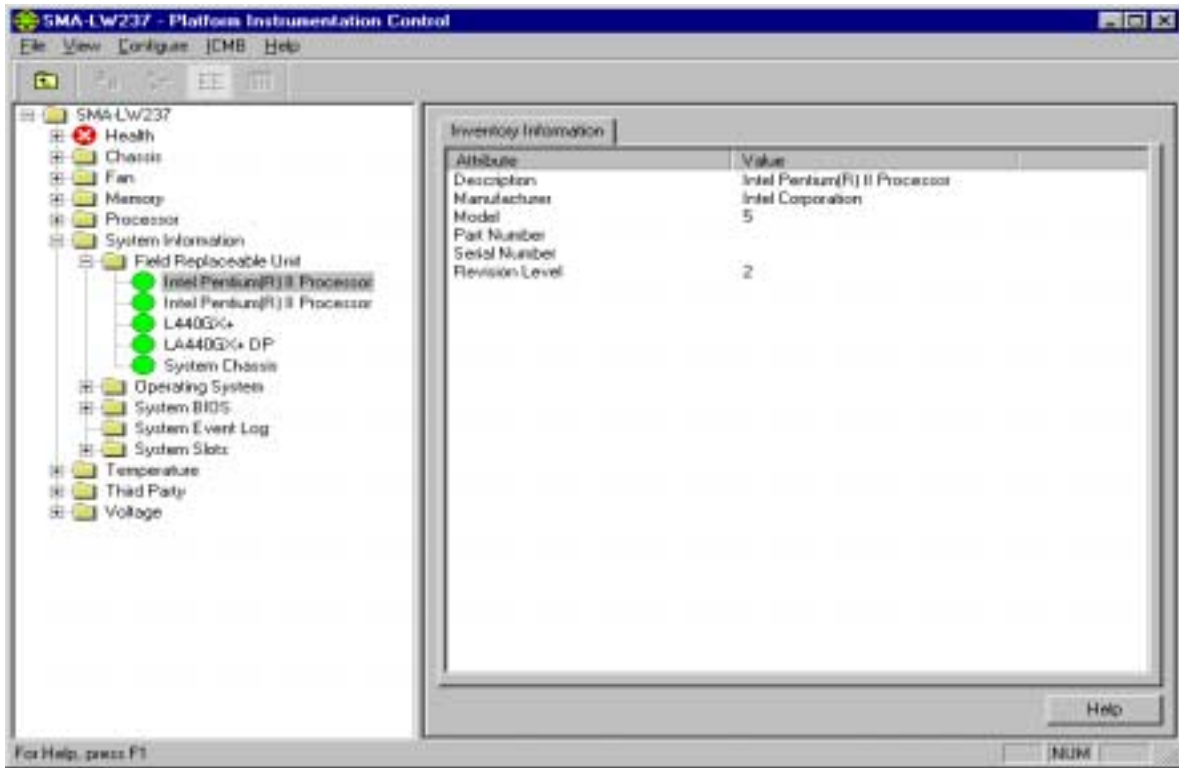


Figure 8 - 42: Field Replaceable Unit (FRU) Inventory Information

The Inventory Information tab page displays the following FRU attributes:

- Description – A description of this FRU device.
- Manufacturer – The name of the company manufacturing or providing this FRU device.
- Model – The manufacturer's model number for this FRU device.
- Part Number – A part number by which a replacement part can be ordered.
- Serial Number – The manufacturer's serial number for this FRU device.
- Revision Level – The revision level of this FRU device.

6.9.2 Operating System

The Operating System (OS) control displays a list of operating system attributes for all operating systems installed on the managed system.

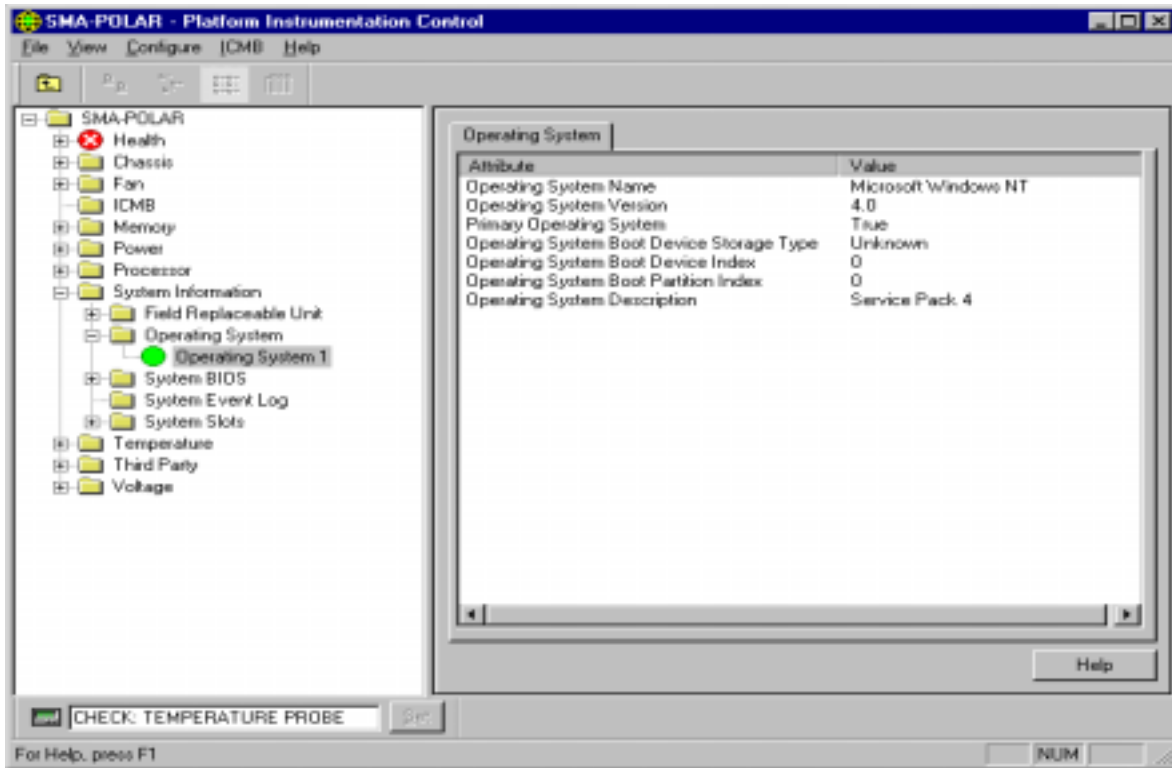


Figure 8 - 43: Operating System Information

The Operating System tab page displays the following information:

- Operating System Name – The name of this operating system.
- Operating System Version – The version number of this operating system.
- Primary Operating System – If True, then this is the primary operating system on this server.
- Operating System Boot Device Storage Type – An index into the Disks Table to indicate the device from which this operating system was booted. To fully access the Disks Table, this index must be combined with the attribute Boot Device Index.
- Operating System Boot Device Index – An index into the Disks Table.
- Operating System Boot Partition Index – An index into the Partition table indicating the partition from which this operating system booted.
- Operating System Description – A description of this operating system.

6.9.3 System BIOS

The System BIOS control displays a list of BIOS attributes for all system BIOSs installed on the managed system.

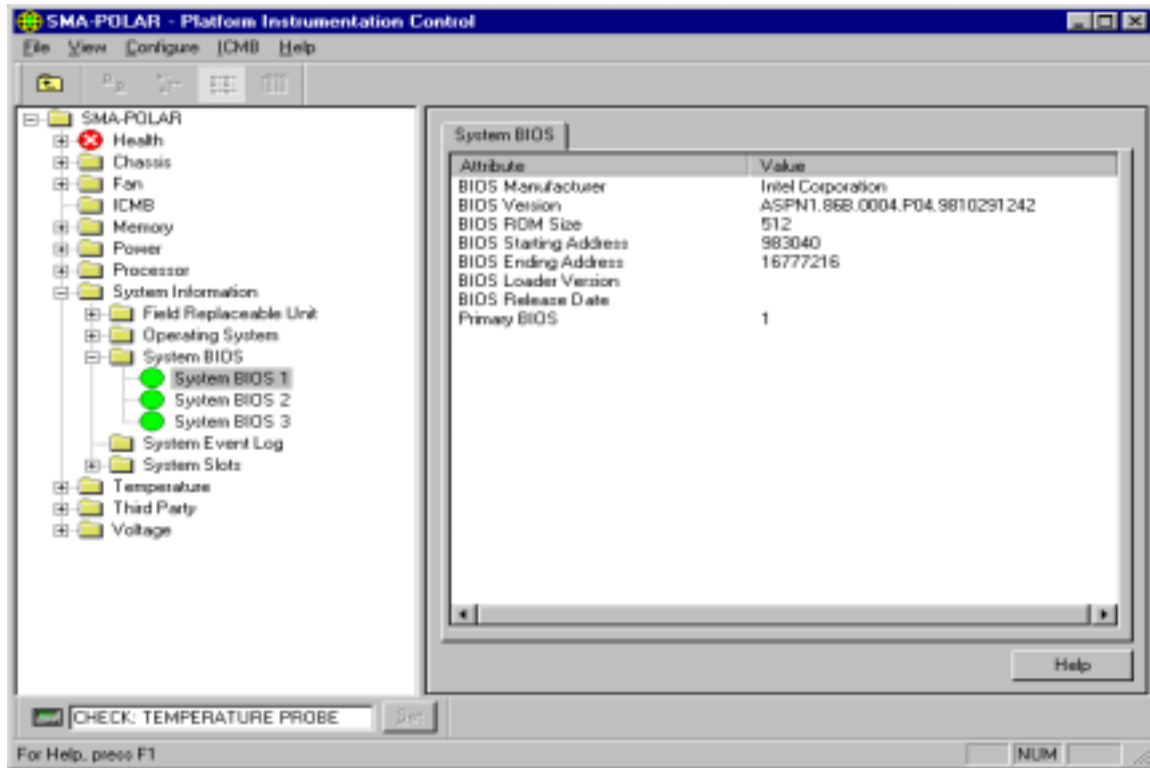


Figure 8 - 44: System BIOS Information

The System BIOS tab page displays the following information:

- BIOS Manufacturer – The name of the company that wrote this system BIOS.
- BIOS Version – The version number or version string of this BIOS.
- BIOS ROM Size – The physical size of this BIOS ROM device in kilobytes.
- BIOS Starting Address – The starting physical address for the memory, which the BIOS occupies.
- BIOS Ending Address – The ending physical address for the memory, which the BIOS occupies.
- BIOS Loader Version – The BIOS flash loader version number or string.
- BIOS Release Date – The BIOS release date.
- Primary BIOS – If true, this is the primary System BIOS.

6.9.4 System Event Log (SEL)

The SEL control displays a list of BIOS attributes on the managed system. The BIOS list shows the manufacturer, version, and other BIOS attributes.

The SEL control allows the user to view the contents of the managed server's system event log.

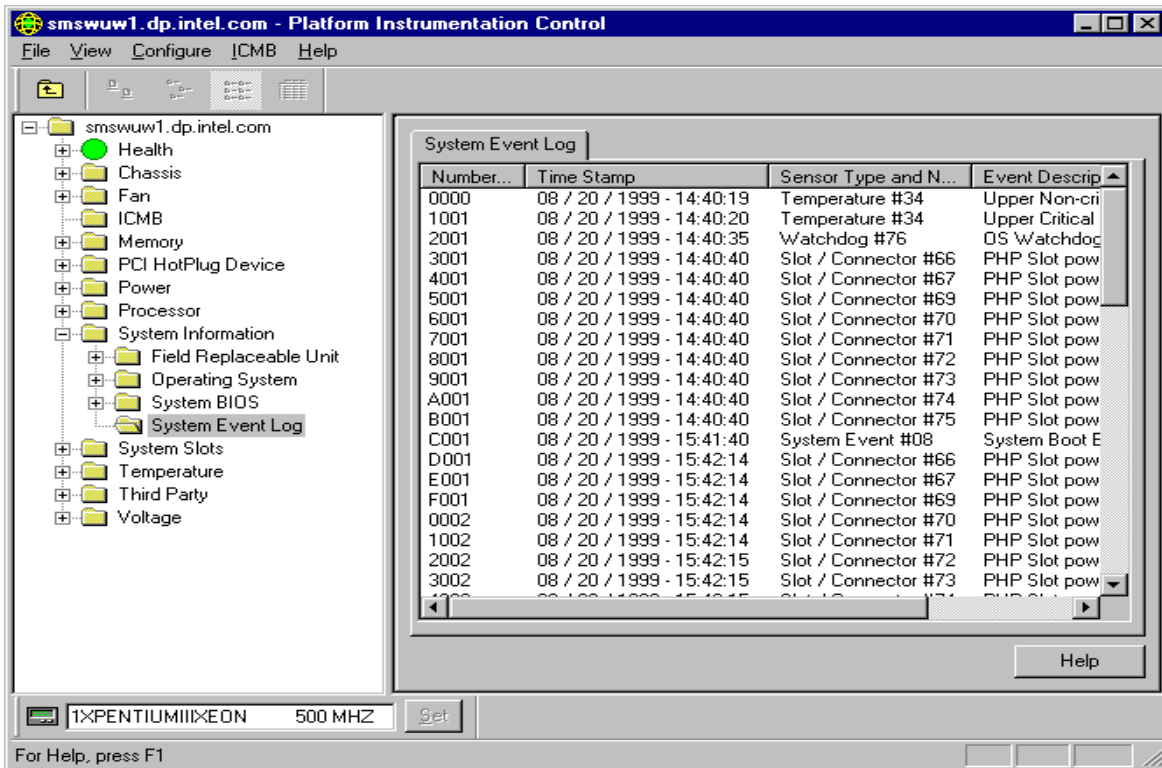


Figure 8 - 45: System Event Log Information

The SEL tab page displays the following information for each record in the system event log:

- Number of Events – a numbered listing to uniquely identify each record. Numbers may vary each time SEL is displayed.
- Timestamp – Date and Time record was recorded. If the record was generated prior to the BIOS loading, the timestamp has a value of “Pre-Init Timestamp”.
- Sensor Type and Number – Unique identification of event originator.
- Event Description – Description of event.
- Generator ID – The component or sensor that generated the event (e.g. BIOS, SMI Handler).

6.10 System Slots

The System Slots control displays information for all system slot sensors on the managed server. System Slots are categorized into two groups:

- PCI Hot Plug (PHP) slots
- All other non-PHP system slots

Slot names containing “PCI 64-bit” identify PCI Hot Plug or PHP slots. For PHP type slots, there are three tab pages available in the Presentation Pane: Sensor Status, and Alert Action, and Sensor Information. For non-PHP slots, only the Sensor Information tab page is available.

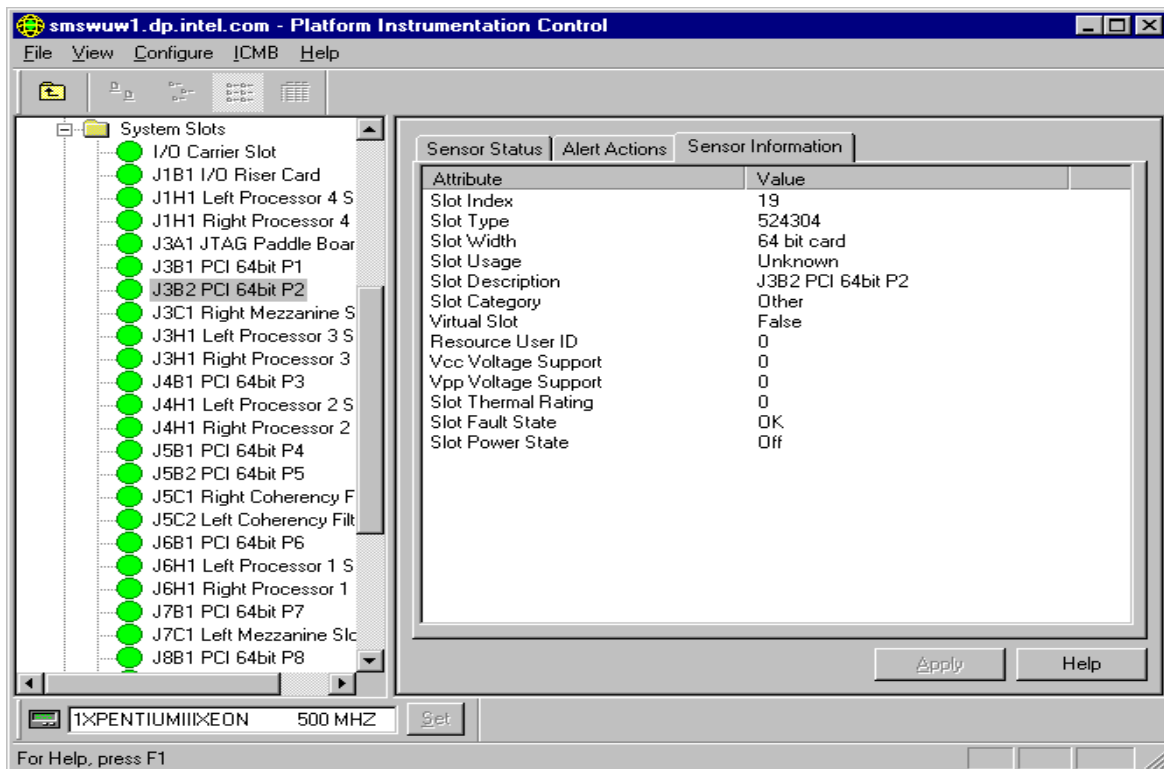


Figure 8 - 46: PHP System Slots Sensor Information

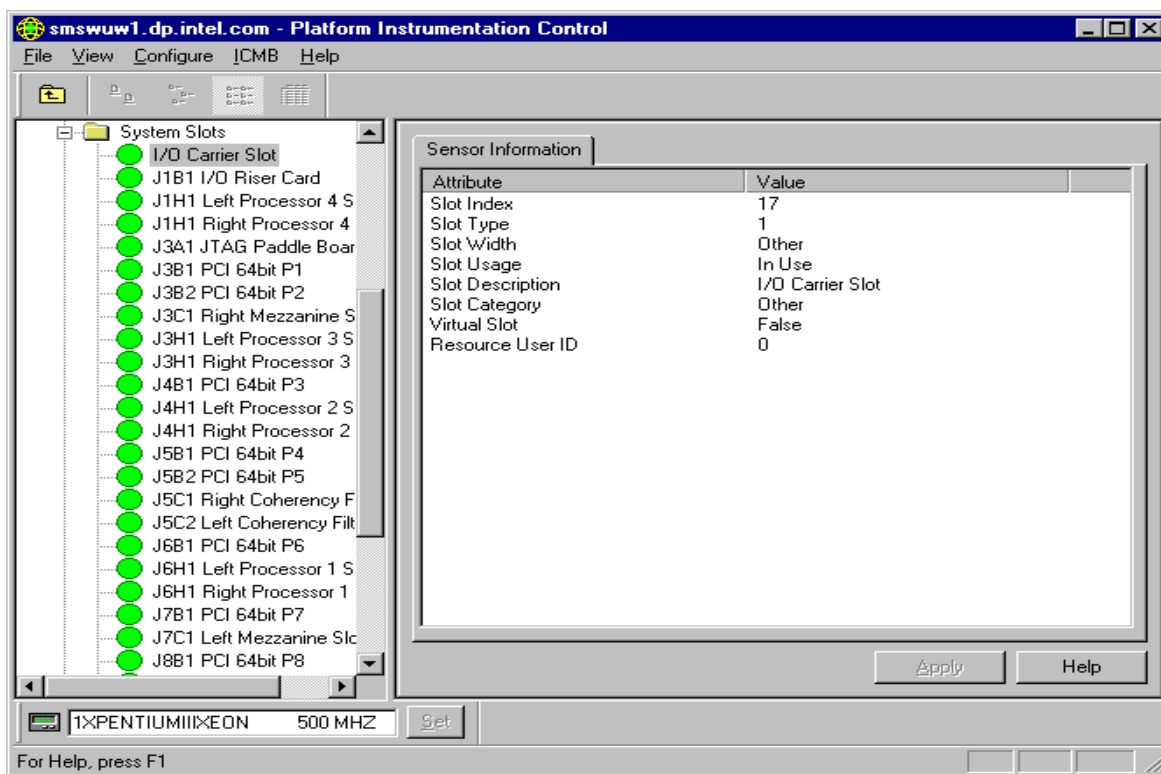


Figure 8 - 47: Non-PHP System Slots Sensor Information

On the Sensor Status tab page, Current Status can have the following values for PHP slots:

- OK
- Critical
- Unknown

On the Alert Action tab page, the user can configure event actions for the following threshold state changes:

- Slot Status change to OK
- Slot Status change to Critical
- Slot Powered On
- Slot Powered Off

The Sensor Information tab page displays the following information for each slot (PHP or non-PHP):

- Slot Index – An index into the system slot table.
- Slot Type – The bus type supported in this slot.
- Slot Width – The maximum bus width of card in this slot.
- Slot Usage – Slot in use indicator (Available/In Use).
- Slot Description – A description of the card currently in the slot.

- Slot Category – Which category of physical slot is this table entry defining?
- Virtual Slot – Indicate whether this is a ‘virtual slot’.
- Resource User ID – Locates the rows in the System Resource table used for this slot.
- Vcc Voltage Support – Device Vcc Mixed Voltage support.
- Vpp Voltage Support – Device Vpp Mixed Voltage support.
- Slot Thermal Rating – The maximum thermal dissipation of the slot in milliwatts.
- Slot Fault State – The current error state for the PHP system slot. (OK/Failed – Apply to PHP slot only)
- Slot Power State – The current power state of the PHP system slot. (On/Off – Apply to PHP slot only)

6.11 Temperature

The Temperature control displays information for all temperature sensors on the managed server. For temperature sensors, three tab pages are available in the Presentation Pane:

- Sensor Settings
- Alert Actions
- Sensor Information

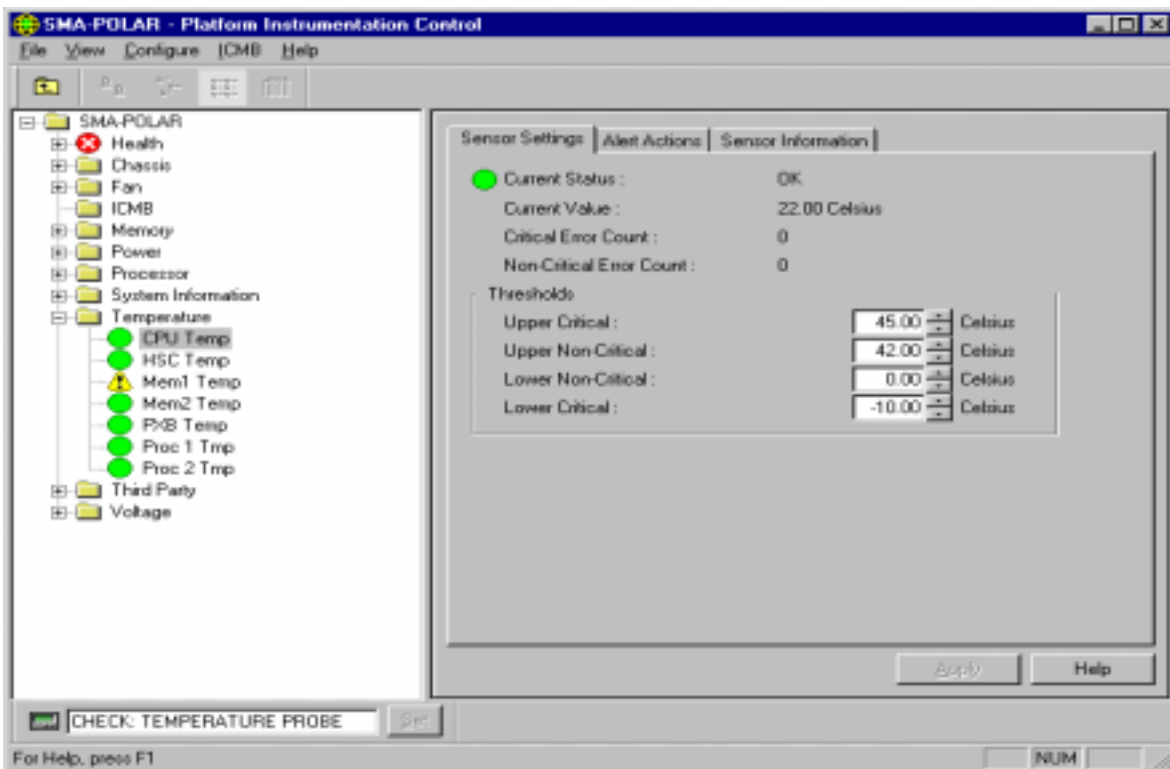


Figure 8 - 48: Temperature Sensor Settings

On the Sensor Settings tab page, the Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

Depending on the individual temperature sensor and the server platform, some thresholds are unsupported and will appear disabled (grayed out) in the control. The user can display temperature information in Celsius or Fahrenheit. The display format can be changed by selecting the Main Menu / View / Options menu selection. The default temperature display format is Celsius.

On the Alert Action tab page, the user can configure event actions for the following threshold state changes:

- Temperature – Status Changed to OK
- Temperature – Status Changed to Upper Critical
- Temperature – Status Changed to Lower Critical
- Temperature – Status Changed from OK to Upper Non-Critical
- Temperature – Status Changed from OK to Lower Non-Critical
- Temperature – Status Changed from Critical to Upper Non-Critical
- Temperature – Status Changed from Critical to Lower Non-Critical

The Sensor Information tab page displays the following temperature sensor attributes:

- Sensor Units – the temperature display unit in either Celsius or Fahrenheit. The default is Celsius.
- Sensor Accuracy – The accuracy for the reading from this temperature probe, in plus/minus hundredths of a percent.
- Sensor Resolution – The resolution for the reading from this temperature probe.
- Sensor Tolerance – The tolerance for the reading from this temperature probe, in plus/minus Sensor Units.
- Probe Maximum – The maximum temperature level specified to be readable by this probe.
- Normal Maximum – The normal maximum temperature reading of the temperature monitored by this probe.
- Nominal Reading – The nominal temperature reading of the temperature monitored by this probe.
- Normal Minimum – The normal minimum temperature reading of the temperature monitored by this probe.
- Probe Minimum – The minimum temperature level specified to be readable by this probe.

6.12 Third Party Instrumentation

The Third Party control displays event configuration information for supported third party instrumentation on the managed server. For third party instrumentation, one tab page is available in the Presentation Pane: Alert Actions. Note: not all servers support all third party instrumentation.

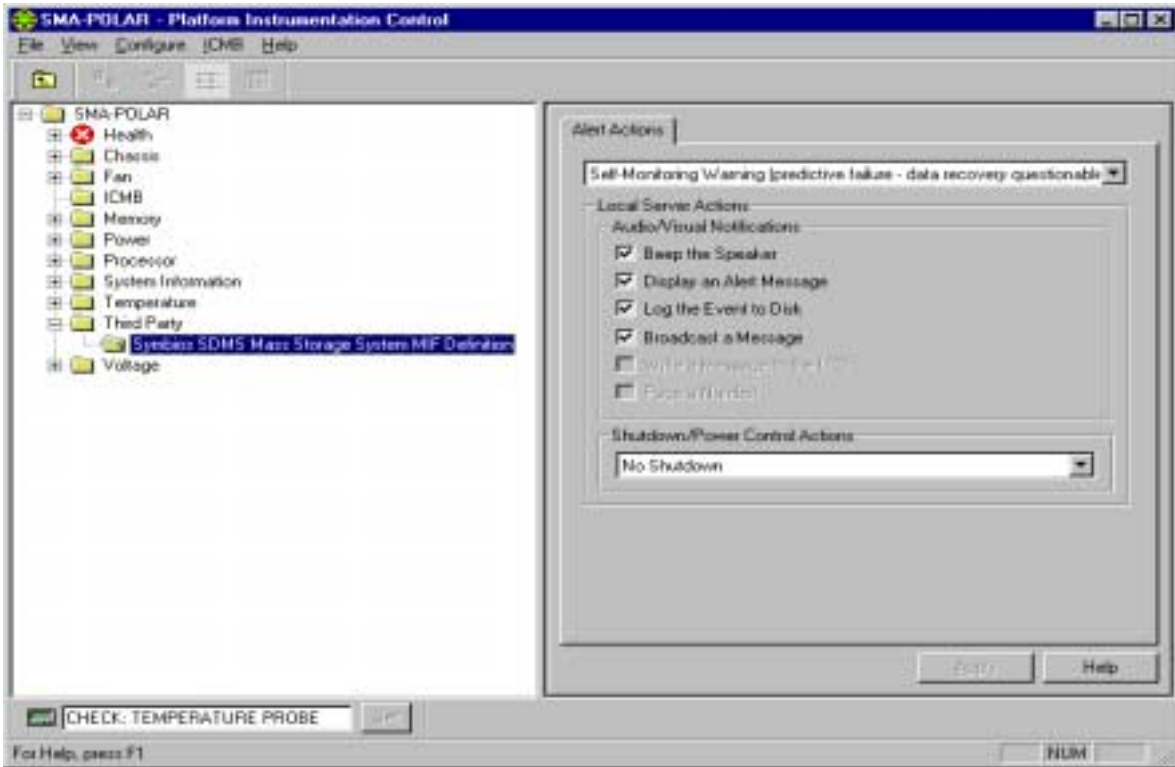


Figure 8 - 49: Third Party Alert Actions

The following versions of Third Party instrumentation is supported by PIC:

- Adaptec* SCSI
- Adaptec CI/O Standard Group MIF
- Symbios* Scientific Data Management System (SDMS) Mass Storage System MIF
- Symbios DMI 2.0 MIF Definition
- Intel EtherExpress™ PRO/100B LAN Adapter
- Intel Ethernet LAN Adapter(s)

On the Alert Action tab page, the user can configure event actions for the following Adaptec SCSI events:

- Host Adapter – Discovered
- Host Adapter – Changed
- Host Adapter – Failed
- Host Adapter – Recovered
- Logical Unit – Discovered
- Logical Unit – Changed
- Logical Unit – Failed
- Logical Unit – Recovered
- Logical Unit – Failure Predicted

On the Alert Action tab page, the user can configure event actions for the following Adaptec CI/O Standard Group MIF events:

- Storage device state information
- Storage device recovered error – Bad block repaired
- Storage device member marked down
- Storage controller state information
- Storage controller SMART event
- Storage controller status unacceptable
- Volume set state information
- Volume set recovered error
- Volume set Array status – offline
- ARO spare not functional
- Enclosure state information

On the Alert Action tab page, you can configure event actions for the following Symbios SDMS Mass Storage System MIF events:

- Device Error (not responding)
- Device Warning (predicted failure (S.M.A.R.T.))
- Controller Error (not responding)
- New Storage controller detected
- New device detected
- Existing controller changed
- Existing device changed

On the Alert Action tab page, you can configure event actions for the following Symbios DMI 2.0 MIF Definition events:

- Device Error (not responding)
- Device Warning (predicted failure (S.M.A.R.T.))
- Controller Error (not responding)
- New Storage controller detected
- New device detected
- Existing controller changed
- Existing device changed

On the Alert Action tab page, you can configure event actions for the Intel EtherExpress PRO/100B LAN Adapter events:

- Transmit Errors crossing thresholds
- Receive Errors crossing thresholds
- Host Errors crossing thresholds
- Wire Errors crossing thresholds

On the Alert Action tab page, the user can configure event actions for the following Intel Ethernet LAN Adapter(s) events:

- Cable unplugged / No LAN activity
- Adapter initialization failure
- The Primary Adapter is switching over and the Secondary Adapter toOK over
- The Primary adapter became active
- Secondary Adapter is deactivated from the team
- The last Adapter has lost link. Network connection has been lost
- Preferred Primary Adapter has been detected
- The team only has one active adapter
- The Secondary adapter has re-joined the team
- Preferred Primary Adapter has taken over
- Network Connection restored

6.13 Voltage

The Voltage control displays information for all voltage sensors on the managed server. For voltage sensors, three tab pages are available in the Presentation Pane:

- Sensor Settings
- Alert Actions
- Sensor Information

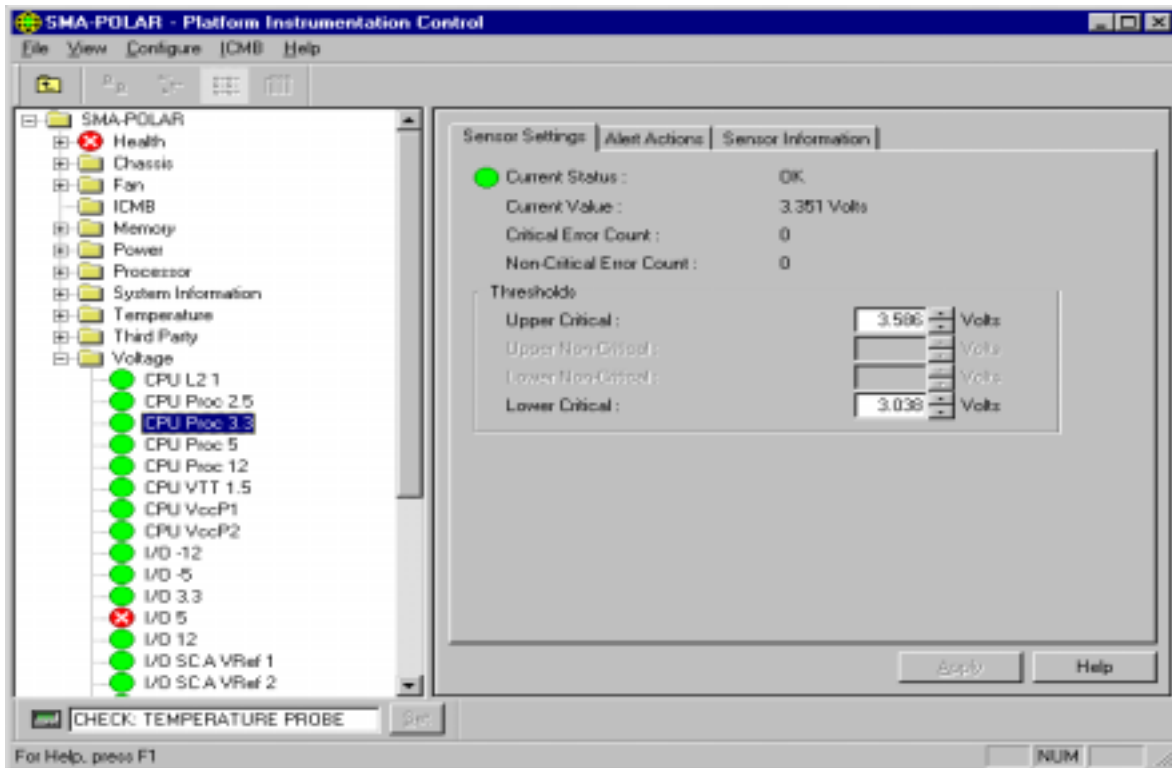


Figure 8 - 50: Voltage Sensor Settings

On the Sensor Settings tab page, the Current Status can have the following values:

- OK
- Non-Critical
- Critical
- Unknown

Depending on the individual voltage sensor and the server platform, some thresholds are unsupported and will appear disabled (grayed out) in the control. All values are displayed in “Volts”.

On the Alert Action tab page, the user can configure event actions for the following threshold state changes:

- Voltage – Status Changed to OK
- Voltage – Status Changed to Upper Critical
- Voltage – Status Changed to Lower Critical
- Voltage – Status Changed from OK to Upper Non-Critical
- Voltage – Status Changed from OK to Lower Non-Critical
- Voltage – Status Changed from Critical to Upper Non-Critical
- Voltage – Status Changed from Critical to Lower Non-Critical

The Sensor Information tab page displays the following voltage sensor attributes:

- Sensor Units – the voltage display unit, which is Volts.
- Sensor Accuracy – The accuracy for the reading from this voltage probe, in plus/minus hundredths of a percent.
- Sensor Resolution – The resolution for the reading from this voltage probe.
- Sensor Tolerance – The tolerance for the reading from this voltage probe, in plus/minus Volts.
- Probe Maximum – The maximum voltage level specified to be readable by this probe.
- Normal Maximum – The normal maximum voltage level of the voltage monitored by this probe.
- Nominal Reading – The nominal voltage level of the voltage monitored by this probe.
- Normal Minimum – The normal minimum voltage level of the voltage monitored by this probe.
- Probe Minimum – The minimum voltage level specified to be readable by this probe.

Intel® Server Control, Version 3.x TPS

Section 9: ICMB

Table of Contents

- 1. Intelligent Chassis Management Bus (ICMB)..... 1
 - 1.1 ICMB 1
 - 1.1.1 Setting Up an ICMB Connection 1
 - 1.1.2 Configuring the Management Point Server 2
 - 1.2 Setting Up ICMB 2
 - 1.2.1 Discovering Remote ICMB Systems 3
 - 1.2.2 Viewing and Managing Viewing Remote ICMB Systems..... 4

List of Figures

Figure 1: Enabling ICMB Features 4
Figure 2: Viewing Remote Servers via ICMB..... 5
Figure 3: Displaying Remote Server Information 5

List of Tables

No tables appear in this section.

1. Intelligent Chassis Management Bus (ICMB)

The Intelligent Chassis Management Bus (ICMB) provides a means by which an intelligent device on the Intelligent Platform Management Bus (IPMB) in a chassis communicates with the intelligent device on the IPMB in another chassis. The ICMB protocol is used for inter-chassis communications. This is possible because the server provides two 6-pin connectors to enable multiple servers to be daisy chained together.

The ICMB provides additional troubleshooting and status capabilities by providing information that can be used to predict and identify failures on multiple servers. The ICMB is used to provide remote power control and status information on servers that cannot be normally obtained through in-band channels. This may be because the information is not provided through those channels or because the in-band channels are not available, such as when the chassis is powered down. The ICMB, as with other instrumentation described in this document, is accessed by Intel Server Control.

ICMB provides the ability to communicate information such as:

- Chassis management functions
- System Event Log
- Chassis power control
- Field Replaceable Unit part numbers and serial numbers
- Sensors values have been added on SR460AC4 based systems

On IA-32 based systems the ICMB card was plugged into a standard expansion slot and into the IPMB cable system board connector.

1.1 ICMB

You can use ICMB to communicate with servers having operating systems or architectures that are not otherwise supported by the Intel server management software applications. To manage these types of servers you need to do the following:

- Set up an ICMB Connection
- Configure the point server for ICMB

1.1.1 Setting Up an ICMB Connection

In general, you must meet the following connection requirements to manage or monitor servers through an ICMB connection:

- You must establish a Management Point Server. This server is a managed server that has an ICMB interface and has the ISC software installed.
- A functional LAN connection must exist between the Management Point Server and the Client Workstation.
- All servers that you wish to manage or monitor through ICMB must be physically connected through their respective ICMB interface ports. For example, the Management

Point Server is connected to a server, while that server is connected to another server all using ICMB connections.

For more details (if applicable) on connecting a specific server platform for ICMB management, refer to the server's product guide.

1.1.2 Configuring the Management Point Server

Before the Management Point Server can search for and communicate information over an ICMB connection, you must enable the ICMB by starting the EIF service. For a given operating system, follow these steps to start the EIF service:

1.1.2.1 Windows NT and Windows 2000 Systems

1. Go to the Services control panel.
2. Start the Intel EIF Agent service¹.

1.1.2.2 NetWare Systems

1. Open the `ISC_ON.NCM` file for editing.
2. Remove "rem" from the following line: `rem load eif`

Making this change causes the EIF service to be started each time the ISC services are started on the Management Point Server.

1.1.2.3 UnixWare Systems

Enter the following command at the console prompt on the Management Point Server:

```
/etc/init.d/isc start-icmb
```

Stop the service by entering the following command:

```
/etc/init.d/isc stop-icmb
```

1.2 Setting Up ICMB

The Intelligent Chassis Management Bus (ICMB) feature allows you to interconnect and share management information among multiple remote devices even when these devices do not support Intel's server management Platform Instrumentation installed. For example, your managed server could be configured to be an ICMB Management Point² Server and report management information on ICMB devices connected to it through ICMB cabling. Using the ICMB feature, 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 you are trying to manage.

¹ In the control panel you can specify that the EIF service is automatically started each time you start the system.

² Each time you reboot the Management Point Server, you must restart the service. Adding the command that starts the service to `/etc/rc.local` (or a similar startup script) will start the service automatically each time the systems boots.

In order to use the ICMB feature, you must be sure that you have chosen one server to be a Management Point Server and started the EIF service on that system³. For information on how to set up for the ICMB feature, refer to the *Intel® Server Control User's Guide*.

1.2.1 Discovering Remote ICMB Systems

Before you use the ICMB feature to look at connected servers, you must configure the Management Point Server and let it discover all the servers that are connected to it through the ICMB cabling.

Follow these steps to configure the Management Point Server:

1. Using PIC, view the Management Point Server. There will be a folder named "ICMB" in the navigation pane.
2. Open the ICMB folder to display ICMB Configuration dialog to the right of the navigation pane.
3. Check the box labeled "Enable as Management Point" in the "Local ICMB Server Configuration" area of the dialog box.
4. Check the box labeled "Enable Full Sensor View" in the same area of the dialog box.
5. Wait for the Management Point Server to discover all ICMB devices. As servers are discovered through the polling process, they appear in the "Remote ICMB Chassis Configuration" area of the dialog box.
6. Configure each remote ICMB server in the "Remote ICMB Chassis Configuration" area as follows:
 - Select the server in the pull-down field.
 - Choose whether to manage the chassis.
 - Choose whether to enable full-sensor view.
 - Define an event-polling period for that device.

³ It is necessary to start the EIF service on IA32-based servers only. You do not have to start this service if the Management Point Server is an Itanium-based server.

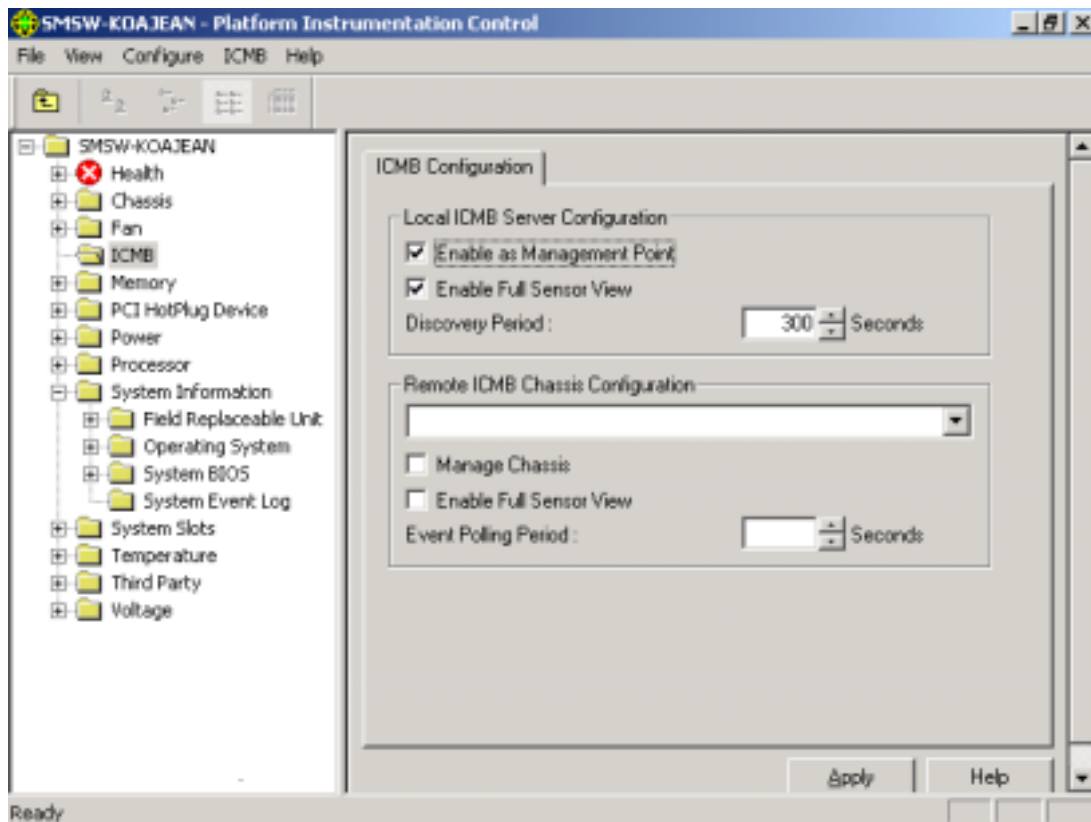


Figure 1: Enabling ICMB Features

1.2.2 Viewing and Managing Viewing Remote ICMB Systems

Once the discovery⁴ process is complete you can expand the ICMB folder shown in the navigation pane when connected to the Management Point Server. Every remote ICMB system appears beneath the folder.

You can view a remote ICMB system one the following two ways:

- Select the system in the navigation pane.
- Use the **ICMB / View Managed Server(s)** menu selection to display a list of all the remote ICMB servers and then select the server you want to view.

⁴ Each time you add or remove a remote ICMB chassis from your network, you must update the ICMB configuration by rediscovering existing ICMB systems.

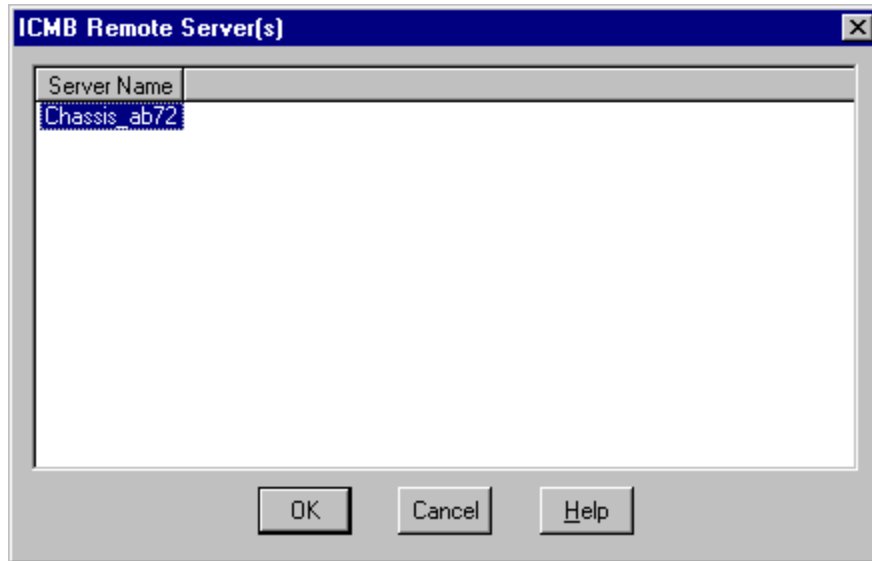


Figure 2: Viewing Remote Servers via ICMB

Either method causes the main dialog area of PIC to display information about the selected server. Information displayed includes the server's health, chassis, and system information for the Field Replaceable Units (FRU) and the System Event Log (SEL).

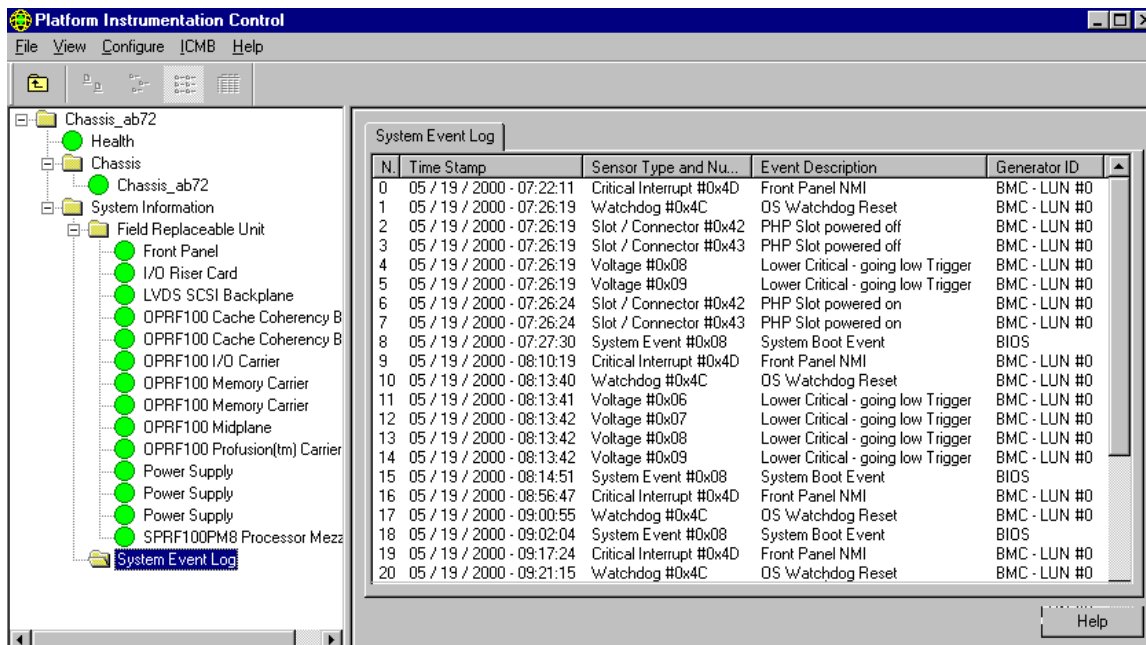


Figure 3: Displaying Remote Server Information

Viewing information about a remote ICMB system does not cause the client to lose connection to the Management Point Server. You can change your view back to the Management Point Server or to any other ICMB-managed device at any time. |

You can reclaim inactive ICMB system resources on the Management Point Server by selecting the **ICMB / Reclaim Inactive Resources** menu selection. Doing so frees the memory taken up by the SDR and FRU information on the Management Point Server for any remote device that is no longer visible on the network over ICMB.

Intel® Server Control, Version 3.x TPS

Section 10: Platform Event Paging

Table of Contents

- 1. Platform Event Paging (PEP) Overview 1
- 2. Page Configuration..... 3
 - 2.1 Platform Event Manager Add-In 3
 - 2.1.1 Platform Event Manager Window 3

List of Figures

Figure 10-1. Platform Event Manager Main Window 3
Figure 10-2. Platform Event Paging Dialog 4
Figure 10-3. Platform Event Action Dialogs..... 6

List of Tables

No tables appear in this section.

1. Platform Event Paging (PEP) Overview

Platform Event Paging is built into the Intel® Server Control platform management technology. This feature allows the platform to proactively alert the system administrator of critical system failures and state changes. It is independent of the state of the operating system or server management software.

Platform Event Paging uses an external modem that is connected to the system on-board Direct Platform Control port COM2 serial connector. This configuration allows the platform to contact a numeric paging service using the external modem.

With Platform Event Paging, the system can be configured to use the external modem to automatically dial a paging service and submit a paging string when a platform event occurs. This includes platform event conditions such as temperature out-of-range, voltage out-of-range, fan failure, and chassis intrusion.

When Platform Event Paging is enabled and the BMC receives or detects a new event, it automatically performs the paging operation. This allows event pages to be sent under conditions where the system processors are down or where system software is unavailable. Platform Event Paging can generate pages during pre-boot and post-boot states. The only requirements for it to function are that the BMC must be functional and power to the system must be available.

Platform Event Paging is built on top of another the Platform Event Filtering (PEF) BMC feature. Platform event filtering provides a flexible, general mechanism that enables the BMC to perform selectable actions triggered by a configurable set of platform events. If the modem is currently in use by another application, the BMC will interrupt and take ownership of the modem to complete the page.

When an alert or a page notifies the system administrator, s/he can use the Intel Server Control software to remotely view server health/status, system logs, and current configuration. The administrator can also reconfigure, reset or power off / on the server; or execute off-line diagnostics to further analyze the condition of the server. The available functionality depends on the availability of the ISC tools (Platform Instrumentation Control [PIC], Direct Platform Control, etc.) based on the current state of the server.

The format of the traps that are generated by the Platform Event Paging feature is based on the standard Platform Event Trap (PET) format¹ approved by the Intel® Wired for Management (WfM) 2.0 specifications.

¹ The PET format specification is available from the IPMI web site <http://developer.intel.com/design/servers/ipmi>

Pages can be configured for the following events:

- Temperature sensor out of range
- Voltage sensor out of range
- Chassis intrusion (security violation)
- Power supply fault
- BIOS: Uncorrectable Error Correcting Code (ECC) error
- BIOS: POST error code
- Fault Resilient Boot (FRB) failures (**Note:** The page will be repeated for each successive FRB time-out until the log limit is reached.)
- Fatal Non-Maskable Interrupt (NMI) from a source other than front panel NMI or an uncorrectable ECC error
- Watchdog timer reset, power down, or power cycle
- System restart (reboot)
- Fan failures

2. Page Configuration

The Baseboard Management Controller maintains an event filter table that is used to select the events that will trigger a page. Platform Event Filtering provides a flexible, general mechanism that enables the BMC to perform selectable actions triggered by a configurable set of platform events. The BMC initiates a page when an event matches one of the filters. System event entries are predefined to match the events that are enabled or disabled in BIOS Setup for IA 32 based server systems.

2.1 Platform Event Manager Add-In

The Platform Event Manager (PEM) lets you configure the following:

- **Platform Event Paging (PEP)**—pages you to notify you of events on the server.
- **BMC LAN Alert (LAN)**—sends a LAN alert to notify you of events on the server.
- **Emergency Management Port (EMP)**— analog modem configuration and numbers on the server.

2.1.1 Platform Event Manager Window

The PEM main window is shown in the figure below.

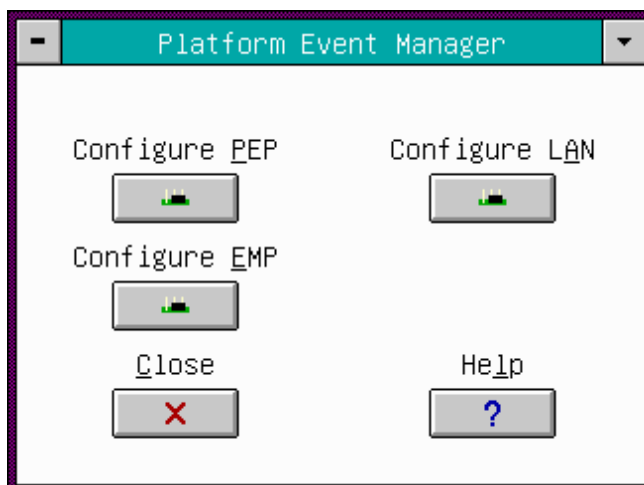


Figure 10-1. Platform Event Manager Main Window

2.1.1.1 Buttons

- **Configure PEP:** Opens a new dialog that allows you to configure the Platform Event Paging features.
- **Configure LAN:** Opens a new dialog that allows you to configure the BMC LAN Alerts features, and general NIC1 supported DPC/CSSU LAN connections.

- **Configure EMP:** Opens a new dialog that allows you to configure the Emergency Management Port features.
- **Close:** Exits the Platform Event Manager and returns you to the AF.
- **Help:** Displays help information.

2.1.1.2 Platform Event Paging Dialog

This dialog allows you to configure the Platform Event Paging features. See the figure below.

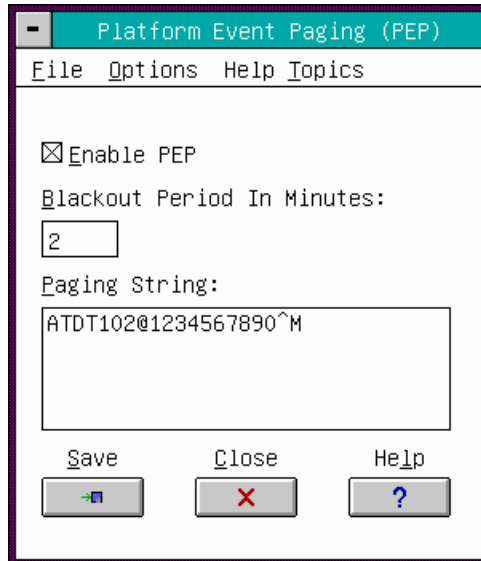


Figure 10-2. Platform Event Paging Dialog

2.1.1.3 File

The File menu has the following options:

- **Save:** Allows you to save the configuration immediately.
- **Close:** Closes the Platform Event Paging dialog without saving changes. If changes have been made, you will be prompted to save changes before closing.

2.1.1.4 Options

The Options menu has the following options:

- **Enable PEP:** Toggles the PEP feature on or off. A check appears next to the menu item when PEP is enabled.
- **Send Alert:** Sends a test page with the configuration currently shown on the screen.
- **Configure Event Actions:** Launches the Platform Event Paging Actions Dialog.

2.1.1.5 Help Topics

The Help Topics menu has the following options:

- **Help Topics:** Displays help information.

2.1.1.5.1 Enable PEP Checkbox

Enable or disable the PEP feature entirely.

2.1.1.5.2 Blackout Period in Minutes

Enter the time, in minutes, between successive pages. The valid range is [0 - 255] where 0 disables the blackout period.

2.1.1.5.3 Paging String

Enter the paging string that contains both the paging service number and the characters that are sent once the connection has been made. The maximum length for the paging string is determined at run-time from firmware. You will be notified if the string is truncated. The screen will show the string that was saved after a save operation is done.

2.1.1.5.4 Buttons

- **Save:** Allows you to save the configuration immediately.
- **Close:** Closes the Platform Event Paging dialog without saving changes. If changes have been made, you will be prompted to save changes before closing.
- **Help:** Displays help information.

2.1.1.6 Platform Event Action Dialogs

These dialogs allow you to configure the platform event action features for PEP and LAN. The dialogs are identical except for the titles. If an event is in the enabled list box, it generates the appropriate action when it occurs. If an event is in the disabled list box, it does not generate an action when it occurs. A page or LAN alert is sent only if both of the following are true:

- The event is enabled in the platform event actions dialogs
- Platform Event Paging and LAN Alerts are enabled in the corresponding dialogs

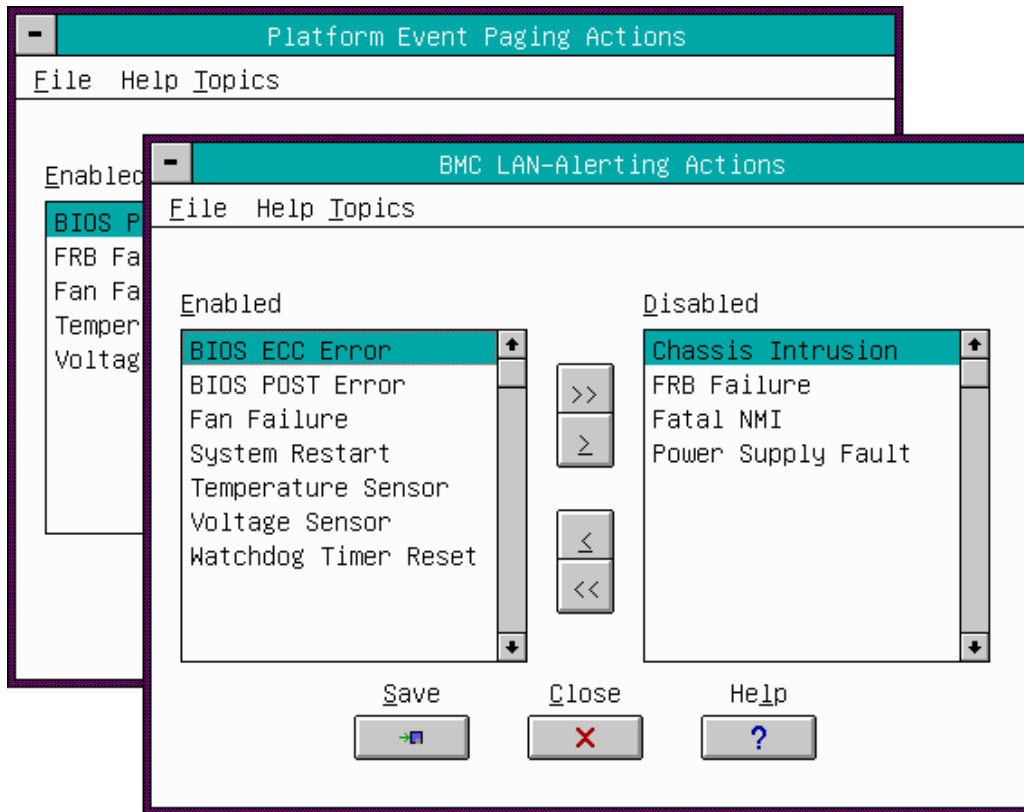


Figure 10-3. Platform Event Action Dialogs

2.1.1.6.1 File Menu

The File menu has the following options:

- **Save:** Allows you to save the configuration immediately.
- **Close:** Allows you to close the Platform Event Action dialog without saving changes. If you have made changes, you will be prompted to save changes before closing.

2.1.1.6.2 Help Topics Menu

The Help Topics menu has the following options:

- **Help Topics:** Displays help information.

2.1.1.6.3 Enabled Listbox

Lists events that generate actions.

2.1.1.6.4 Disabled Listbox

Lists events that do not generate actions.

2.1.1.6.5 Buttons

- **>>**: Moves all events from the enabled list box to the disabled list box.
- **>**: Moves the selected event from the enabled list box to the disabled list box.
- **<**: Moves the selected event from the disabled list box to enabled the list box.
- **<<**: Moves all events from the disabled list box to the enabled list box.
- **Save**: Allows you to save the configuration immediately.
- **Close**: Closes the dialog without saving changes. If you have made changes, you will be prompted to save changes before closing.
- **Help**: Displays help information.

This page intentionally left blank

Intel® Server Control, Version 3.x TPS

Section 11: LAN Alerting

Table of Contents

1. Introduction to LAN Alerting	1
2. Hardware Interface	2
3. Configuration	3
4. Client Address Resolution	5
5. Platform Event Filtering and LAN Alert	6
5.1 Event Record Data	6
6. SNMP Trap Format Used for LAN Alerts	8
6.1 Header	8
6.2 Protocol Data Unit (PDU)	8
6.3 Variable Bindings Field.....	9
7. LAN-Alert Sequence	11
8. LAN-Alert Viewer	12
8.1 Alert Viewer	12
8.2 Program Menu	13
8.3 Tray Status Reporting Icon.....	14
8.4 View Details Dialog	14
8.5 Configure Dialog	15

List of Figures

Figure 11 - 1: Hardware Interface..... 2

Figure 11 - 2: IP-UDP Packet in Ethernet Network..... 5

Figure 11 - 3: LanAlert Viewer..... 12

Figure 11 - 4: Windows Program Menu..... 13

Figure 11 - 5: Status Icon..... 14

Figure 11 - 6: LanAlert Viewer - Alert Details..... 14

Figure 11 - 7: LanAlert Configuration 15

Figure 11 - 8: Alert Notification Dialog 15

List of Tables

Table 11 - 1: SEL Event Record (Type 02h) Format 6

Table 11 - 2: Trap PDU format used by LAN-Alert per RFC 1157 8

Table 11 - 3: Variable Bindings Fields 9

Table 11 - 4: LanAlert Viewer - User Controls 13

Table 11 - 5: Configure Dialog - Options 15

1. Introduction to LAN Alerting

Local Area Network (LAN) Alerting is a new feature of Intel Server Control (ISC) v3.x. The objective of the LAN notification feature is to send alerts for critical system failures to the remote system administrator regardless the state of the host server's operating system. This functionality is similar to Platform Event Paging however the alerts are sent across the LAN/Wide Area Network (WAN).

LAN alerting relies on the Baseboard Management Controller (BMC), which is built into the server baseboard. The BMC runs independently of the system processors and the system operating system. The BMC monitors platform health and critical failures and collects the events into the System Event Log (SEL). The network interface from the BMC is provided through the Server Management Bus (SMBus) or Total Cost of Ownership (TCO) port interface of the on-board 82559-network interface controller (NIC). LAN alerting is dependent on this interface of the 82559 to the BMC to send alerts over the network.

The alerts are generated as a Simple Network Management Protocol (SNMP) Trap and sent over the LAN using User Datagram Protocol/Internet Protocol (UDP/IP) to remote management clients. The trap structure is based on the *Platform Event Trap Format Specification v1.0*, which is part of the Intelligent Platform Management Interface (IPMI) suite of specifications.

Platform Event Filtering (PEF) is a feature, which provides versatility for the user by implementing a filter table, which consists of up to 16 configurable entries. The user has the ability to select which events will cause LAN alert messages and which ones will not. When any event is generated, PEF compares event record fields against the filter entries in the table and on match, triggers the alert. PEF only determines which events will generate the alert and does not impact the recording of all events in the SEL by the BMC.

2. Hardware Interface

The BMC on triggering of critical event sends an alert in SNMP (Version 1) Trap format over network to the interested recipients. The 82559 NIC populated on the baseboard, provides a network path to the BMC through its dedicated Total Cost of Ownership (TCO) port. The BMC communicates with TCO port of 82559 over a private I²C bus. The 82559 asserts the SMBALRT# signal to indicate that it has the data to be received. In response, the BMC reads data from the 82559 using 'receive' protocol. The BMC transmits a network packet using 'transmit' protocol provided by the 82559-command interface over the I²C bus.

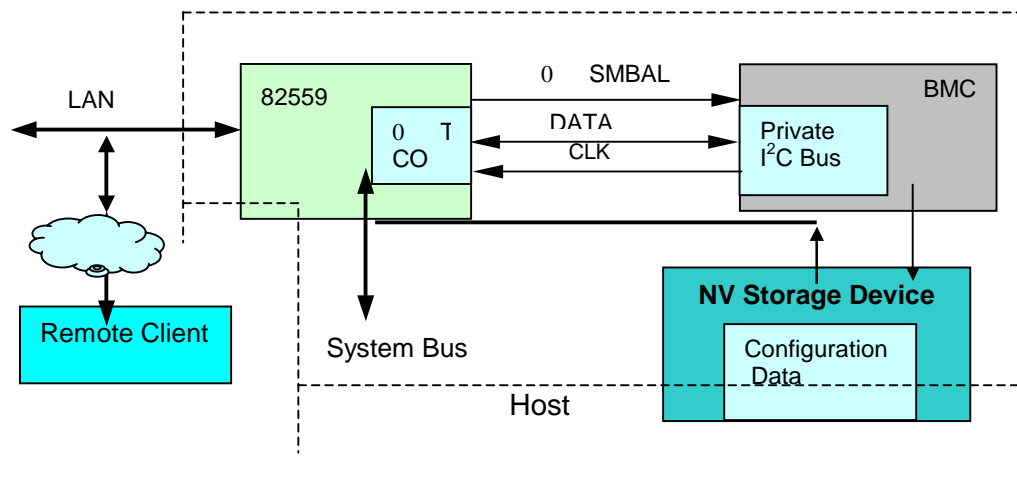


Figure 11 - 1: Hardware Interface

The System Setup Utility (SSU) and Client System Setup Utility (CSSU) provide configuration and setup of the BMC for LAN alerting. The SSU, CSSU and system software use the system bus to communicate the configuration messages to the BMC using the BMC's host interface. On reception of these messages the BMC stores the relevant parameters in the Field Replaceable Unit (FRU) internal use area of its non-volatile storage device. The configuration changes take effect immediately. Re-initialization of the BMC is not required. During power up or after a system reset, the BMC reads the Non Volatile (NV) device to retrieve those parameters required for LAN alert implementation.

3. Configuration

In order to communicate with a remote alert recipient the BMC requires that several network specific configuration parameters and trap specific parameters be set. The BMC stores these parameters in the non-volatile storage device. The user interface is used to configure the Alert destination Internet Protocol (IP) Address and Community String parameters. The other parameters are not visible to the user and need no user input.

Configurable parameters are listed as below:

- **Global Unique Identifier (GUID)** (16 bytes):
This is the same as what is stored in the Preboot Execution Environment (PXE) option RAM. The BMC uses IP address and GUID as its identity and sends as a part of the alert message information. This supports client's (alert recipient) task of host identification.
- **Universal Time Coordinated (UTC) Offset** (2 bytes):
This is the time-zone specific information. The BMC needs this as a part of the Alert information it sends.
- **Host IP Address** (4 bytes):
This is the Logical or Internet Address of the host. The BMC needs this information to send an alert packet over the network. The SSU/CSSU/Platform Instrumentation (PI) software provides this configuration to the BMC. In case of dynamic IP address assignment environment such as Dynamic Host Configuration Protocol (DHCP), the BIOS supports the BMC coherency with the dynamically assigned address.

Note: If the NIC is part of a teaming or fail-over pair that uses DHCP, ISC may not be able to synchronize the BMC with the operating system network configuration information. Do not use the server management assigned NIC as part of the teaming pair. Instead, install an add-on NIC for use as the part of the teaming or fail-over pair or Use a static IP address for the server's server management assigned NIC if it is to be included in a teaming or fail-over pair.
- **Host Media Access Control (MAC) Address** (6 bytes):
Physical Ethernet / link-layer address of the host. The BIOS needs to provide this information to BMC, as BMC does not have access to the 82559 EEPROM configuration.
- **Subnet Mask** (4 bytes):
This is the host's (BMC) subnet mask. The BMC uses this to identify whether the alert destination is in the local subnet or in the other subnet relative to the BMC.
- **Router IP Address** (4 bytes):
This is the logical address of the router or default gateway. In case of the alert destination residing in different subnet relative to the host/BMC, the BMC sends a packet to its default gateway. The router / default gateway then takes care of forwarding or direct delivery to the actual destination.

- **Router MAC Address** (6 bytes):
Physical Ethernet / link-layer address of the router or default gateway. The BMC uses this to send the packet to the router. This is needed by the BMC, as it does not perform Address Resolution Protocol (ARP).
- **Alert Destination IP Address** (4 Bytes):
This is the logical or Internet address of the Alert-Destination. In case of single node destination this is the unicast or specific IP address. This is the IP Subnet address if the alert needs to be broadcasted (instead of a unicast destination) within particular subnet.
- **Community String** (5-16 bytes):
This is a null terminated string that can be configured for the community field in the Header section of the trap. The BMC maintains 'public' as the default string.

4. Client Address Resolution

The BMC sends a LAN-Alert in SNMP-Trap format to the remote client / alert-destination over network (Ethernet). SNMP-Trap uses Universal Datagram Packet (UDP) as a transport layer protocol over IP as a network layer protocol.

The 82559 provides the network interface to the BMC through the SMBus. The BMC sends or receives data packets at the Link-layer and hence it needs to implement link layer protocol in addition to higher layer protocols. Thus, while sending any data packet BMC forms the complete Ethernet frame by adding Ethernet header, IP header and UDP header to the actual data.

The Ethernet header consists of three components: destination physical address, source physical address and the frame type. At the IP layer, the nodes are identified with logical addresses. The ARP (Address Resolution Protocol, at the link layer) provides a mechanism for mapping logical address to physical address.

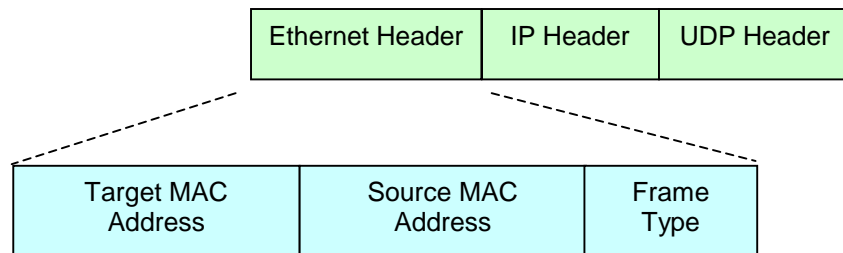


Figure 11 - 2: IP-UDP Packet in Ethernet Network

The BMC takes following steps while sending an alert:

- If the alert destination is within the same subnet, the BMC sends the link-layer broadcast of the Alert.
- If the alert destination is in another subnet, the BMC uses the MAC address of the router stored in NV storage device to send an Alert.

5. Platform Event Filtering and LAN Alert

The BMC maintains an event filter table that can be used to select an event and the associated action. On reception of any event the BMC compares it against the table entries and on match takes the associated action. Accordingly if the action for the event is a LAN alert, it registers a request for alerting with event data as input. The Alert implementation maps the event data to the Platform Event Trap format and sends an SNMP-Trap to the destination.

Following events can be selected for sending an Alert:

- Temperature Sensor out of range
- Voltage Sensor out of range
- Fan Failure
- Chassis Intrusion (Security Violation)
- Power Supply Fault
- BIOS (Server Management Interrupt [SMI] Handler): Uncorrectable Error Correcting Code (ECC) error
- BIOS: POST Error Code
- FRB Failures
- Fatal Non-Maskable Interrupt (NMI) (from source other than Front Panel NMI or Uncorrectable ECC Error).
- Watchdog Timer reset, power down, or power cycle
- System restart (reboot)

5.1 Event Record Data

The following table summarizes the fields of an event record as recorded in the System Event Log and as defined in the IPMI specification. These fields are the input to the platform event filtering process.

Only those events with the following field configuration are currently filtered.

'Type 02h' and EvM Rev = 90h or 01h

Table 11 - 1: SEL Event Record (Type 02h) Format

Byte	Field	Description
1-2	Record ID	ID used for SEL Record access
3	Record Type	02h = system event record
4-7	Timestamp	Time when event was logged

Byte	Field	Description
8-9	Generator ID	RqSA & Logical Unit Number (LUN) if event was generated from IPMB. Software ID if event was generated from system software. <u>Byte 1</u> 7:1 7-bit I ² C Slave Address, or 7-bit system software ID 0 0=ID is IPMB Slave Address, 1=system software ID <u>Byte 2</u> 7:2 reserved. Write as '0'. Ignore when read. 1:0 Intelligent Platform Management Bus (IPMB) device LUN if byte 1 holds Slave Address. 00b otherwise.
10	EvM Rev	Event Message format version
11	Sensor Type	Sensor Type Code for a sensor that generated the event
12	Sensor Number	Number of a sensor that generated the event
13	Event Type	Type of trigger for the event, e.g. critical threshold going high, state asserted, etc. Also indicates class of the event. E.g. digital, discrete, or 'analog'. The Event Type field is encoded using the Event/Reading Type Code. See IPMI Specification Event/Reading Type Codes table.
14	Event Data 1	FFh if data byte not provided.
15	Event Data 2	FFh if data byte not provided.
16	Event Data 3	FFh if data byte not provided.

6. SNMP Trap Format Used for LAN Alerts

This section describes the format of the various fields of the Platform Event Trap (PET) from the BMC's perspective. Refer to the [Platform Event Trap Format Specification v1.0](#) for more generic details. The Alert implementation in the BMC encodes the trap fields and bundles them into Type-Length-Value format.

The specific trap and 'variable-bindings' field encodes the actual Alert information for the alert-recipient.

6.1 Header

The trap header consists of the following two fields.

- **Version** Simple Network Management Protocol (SNMP), Revision 1
- **Community String** Configurable by the user. Default is 'public'.

6.2 Protocol Data Unit (PDU)

The trap PDU fields are described in the following table.

Table 11 - 2: Trap PDU format used by LAN-Alert per RFC 1157

Field	Description
Enterprise	OID = 1.3.6.1.4.1.3183.1.1
Agent-addr	Network Logical address / Internet Address (IP)
Generic-trap	Enterprise Specific (6)
Specific-trap	<p>32 bits Integer. The BMC encodes this field as below.</p> <p>31:24 0000 0000b</p> <p>23:16 <u>Event Sensor Type</u> The Event Sensor Type field indicates what types of events the sensor is monitoring. 'Sensor Type' field of the event message</p> <p>15:8 <u>Event Type</u> 'Event Type' field of the event message</p> <p>7:0 <u>Event Offset</u> Indicates which particular event occurred for a given Event Type.</p> <p>7 0 = Assertion Event. (Event occurred when state became asserted) 1 = Deassertion Event.</p> <p>6:4 reserved. 000b.</p> <p>3:0 'Event Data 1' of the event message . 0Fh = unspecified.</p>
Time-stamp	Time elapsed between last (re) initialization of the network entity and the generation of the trap. The unit is 1/100 th of a second. The BMC initializes this timer when it receives a request from the BIOS to log a system boot.
Variable-bindings	Defined below

Offset	Name	Size	Description
30	Entity	Byte	Entity ID from IPMI v1.0 specification. Indicates the platform entity the event is associated with - e.g. processor, system board, etc. The BMC leaves this field unspecified. 00h = unspecified.
31	Entity Instance	Byte	Indicates which instance of the Entity the event is for. E.g. processor 1 or processor 2. The BMC leaves this field unspecified. 00h = unspecified.
32:39	Event Data	8 Bytes	Other event specific information. The BMC maps this to 'Event Data 1', 'Event Data 2' and 'Event Data 3' of the event message. Rest 5 bytes are padded with FFh.
40	Language Code	Byte	Per IPMI v1.0 FRU Information Format. FFh = unspecified.
41:44	Manufacturer ID	Dword 4 Bytes	Manufacturer ID using Private Enterprise IDs per Internet Assigned Numbers Authority (IANA). The BMC uses this from FRU.
45:46	System ID	Word 2 Bytes	This number can be used to identify the particular system/product model or type. The BMC returns same as the product-Id field in the application command GetDeviceId.

7. LAN-Alert Sequence

The following steps outline the process of sending an alert over LAN.

During initialization

1. The LAN Alert implementation retrieves certain configuration information from the Non-Volatile storage that is required to construct a trap message. At run-time, any changes in this configuration information caused by BMC command processing immediately take effect.

During run-time

1. The PEF implementation in the BMC issues a LAN-Alert request and passes the SEL message as input information.
2. The LAN Alert implementation in the BMC pushes the event message in its message queue.
3. The Alert Task pops the event data message from the queue and uses it to build a Trap message per the PET format. The variable-bindings field of the trap Message contains most of the event specific information.
4. Alert task encodes all the trap information and bundles it into SNMP specific Type-Length-Value format.
5. Alert task constructs an IP-UDP packet with an alert recipient as the target address.
6. Alert task sends a packet to the Ethernet controller (82559) over the SMBus.
7. The 82559 sends the packet (Trap) over the network.
8. The alert recipient decodes the trap fields specifically the variable binding field to know more about the alert event.

8. LAN-Alert Viewer

The LAN Alert viewer is a new application under the Intel Server Control family. It is a Win32* applet that is used to receive and view the alert traps generated by the remote server system. The applet may be installed as a stand-alone application or on the same console as the Direct Platform Control or Client System Setup Utilities.

8.1 Alert Viewer

The following figure shows a sample of how the LAN Alert viewer displays important fields as decoded from the SNMP trap.

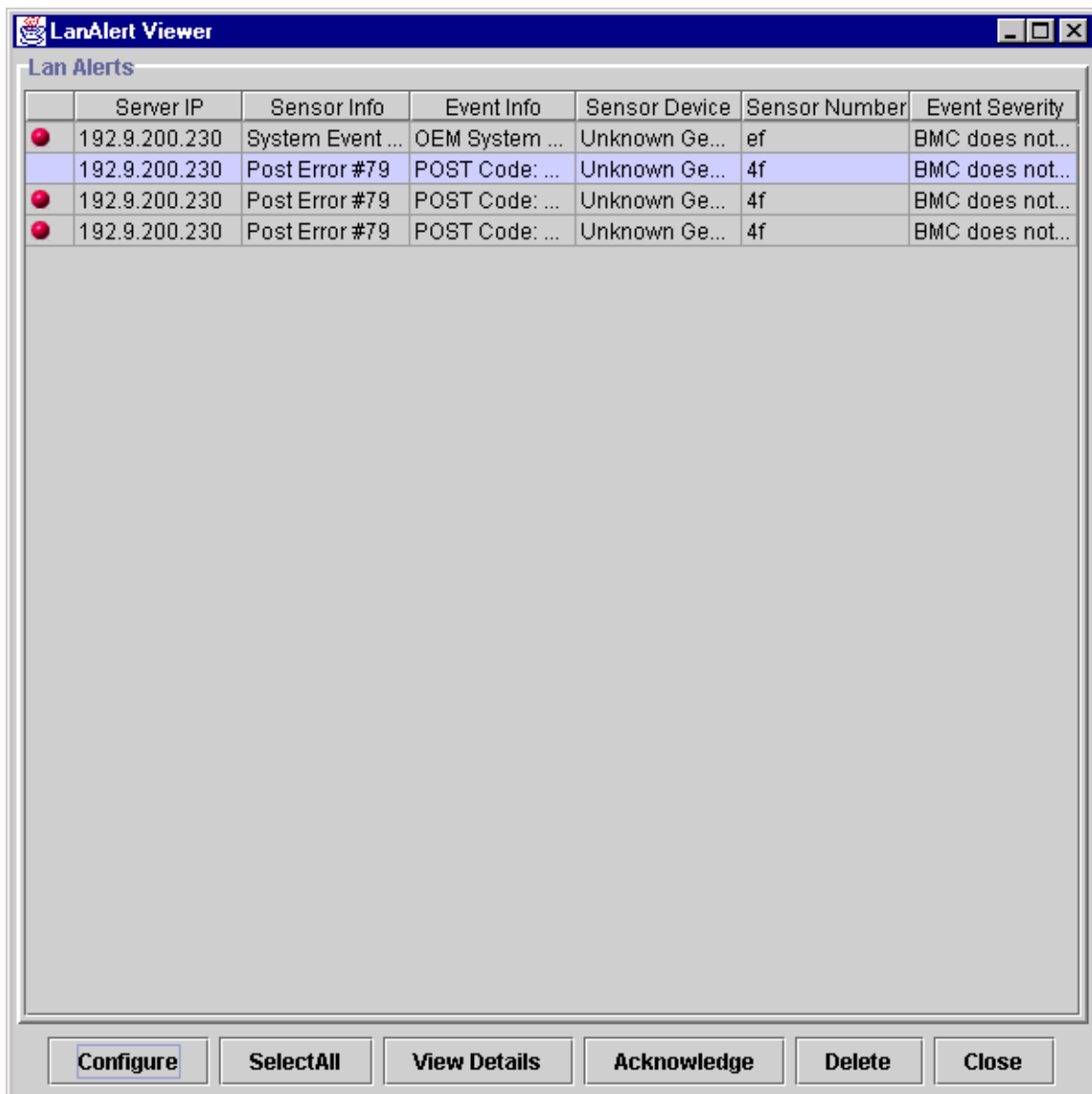


Figure 11 - 3: LanAlert Viewer

The following table describes the User controls available from the LAN Alert Viewer utility.

Table 11 - 4: LanAlert Viewer - User Controls

Option	Description
Configure	This launches the LAN Alert configuration dialog which allows the user to configure different notification and viewer options
Acknowledge	This sets the selected alerts' "status" to acknowledge. This means the user has seen/aware of the alert. The red icon will be removed from the first field for acknowledged alerts.
Delete	Delete removes the selected alert from the list of alerts.
Close	This closes the viewer
Select All	This selects all alerts; this will help the user in performing delete and acknowledge operations.
View Details	This will launch the detailed view of the selected alert(s), which will have all the information about the selected alerts.

8.2 Program Menu

User can launch the LAN Alert Viewer either from the Windows* program menu or by double clicking the status icon in the system tray. All the unacknowledged alerts will have a red icon associated with it in the first column. Once an alert has been viewed the red icon will be removed.

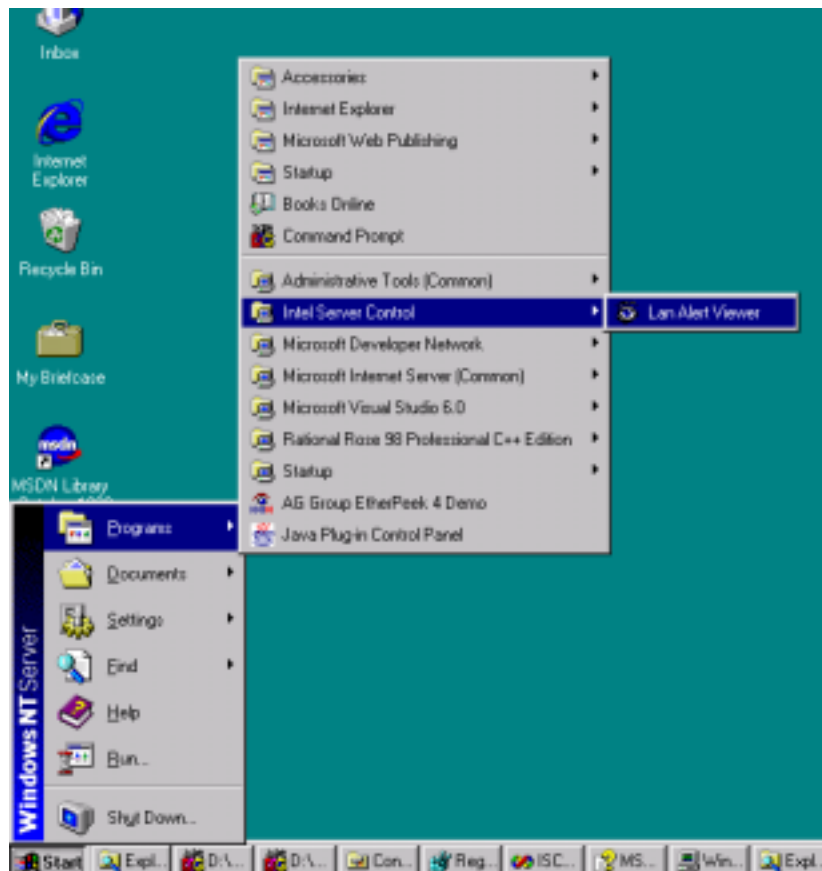


Figure 11 - 4: Windows Program Menu

8.3 Tray Status Reporting Icon

A status icon is displayed in the system tray when LAN Alert manager is running, as shown below. The icon will show as Green when no unacknowledged alerts are present and will show as Red when new alerts have not been viewed.



Figure 11 - 5: Status Icon

When an alert comes in, the status icon will start to flash (changes between red and green).

Users will be able to launch the viewer by double clicking on the icon at any time. When all alerts in the viewer are acknowledged the icon goes back to the normal state (green)

8.4 View Details Dialog

The following figure displays the detailed information presented with the “View Details” option is selected. All of the displayed information follows the Platform Event Trap Specification and is decoded from the SNMP Trap.

Name	Value
Event Severity	BMC does not specify event severity
Server IP	192.9.200.230
Sensor Number	4f
Sensor Device	Unknown Generator ID - LUN #0
Sensor Info	Post Error #79
Event Info	POST Code: 0xF0 0x0D 0x81
Event Source Type	IPMI
SNMP TimeStamp	0 : 0 : 42
Local TimeStamp	
Trap Source	BMC
Generic Trap	6
Sequence Cookie	0
UTC Offset	22068
Entity	BMC does not specify alert entity
Entity Instance	BMC does not specify alert entity instance
Var Bind Name	1.3.6.1.4.3183.1.1.1
Enterprise	1.3.6.1.4.3183.1.1
Community	public
System ID	256
Manufacture ID	1459683328
Platform GUID	123456789abcdef10
Language	Default
Version	1.0

Figure 11 - 6: LanAlert Viewer - Alert Details

8.5 Configure Dialog

The User has the option to configure how event alerts will be displayed.

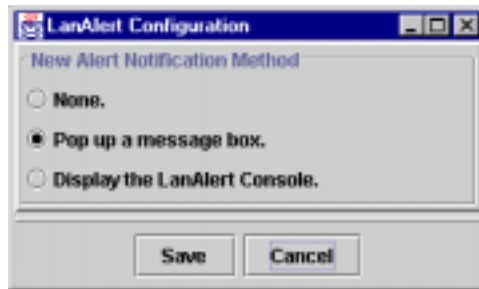


Figure 11 - 7: LanAlert Configuration

The Configuration dialog box allows the user to configure alert notification methods.

Table 11 - 5: Configure Dialog - Options

Options	Description
None	There won't be any notification to the user other than the flashing sys tray icon. If the user wants to see the alert will have to launch the viewer from the program menu or by double clicking the tray icon.
Pop up message box	If this is s, a dialog box will be displayed on the arrival of a new alert (Fig xxx.1).
Display the LAN Alert Viewer console	If this is set the alert viewer will be launched on the arrival of the new alert and will be made the active window.

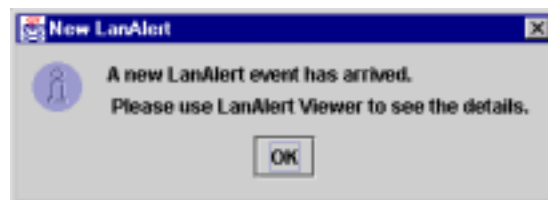


Figure 11 - 8: Alert Notification Dialog

This page intentionally left blank

Intel® Server Control, Version 3.x TPS

Section 12: Install and Uninstall

Table of Contents

- 1. Introduction to Install and Uninstall..... 1
- 2. Supported Operating Systems 2
- 3. Internationalization..... 3
- 4. Recommended Files and Registry Tree Structures 4
 - 4.1 Source Files 4
 - 4.2 Windows Registry 4

List of Figures

No figures appear in this section.

List of Tables

No tables appear in this section.

1. Introduction to Install and Uninstall

This section describes the installation environment for ISC in those instances where Intel® Server Control (ISC), Desktop Management Interface (DMI) 2.0 SP, Explorer browser, and the Managed Object Toolkit (MOT) are installed.

ISC provides installation and de-installation routines. During installation, all ISC ActiveX* controls are registered, icons are created, and files are copied. If the de-installation process is used, the opposite occurs – controls are unregistered, and icons and files are deleted.

Note: The user must have administrative or equivalent rights to install ISC onto a server for NetWare*, Windows NT*, and UnixWare*.

The ISC installation supports the following objectives:

- Auto-detection, installation and operation under Management Consoles
 - LANDesk® Server Manager 6.1
 - HP* OpenView* Network Node Manager 6.1 (Windows NT version)
 - CA Unicenter* TNG* Framework 2.21 (Windows NT version)
 - No console (ISC Stand-alone)
- Installation of DMI 2.0 Service Providers (Win32*, NetWare, UnixWare)
- Installation of DMI 2.0 Browser (Explorer)
- Installation of Managed Object Toolkit (MOT)
- Extensibility, Customization. The ISC installation framework does not have specific knowledge about the applications that it is installing. In order to be installed by the framework, owners of individual components (e.g. Client SSU, PIC, PI and/or OEMs) create configuration files to describe the necessary steps to install that component on a system. OEMs can customize the ISC installation by modifying the configuration files provided and by inserting their own configuration files.
- The same interfaces across supported OSs. In the past, each supported OS had its own installation structure. In order for a component to be installed on several OSs, source code often had to be modified. The installation framework simplifies the process by using configuration files with the same format across OSs. However, component owners will need to provide a set of configuration files for each OS because they require different installation steps (e.g. No registry on NetWare or UnixWare).

The remote installation of console / server components. ISC's installation framework can install Win32 components (consoles or server) on local or remote systems. Red Hat Linux, NetWare or UnixWare components *must* be installed remotely, but the installer will need access to the Linux / NetWare / UnixWare server to start the Local Setup process. This is not required on Win32 systems where the Local Setup process can be started remotely from the installation console.

2. Supported Operating Systems

The Installation Console supports Windows 98, Windows NT 4.0, and Windows 2000. Remote target systems can be Windows NT 4.0, Windows 2000, NetWare 4.2, NetWare 5.1, Red Hat Linux 6.2 SBE2, and UnixWare 7.1

3. Internationalization

The installation console determines the local machine language and will load the appropriate resources files. If there are no resources associated with the current language, US English resources are loaded by default.

4. Recommended Files and Registry Tree Structures

4.1 Source Files

Although there are no restrictions on where applications installed by ISC should place their binaries, it is recommended that all files be copied into `%ISCPATH%\bin` (on Win32 platforms). The directory will be added to the system path.

4.2 Windows Registry

The Intel Server Control Windows Registry tree structure will have the following format:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Intel
      \Server Control
        \Console
        \Server
```

All ISC console and server applications should create registry entries under their respective branch (`\Console` or `\Server`).

Example:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Intel
      \Server Control
        \Console
          \DPC
          ...
          \Phone Book
          ...
          \PIC
          ...
          \StandAlone
          ...
          \Client SSU
          ...
        \Server
          \PI
```

Intel® Server Control, Version 3.x TPS

Section 13: Common Interface

Table of Contents

1. Introduction to the Common Interface	1
1.1 ISC Instrumentation Controls	1
1.2 ISC Core Components	1
1.3 DMI Managed Object Toolkit (MOT) Engine.....	2
1.4 DMI Managed Object Toolkit (MOT) Engine.....	2
1.5 Navigator Container	2
2. FRU Implementation	3
2.1 Screen Display	3
2.1.1 Navigation Pane	3
2.1.2 Presentation Pane.....	4
2.1.3 Description	4
2.1.4 Container Functionality.....	5
2.1.5 Supported Commands	5
2.2 Available FRU Information.....	6
3. SDR Implementation	7
3.1 Screen Display	7
3.2 Navigation Pane	7
3.2.1 Display Name Rules for Sensor Record	7
3.3 Presentation View	8
3.4 Description	9
3.5 Container Functionality.....	10
3.5.1 Supported Commands	10
4. SEL Implementation	12
4.1 Screen Display	12
4.2 Viewer	12
4.3 Container Functionality.....	13
4.3.1 Supported Commands	13
4.4 Available Information.....	14
5. RSA Implementation	15
5.1 Screen Display	15
5.2 Available Information.....	16

List of Figures

Figure 13 - 1: FRU Manager	3
Figure 13 - 2: SDR Grid.....	9
Figure 13 - 3: SDR Properties Dialog	11
Figure 13 - 4: SEL Manager	12
Figure 13 - 5: SEL Properties Dialog.....	14
Figure 13 - 6: RSA Manager Options Dialog	15
Figure 13 - 7: RSA Manager - View 1.....	16
Figure 13 - 8: RSA Manager - View 2.....	16

List of Tables

Table 13 - 1: Presentation Pane Information Available.....	4
Table 13 - 2: FRU Manager File Commands.....	5
Table 13 - 3: Available FRU Information.....	6
Table 13 - 4: SDR Tree View Details.....	8
Table 13 - 5: SDR Grid Fields	9
Table 13 - 6: SDR Menu - Supported Commands	10
Table 13 - 7: SEL Menu - Supported Commands.....	13

1. Introduction to the Common Interface

This chapter describes common GUI features of ISC 3.0. The GUI is implemented in three different ways: for the FRU, SDR, and SEL. This chapter provides an overview of each of these implementations.

Regardless of the implementation, the architecture of the ISC GUI consists of four major components:

- ISC Instrumentation Controls
- ISC Core Components
- DMI Managed Object Toolkit (MOT) Engine
- Navigator Container

Each of these is discussed below.

1.1 ISC Instrumentation Controls

The ISC Instrumentation Controls User Interface (UI) consists of ActiveX* components that are required to interface ISC functionality with the user. The ISC UI Controls interact with core components in the console to obtain the current values that are displayed on the screen and to change values set by the user. The UI Controls allow users to configure sensor thresholds and provide detailed sensor information.

The health icon and screen within the UI is dynamically updated to show the current state of the server. The UI also updates the current screen when changes are applied. A refresh menu item allows the user to update the screens with the latest values.

1.2 ISC Core Components

The ISC Core is the interface between the ActiveX component layer and the transport layer. The ActiveX control components do not communicate with the Managed Object Toolkit (MOT) control, but rather through the ISC Core components.

The ISC Core interfaces with the following components:

- ISC executable: Navigator, ICMB, and health functions.
- ActiveX controls: to display and change object attributes.
- ICLW SM Abstraction layer: APIs for obtaining machine OS type.
- MOT (DMI Object Model): used to get and set information for DMI attributes.
- ISecurity control: common security functionality for checking user authorization.
- A path list of all rows in all components for a given group.

1.3 DMI Managed Object Toolkit (MOT) Engine

The DMI Managed Object Toolkit Engine provides access from the console to the server's DMI Service Provider. The MOT Engine is an ActiveX control that provides a connection to the server and transportation of DMI data to and from the server.

1.4 DMI Managed Object Toolkit (MOT) Engine

The DMI Managed Object Toolkit Engine provides access from the console to the server's DMI Service Provider. The MOT Engine is an ActiveX control that provides a connection to the server and transportation of DMI data to and from the server.

1.5 Navigator Container

The Navigator container provides access to the ISC features, a toolbar, and other menu items. The purpose of the Navigator is to map the list, toolbar, and menu items to an ISC control that is launched when an item is selected. The system default settings are used for the window size, the position on the desktop, the font, and other screen information.

2. FRU Implementation

When the FRU Manager is started, a Status Box is displayed to indicate that the manager is loading Field Replaceable Unit information from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If the server is connected when the FRU Manager is launched, a Connect Dialog Box will appear. This box also has a Cancel button.

2.1 Screen Display

The FRU Manager conforms to the Microsoft Windows Explorer-like model, with a Navigation Pane, a Presentation Pane and a description area. The individual panes and data columns can be resized by using a split bar.

The FRU Manager is an ActiveX control. This means it can be used across several server management applications. A sample screen shot of the FRU Manager user-interface is shown below.

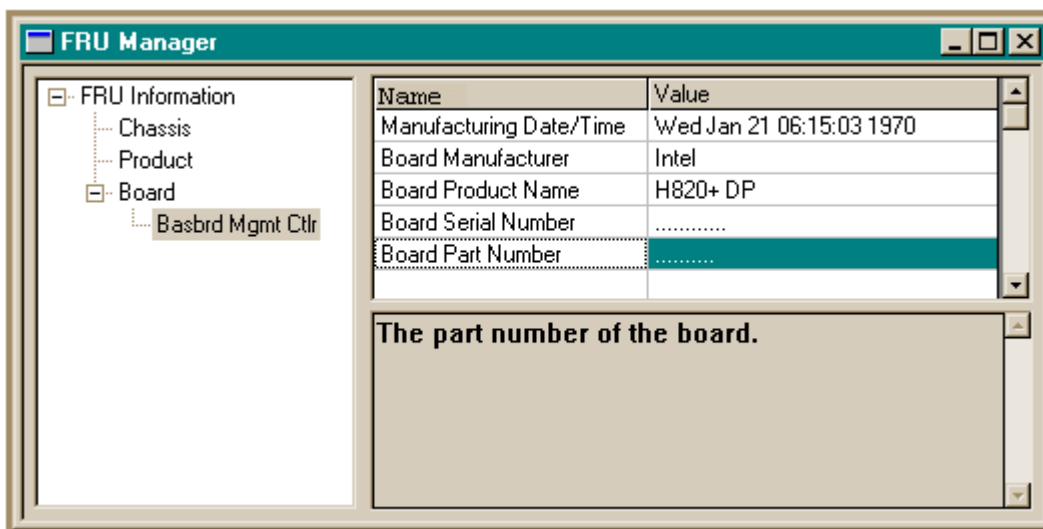


Figure 13 - 1: FRU Manager

2.1.1 Navigation Pane

The Navigation Pane is implemented with a Tree View (hierarchical). The root of the Navigation Pane is "FRU Information," under which the information areas are displayed. Information areas available in the FRU implementation include Chassis, Product, and Board.

Under the Product category, all devices with Product Area information are enumerated as child nodes. A listing of the devices available on the server must be obtained from the Device Locator Records in the Sensor Data Record Repository. There is no logical grouping defined for the display of these areas and devices. For the convenience of the user, items within each logical group may be presented in a sorted order.

2.1.2 Presentation Pane

The Presentation Pane on the top right side of the screen consists of a Grid View for displaying attributes of the node selected from the Navigation Pane.

The Presentation Pane is modeled after an attribute-value paradigm, wherein the attributes of the device selected from the Navigation Pane are displayed in a three-column format. Only those attributes that have meaning from a user's point of view will be displayed here. The following are the fields that may be displayed in the Presentation Pane.

Table 13 - 1: Presentation Pane Information Available

Option Selected from Navigation Pane	Fields Displayed in Presentation Pane
Chassis	Chassis Type (Interpret and display this field) Chassis Part Number Chassis Serial Number
Product	Manufacturer Name Product Name Product Part Number Product Version Product Serial Number Asset Tag
Board	Manufacturing Date/Time (Interpret and display this field) Board Manufacturer Board Product Name Board Serial Number Board Part Number

The Attribute frame describes in the category of the information that is displayed and the Value frame provides specific information for that category. For example, if the Attribute contains "Serial Number" the Value contains the actual serial number information.

2.1.3 Description

As users highlight an attribute name or value in the Presentation Pane, the corresponding attribute description is displayed in the description text box under the Presentation Pane. For ISC 2.x the description box will remain static.

2.1.4 Container Functionality

PIC, DPC and SSU will provide functionality that is generic to the FRU manager, such as the file menu.

2.1.5 Supported Commands

ISC enables and disables specific UI controls to make supported commands available. The commands are implemented as menu selections of the control container.

File	Open...
	Save As...
	Print...
	Exit
FRU	Reload
Help	

2.1.5.1 File Commands

Table 13 - 2: FRU Manager File Commands

Command	Description
Open	Open a file. It opens a standard Window's file dialog allowing users to select a file from a directory. Only the opening of a standard FRU formatted file will supported.
Save As	Save the file to a directory. It opens a standard Window's file dialog for saving a file. In all cases, the entire FRU file for that device is saved. Only the information for a specific FRU device is saved to a FRU file at any one time. The FRU information written to a file is in FRU file format, with an extension of ".FRU". The FRU file format is specified by the relevant Non-Volatile Storage Load File Format Specification and the IPMI Platform Management FRU Information Storage Definition.
Print	Generic Win32 Print functionality. This option prints the FRU information, as it would be done in a standard Windows application. Unlike the "Save As" function, this feature will print the information as it is displayed. In addition, the print function will support printing selected leafs and nodes of information.

2.2 Available FRU Information

FRU devices provide inventory information, based on the Intelligent Platform Management Interface specification. The format of the information is divided into six different areas:

Table 13 - 3: Available FRU Information

Area	Description
Chassis Info Area	This area is used to hold Serial Number, Part Number, and other information about the system Chassis. A system can have multiple FRU Information Devices within a chassis, but only one device should provide the Chassis Info Area. Thus, this area will typically be absent from most FRU Information Devices.
Product Info Area	This area is present if the FRU itself is a separate product. This is typically seen when the FRU is an add-in card. When this area is provided in the FRU Information Device that contains the Chassis Info Area, the product info is for the overall system, as initially manufactured.
Board Info Area	This area provides Serial Number, Part Number and other information about the board on which the FRU Information Device is located.
Common Header	The Common Header is mandatory for all FRU Information Device implementations. It holds version information for the overall information format specification and offsets to the other information areas. The other areas may or may not be present, based on the application of the device.
Internal Use Area	This area provides private, implementation-specific information storage for other devices that exist on the same FRU as the FRU Information Device. The Internal Use Area is usually used to provide private non-volatile storage for a management controller.
MultiRecord Info Area	The MultiRecord Information Area provides a region that holds one or more records where the type and format of the information is specified in the individual headers for the records. This differs from the other information areas, where the type and format of the information are implied by which offset is used in the Common Header. The MultiRecord Info Area provides a mechanism for extending the FRU Information Specification to cover new information types without impacting the existing area definitions.

The FRU Manager will display only the information useful to the end-user from the Chassis, Board and Product information areas. The Common Header, Internal Use or MultiRecord information areas are not displayed.

3. SDR Implementation

When the SDR Manager is launched, a Status Box is displayed to indicate that the manager is loading Sensor Data Records from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If no server is connected when the SDR Manager is invoked, a Connect Dialog Box will appear. This box will also support a cancel option.

3.1 Screen Display

The SDR Manager conforms to the Microsoft Windows Explorer-like model, with a Navigation Pane, a Presentation Pane and a description area. The individual panes and data columns can be resized by using a split bar.

The data in the Value column of the Presentation Pane is followed either by an “h” to denote it is a hexadecimal number, a “b” to denote it is a binary number, or by nothing to denote it is a decimal number.

The SDR Manager is an ActiveX control. This means it can be used across several server management applications. A sample screen shot of the SDR Manager user-interface is shown below.

Figure 13 - 2 is the example of SDR Manager displaying IPMI 1.0 data. The numbers in the Value column are followed by either a “h” to denote it is a hexadecimal number, a “b” to denote it is a binary number, or by nothing to denote it is a decimal number.

3.2 Navigation Pane

The Navigation Pane is implemented as a Tree View with “SDR Information” at the root. Under the root, SDR records are logically grouped based upon record type. All individual sensor records are organized as leaf nodes under the corresponding branch name. The name used for each sensor record depends on the record type.

3.2.1 Display Name Rules for Sensor Record

- Record ID is displayed in hex i.e. xxxhx. The hexadecimal number is followed by a “h” to denote it is a hexadecimal number.
- The '(ID String Bytes)' should not be displayed if none is specified i.e. the type/length field is zero length.

Following is the list of display names for IPMI v0.9 and v1.0 implementation. In this table, 0Xh is the hexadecimal sensor type and #0xNN is the hexadecimal sensor number.

Table 13 - 4: SDR Tree View Details

IPMI 0.9 Implementation	
SDR Type 01h, Internal Sensor with Thresholds	0Xh - Sensor Type (ID String Bytes) (Record ID)
SDR Type 02h, Digital/Discrete Reading, no Thresholds	0Xh - Sensor Type (ID String Bytes) (Record ID)
SDR Type 10h, IMPB Device Locator Record	0Xh - Device Type (ID String Bytes) (Record ID)
SDR Type 0C0h, OEM SDR	OEM SDR Record (Record ID)
SDR Type 01h, Full Sensor Record	0Xh – Sensor Type #0xNN (ID String Bytes)
SDR Type 02h, Compact Sensor Record	0Xh – Sensor Type #0xNN (ID String Bytes)
SDR Type 08h, Entity Association	Entity Association Record
SDR Type 10h, Generic Device Locator Record	0Xh – Device Type (ID String Bytes)
SDR Type 11h, FRU Device Locator	0Xh – Device Type (ID String Bytes)
SDR Type 12h, Management Controller Device Locator Record	0Xh – Entity ID (ID String Bytes)
SDR Type 13h, Management Controller Confirmation	0Xh – Device ID
SDR Type 14h, BMC Message Channel Info	BMC Message Channel Info
SDR Type 0C0h, OEM SDR	OEM SDR Record

For example, in the case of two fans and two temperatures; the tree display is organized as:

- Full Sensor Record
- 4h – Fan #0x32 (Baseboard Fan 1)
- 4h – Fan #0x33 (Processor 1 Fan)
- 1h – Temperature #0x04
- 1h – Temperature #0x30 (Hot Swap Temp)

3.3 Presentation View

The Presentation View consists of a grid and a description text box. The grid contains four columns:

- +/- (Expand/Collapse sign)
- Byte
- Name
- Value

For each SDR device (leaf node) selected in the Tree View, the corresponding attribute information is displayed in the Grid. All attribute information is displayed.

The description box at the bottom of grid displays the description of the item in the grid that is currently selected. The description text box supports a vertical scroll bar.

+/-	Byte	Name	Value
	8	Sensor Number	1Fh
-	9:10	Sensor Owner Confirmation	0005h
	(15:8)	Byte 2: Firmware Revision	00h
	(7:0)	Byte 1: Device ID (LSB)	05h
-	11	Sensor Module FRU Inventory	10h
	(7)	Device Owner ID Type	0b - ID is IPMB
	(6:0)	I ² C Slave Address	0010000b
-	12	Sensor Initialization	F1h
	(7)	Sensor Init	1b - Init sensor
	(6)	Init Scanning	1b - Enable scanning
	(5)	Init Event Messages	1b - Enable event messages
	(4:2)	Reserved	XXX

Figure 13 - 2: SDR Grid

Table 13 - 5: SDR Grid Fields

Field	Function
+/- (expand / collapse)	<p>The rows of '+/-' column have three possible states:</p> <p>Can be expanded (+): Indicates the row contains Byte information that can be described in further detail. Click the '+' to expand the row.</p> <p>Can be collapsed (-): Indicates the row containing Byte information is expanded to display the detailed information related to its constituent bits. Click the '-' to collapse rows with Bit information.</p> <p>Can't be expand and can't be collapsed: The column of expand sign is empty if the row can not be expanded or collapsed.</p> <p>Note: Expand/Collapse is available in rows with Byte information, but not in rows with Bit information.</p>
Byte	The byte column displays the byte number or the bit number. The bits for a byte are enclosed by the parentheses. For example, the bit 6 to bit 0 of byte 11 is represented by (6:0).
Name	The Name column is similar to the "Field Name " of each SDR type in the IPMI specification.
Value	The "Value" column cell displays the actual decoded value as received from the Server.

3.4 Description

As users highlight any element of a row, the corresponding description is displayed in the text box at the bottom of the grid view.

3.5 Container Functionality

The ISC component applications provide some generic functionality for the SDR manager.

3.5.1 Supported Commands

Each command is implemented as a menu selection. “Open”, “Save As”, and “Print” are selections under the “File” menu. “Properties” and “Reload” selections under the “SDR” menu. The menu can be outlined as follows:

Table 13 - 6: SDR Menu - Supported Commands

Menu Option	Sub-option	Description
<u>F</u> ile		
	<u>O</u> pen...	Open a file. It opens the Microsoft Win32 Common Open Dialog to allow users to select a file from directory. Only the opening of a standard SDR formatted file is supported.
	Save <u>A</u> s...	Save the file to a directory. It opens Microsoft Win32 Common Save Dialog for saving a file. In all cases the entire SDR file is saved. The SDR information written to a file is in SDR file format, with a “.SDR” extension. The SDR file format is specified by the Non-Volatile Storage Load File Format Specification, and the Intelligent Platform Management Interface Specification
	<u>P</u> rint...	Generic Microsoft Win32 Common Print functionality. Print the SDR information, as it would be done in a standard Windows application. Unlike the “Save As” function; this feature prints the information as it is displayed. Additionally, the printing function supports the printing of selected leafs and nodes of information. All leaves included in the selected node are printed. The root ‘SDR Information’ node can be selected to print the entire SDR information. The Microsoft Win32 Common Print Dialog is displayed with the “All” radio button selected in the “Print range” group box and the other radio buttons disabled. The “Print to file” check box is hidden. The selected node is written centered at the top of the print out with the attributes displayed on the left side of the page and the values displayed on the right half of the page.
<u>S</u> DR		
	<u>P</u> roperties	Displays SDR information. Refer to the figure above for information displayed in a dialog box when user selects this option. Both ‘Number of Entries’ and ‘Free Space Remaining’ are displayed as decimal values. Free space remaining is the number of bytes remaining
	<u>R</u> eload	This option allows the user to update the display with data from the server. For performance requirements, particularly when retrieving via modem, SDR information is retrieved only if ‘ Last Add Time’ or ‘ Last Erase Time’ has been changed since last retrieval, or the user had cancelled the earlier load.
<u>H</u> elp		
	Help <u>T</u> opics	
	<u>A</u> bout SDR Manager	

3.5.1.1 SDR Command Detail

The following information is displayed if a connection to a server has been established:

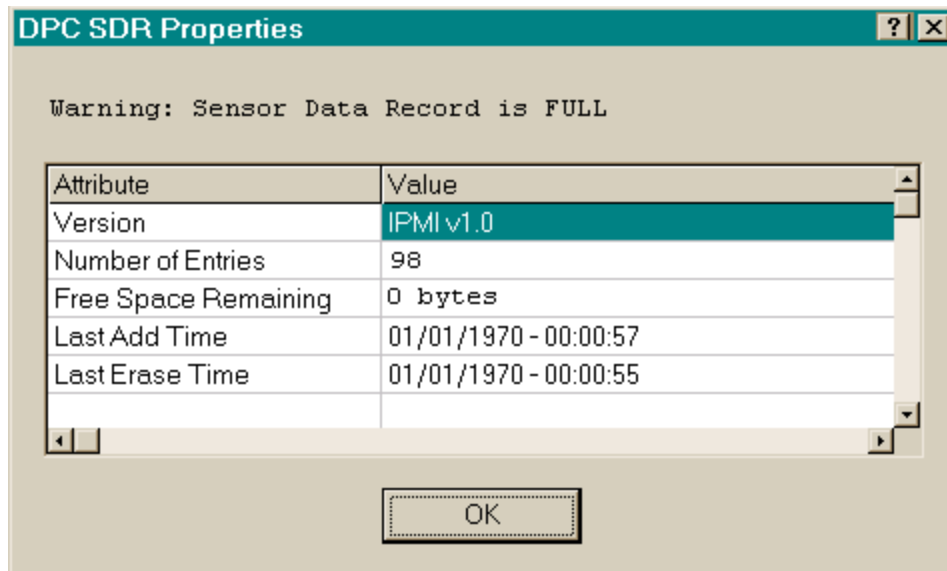


Figure 13 - 3: SDR Properties Dialog

4. SEL Implementation

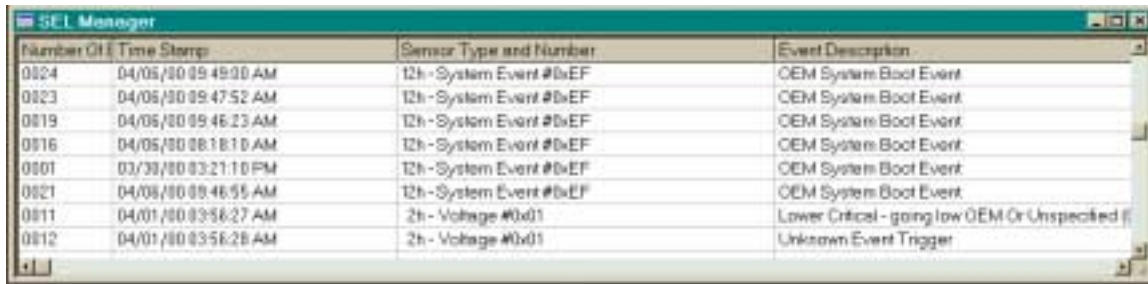
When the SEL Manager is launched, a Status Box is displayed to indicate that the manager is loading Sensor Event Log records from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If no server is connected when the SEL Manager is invoked, a Connect Dialog Box will appear. This box will also support a cancel option.

4.1 Screen Display

The SEL Manager will conform to Microsoft Windows Explorer-like model, using a Presentation Pane. Users can resize the individual data columns in the view. The SEL Manager as an ActiveX control so that it may be used across several server management applications.

For all ISC components, the SEL Manager will appear as follows:



Number Of Events	Time Stamp	Sensor Type and Number	Event Description
0824	04/05/80 09:49:00 AM	12h - System Event #0x01	OEM System Boot Event
0823	04/05/80 09:47:52 AM	12h - System Event #0x01	OEM System Boot Event
0819	04/05/80 09:46:23 AM	12h - System Event #0x01	OEM System Boot Event
0816	04/05/80 08:18:10 AM	12h - System Event #0x01	OEM System Boot Event
0801	03/30/80 03:21:10 PM	12h - System Event #0x01	OEM System Boot Event
0821	04/05/80 09:46:55 AM	12h - System Event #0x01	OEM System Boot Event
0811	04/01/80 03:56:27 AM	2h - Voltage #0x01	Lower Critical - going low OEM Or Unspecified
0812	04/01/80 03:56:28 AM	2h - Voltage #0x01	Unknown Event Trigger

Figure 13 - 4: SEL Manager

4.2 Viewer

The Presentation Pane (list view) is based on a multi-column format. All SEL record information is displayed in the List View, one system event per row. The SEL data information are ordered and named as follows:

- A count of the system events being displayed. Starting with 1, and increasing by one for each event. The title is selected as 'Number Of Events', so that if the column is shortened 'Num' is still meaningful.
- Timestamp
- Sensor Type and number
- Event description
- Generator ID

The interpretation of the event, event type, and event data 1, 2, and 3 is presented in the Event Description column.

Each of the columns can be sorted by clicking on the column heading.

4.3 Container Functionality

ISC will enable and disable specific UI controls to make the supported commands available. All the commands are implemented as menu selection of the control container and are on the containers menu bar. “Open”, “Save As”, and “Print” are sub menu items under “File” menu.

4.3.1 Supported Commands

All the commands are implemented as menu selection of the control container. “Save As”, and “Print” are sub menu items under the “File” menu. “Properties”, “Reload” and “Clear” are sub menu items under the “SEL” menu.

Table 13 - 7: SEL Menu - Supported Commands

Menu Item	Sub-item	Description
<u>F</u> ile		
	Save As...	Save the file to a directory. It opens Microsoft Win32 Common Save Dialog. All SEL information is written to a file in SEL file format, with a “.SEL” extension. The first six rows in the file list the SEL Properties in the order seen in the SEL Properties Dialog. The next row is blank and the following row lists the column headings. The SEL file format is specified as an ASCII readable text file, with each field delimited by a TAB and each System Event ending with a Carriage Return/Line Feed. In the simplest terms, whatever is displayed on the screen is written to the file, including the sort order in effect on the screen. The columns most likely do not line up. This is intentional so that the file may be opened in programs such as MS-Excel.
	Print...	Generic Win32* Print functionality. Print the SEL information, as it would be done in a standard Windows application. Printed in the same format as described in “Save As” with the addition that each page after page one begins with the underlined column headers and end with a page number centered in the border. The Microsoft Win32 Common Print Dialog is displayed with the “All” radio button selected in the “Print range” group box and the other radio buttons disabled. The “Print to file” check box is hidden. The columns of information wrap if they are too long to be displayed in the area provided.
<u>S</u> EL		
	<u>P</u> roperties	Displays SEL information. Refer to the figure above for information displayed in a dialog box when user selects this option. If the SEL is not full then there is no text displayed to indicate it. The warning related to SEL is full is displayed when the ‘Number of Entries remaining’ is 0.Both ‘Number of Entries’ and ‘Free Space Remaining’ are displayed as decimal values.
	<u>C</u> lear	Clicking this function clears the System Event Log on the server, then update the display with the latest information, which is likely to be nothing. A dialog box informs the user what actions will take place and asks for confirmation, i.e. this is a destructive operation, not just clear the viewer.
	<u>R</u> eload	This option allows the user to update the display with any newly generated entries. For performance requirements, particularly when retrieving SEL information via modem, SEL information is retrieved only if ‘Last Add Time’ or ‘Last Erase Time has been changed since last retrieval, or if the user had cancelled the load operation.
<u>H</u> elp		
	Help Topics	
	<u>A</u> bout SEL Manager	

4.3.1.1 Details for SEL Commands

A message informs the user if no SEL records are available. If the connection to a server has been established, then the following information is displayed. In the case when the SEL information was being read from the server and the user canceled the status, only the information read up to that time, is available for manipulation.

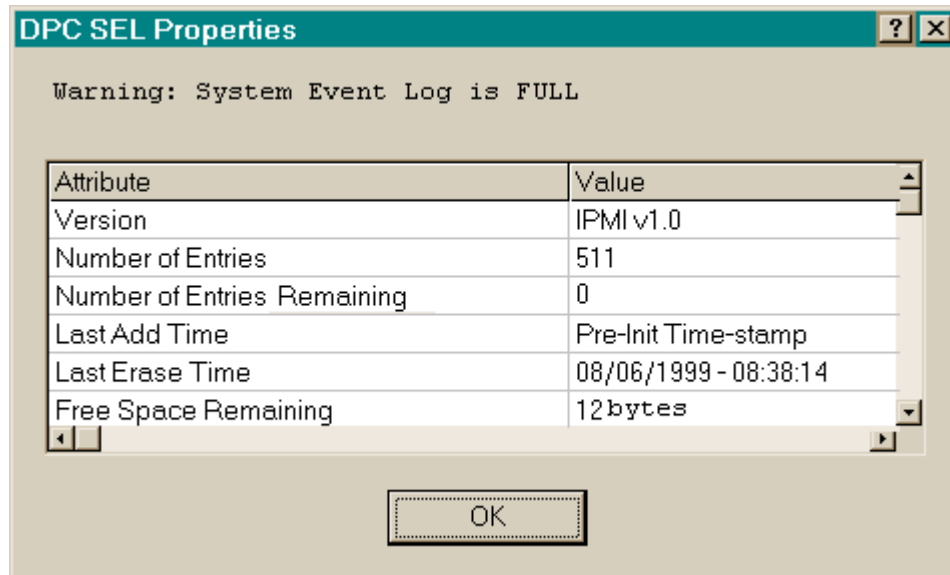


Figure 13 - 5: SEL Properties Dialog

4.4 Available Information

The SEL information is IPMI 1.0 compliant. Refer to the IPMI specification for details.

5. RSA Implementation

When the RSA Manager is launched, a Status Box is displayed to indicate that the manager is loading RSA data from the server (assuming a connection to a server exists). A Cancel button is available in the Status Box so the load operation can be terminated.

If no server is connected when the RSA Manager is invoked, a Connect Dialog Box will appear. This box will also support a cancel option. If the server is powered down, most sensors will be inaccessible to read. If a sensor cannot be read, the Current Status will read “Unknown”.

The user is given the option of choosing between Fahrenheit and Celsius for applicable fields via the RSA/Options menu item. This manager will display the value as it is retrieved from the server and will not update dynamically. However, a Reload menu item updates the values upon user selection.

5.1 Screen Display

When the RSA Manager is the active view, the RSA menu item is placed between the Action and Window menu items at the top of the screen. The RSA menu consists of two sub-items: Reload and Options. Reload behaves similar to the FRU and SDR Reload menu item.

The options dialog allow the user to choose Celsius or Fahrenheit. Upon pressing OK in the RSA Manager Options Dialog the Manager updates all values based on the selections made. The figure below displays the Options Dialog.

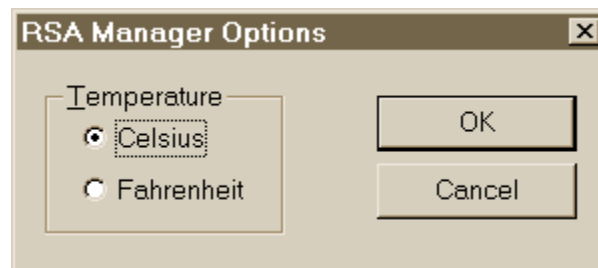


Figure 13 - 6: RSA Manager Options Dialog

The manager consists of a tree view and a property view. The tree view displays all sensors detected by the DPC Console. The property view displays the values for the current selection in the tree. This is consistent with the FRU, SEL and SDR managers.

Following are views of what the user might see in the RSA Manager.

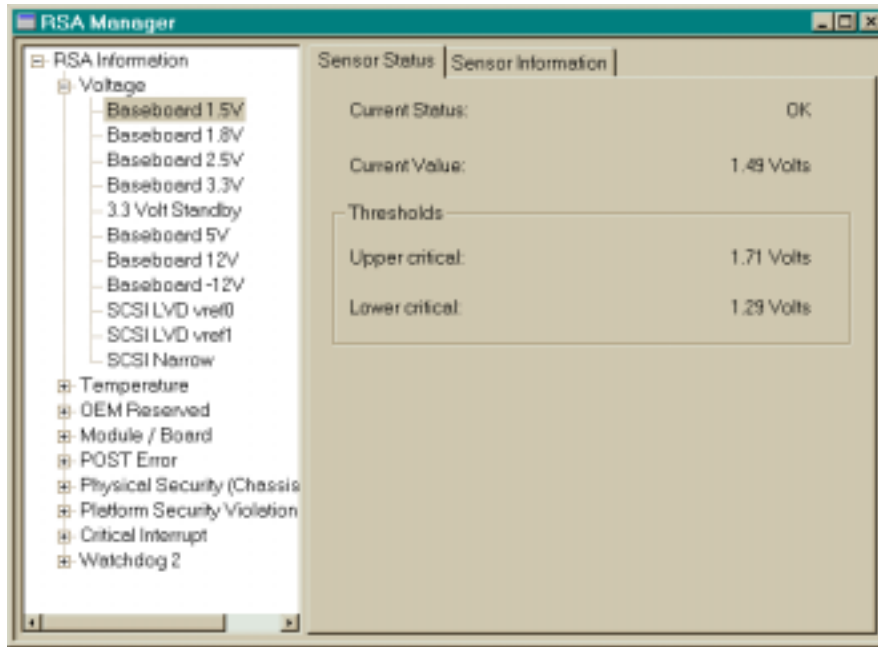


Figure 13 - 7: RSA Manager - View 1

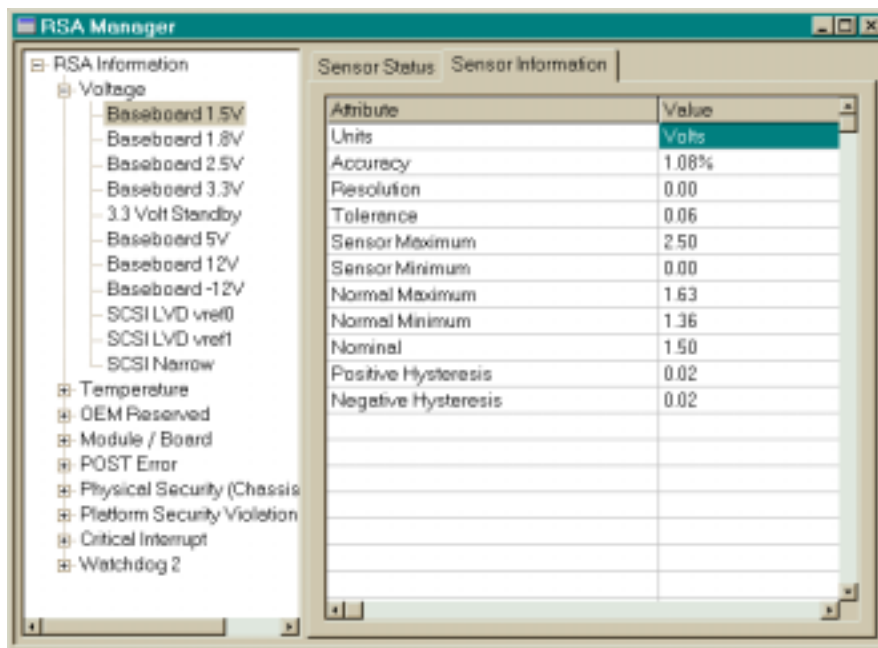


Figure 13 - 8: RSA Manager - View 2

5.2 Available Information

The RSA information is IPMI 1.0 compliant. Refer to the IPMI specification for details.

Intel® Server Control, Version 3.x TPS

Section 14: Security

Table of Contents

- 1. Introduction to Security 1
- 2. Security Implementation 2
 - 2.1 Platform Instrumentation 2
 - 2.1.1 New Authentication Scheme 2
 - 2.1.2 LRA Notification-Only Control..... 2
 - 2.1.3 SNMP Read-only Access Control..... 3
 - 2.2 DPC/CSSU Security 3
 - 2.3 LAN Based Security (IP Filtering) 3
 - 2.4 Invalid Password Handling 3
 - 2.5 Session Expiration..... 3
 - 2.6 Setup..... 4
 - 2.7 Password Length and Character-set Support..... 4

List of Figures

No figures appear in this section.

List of Tables

Table 14 - 1: ASCII Character Codes Supported by the DPC Password 4

1. Introduction to Security

ISC security is implemented through the use of passwords. When connecting to the server, either from Platform Instrumentation Control (PIC), the Client System Setup Utility (CSSU), or Direct Platform Control (DPC), each component prompts the user for a password before initiating a connection.

The default password of “null” (no password) can be configured with the System Setup Utility, to a maximum size of 16 alphanumeric characters. Since the password is not stored in the machine running PIC, CSSU, or DPC, it must be entered each time the user begins the connection process.

When connecting to the server over a serial connection, that the user enters on the client system is sent to the server in clear text. Unlike a serial connection, a LAN connection does not send the password over the wire. Instead, a Challenge Handshake Authentication Protocol (CHAP) is used.

The CHAP uses a ‘one-way’ hashing algorithm to determine the hash value. It is computationally infeasible to determine the password or secret key used for the calculation. The current implementation of the hash, or message digest, is MD2 – Message Digest version 2. The client and the authenticator share the password, which is never passed over the link.

2. Security Implementation

ISC v3.0 provides security enhancements over previous releases of ISC. These enhancements are primarily in the area of Local Area / Wide Area Network connections. A method of authentication has been incorporated and will be described in the next sections.

2.1 Platform Instrumentation

The objective of the Platform Instrumentation (PI) running on the management server is to provide an administrator with the ability to use standards-based management tools to gather information from a server and to perform various control functions to the server.

These controls provide the user with the ability to make significant changes to the server status, such as causing it to power down or reset. Because this functionality is available via a standards-based interface, it is easy for many tools to perform these actions. The ISC v3.0 release of the PI will provide the following enhancements to improve the PI security:

- Replacing the legacy method for performing powerful control actions with a new versions that require authentication.
- Providing an option to configure services that automate actions so that they cannot use power control actions.
- Providing an option to configure SNMP communication to only allow read-only access.

2.1.1 New Authentication Scheme

The new authentication scheme is based on Challenge Handshake Authentication Protocol (CHAP) with Message Digest 2 (MD2) hashing for authentication. Platform Instrumentation (PI) retrieves the password that is stored in firmware and uses it during runtime to hash the challenge strings to authenticate to users knowledge of the password.

The challenge string is a 16-byte string that consists of: a timestamp in the highest four bytes and a unique sequence number in the next four bytes, in addition to another four bytes that are chosen at random. The final four bytes of the 16 byte string is currently not used and set to zeros. The timestamp and sequence numbers are used to ensure that the challenge strings are short lived and only used once.

The application that requests the connection, such as PIC, must read the challenge attribute and use this value as a key to hash the password that is stored in firmware. This implementation ensures that each challenge string is unique and can only be used to perform an action once and only within a short time period from when it was issued.

2.1.2 LRA Notification-Only Control

ISC installation provides an option to configure services that use automated actions so that it will provide only notification actions (no power control actions). The additional four bytes are random and change each time they are used. They are not part of the sequence number. The user is shown a “check box” that allows the Notification-Only option.

As an alternative, an LRA configuration file (lra.cfg) is provided. This file supports a Notification-Only parameter that, when set to true, will cause LRA to limit the actions it issues to only

notification actions. If the Notification-Only parameter is not in the `Ira.cfg` file, LRA will have the ability to perform power control actions. The default is to have this option set to false.

2.1.3 SNMP Read-only Access Control

The ISC installation provides an option to configure the SNMP support to only allow read-only access. The installer is given a check box that allows the Read-Only option.

As an alternative, an SDLINK configuration file (`sdlink.cfg`) is provided to support a “ReadOnly” parameter. If this parameter is set to true, SDLINK will respond successfully only to get and get-next requests. All set requests will result in an error response. The default is to for this option to be set to false.

2.2 DPC/CSSU Security

Security for a connection via DPC or the Client SSU uses the same firmware-stored password as the Platform Instrumentation. When the user tries to connect using either DPC or the CSSU, the same Challenge Handshake Authentication Protocol algorithm is used.

2.3 LAN Based Security (IP Filtering)

When the management console uses the LAN to connect to the firmware / NIC subsystem on the managed server, the session is authenticated via the CHAP mechanism. If applicable, the session must be maintained while the server boots from its Service Partition (DPC or CSSU).

Once the connection is established, the IP address on the client is recorded. From then on, all of the services running on the server accept only connections from the authenticated IP address. Connection attempts originating from any other IP address are rejected. IP filtering also applies to any network-aware applications running from the service partition. For the duration of the connection all of the services running on the server accept only connections from the authenticated IP address.

2.4 Invalid Password Handling

If the user enters an incorrect password while opening a connection, the DPC / CSSU client will generate an invalid hash and the server will not authorize the user to continue with the session. After three successive false attempts at opening a session, the server suspends the connection ability on the server for five minutes. The server accepts the *open-session* requests only after expiration of this time interval.

2.5 Session Expiration

The server maintains a session expiration timer of five minutes. The server discontinues the session if it does not receive a valid message request from the client for five minutes since the last valid message request was received. If this happens, the client needs to re-establish the session.

2.6 Setup

The SSU provides the user interface to setup a password. The SSU sends the password to the system firmware over the IPMI interface. On reception, firmware encrypts the password and stores it in non-volatile storage.

2.7 Password Length and Character-set Support

A NULL-terminated ASCII string (00h) should be used for the password, which should not be longer than 16 characters, with one byte used for each character. The firmware supports ASCII character codes from 32 to 126 as described in ISO 646/8859-1. The following table illustrates the supported character set. The password can be disabled by using a NULL password (A password string with no characters other than the NULL terminator). The default password is 'NULL'.

Table 14 - 1: ASCII Character Codes Supported by the DPC Password

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
	<SP>		< 0 >		< @ >		< P >		< ` >		< p >
	< ! >		< 1 >		< A >		< Q >		< a >		< q >
	< " >		< 2 >		< B >		< R >		< b >		< r >
	< # >		< 3 >		< C >		< S >		< c >		< s >
	< \$ >		< 4 >		< D >		< T >		< d >		< t >
	< % >		< 5 >		< E >		< U >		< e >		< u >
	< & >		< 6 >		< F >		< V >		< f >		< v >
	< ' >		< 7 >		< G >		< W >		< g >		< w >
	< (>		< 8 >		< H >		< X >		< h >		< x >
	<) >		< 9 >		< I >		< Y >		< l >		< y >
	< * >		< : >		< J >		< Z >		< j >		< z >
	< + >		< ; >		< K >		< [>		< k >		< { >
	< , >		< < >		< L >		< \ >		< l >		< >
	< - >		< = >		< M >		<] >		< m >		< } >
	< . >		< > >		< N >		< ^ >		< n >		< ~ >
	< / >		< ? >		< O >		< _ >		< o >		

Appendix A: ISC 3.5 Update

Intel Server Control 3.5.1 ships with the SDS2, SCB2, TSRLT2 system platforms. This appendix describes the differences between ISC 3.5.x and ISC 3.0/3.1 that was used on SKA4-based systems. Differences include the following:

- The addition of IPMI 1.5 compliancy
- Addition of Korean GUI translation
- Addition of DPC GUI configuration status enhancements
- Removal DPC's remote diagnostics (Refer to "Installing and Remotely Running BYO Platform Confidence Test Software on a SCB2 Service Partition White Paper" for limited remote testing purposes)
- The defeaturing of CSSU's SUA remote BIOS update on SDS2 systems.
- ISC 3.5 is supported on SCB2, and TSRLT2 systems only.
- ISC 3.5.1 is supported on SDS2, and SCB2, systems only. For SCB2 systems it is recommended to upgrade to ISC 3.5.1 as soon as possible.
- DPC over LAN /CSSU over LAN access is limited to onboard NIC1.

Compliance with IPMI 1.5

The ISC 3.5.1 Platform Instrumentation (PI) retains backward compatibility with IPMI 1.0 while adding some new capabilities. Sensor operation, Sensor Data Records (SDR), System Event Log (SEL), Field Replaceable Unit (FRU), Watchdog Timer, and System Interfaces are almost nearly unchanged from IPMI 1.0. Therefore, ISC 3.5.1 Platform Instrumentation (PI) essentially provides the same features as an IPMI 1.0 system with modifications to conform to IPMI 1.5. ISC 3.5.1 PI supports both IPMI 1.5-based and 1.0-based systems.

The ISC 3.5.1 release of PI provides the following enhancements to comply with the IPMI 1.5 specifications. Earlier these features were supported using proprietary commands.

- Users, Privileges, and Authentication Support for Security features with BMC calls compliant with new standards. User Password requirements for DPC/CSSU connections, and CHAP authentication are how this is implemented. However, from a user standpoint, ISC PIC functionality is identical to that on ISC 3.1 SKA4 based system.
- Serial/Modem Alerting and Paging to provide standards-based Dial Paging (numeric paging via a modem).
- The following new Direct Platform Control (DPC) related operations are provided:
 - Boot option allows BIOS to boot to a 'service partition' instead of to the main operating system partition. (i.e. "F4" on on AMI* based BIOSes)
 - Functionality to detect a Service Partition, scan the Service Partition, and get and set DPC/CSSU boot partition are enhanced to comply with IPMI 1.5 specification.

- The ability to provide RAID level 1 and 5 service partition support on SCB2 ATA Promise RAID systems. (Refer to the TA-433.pdf “Intel Server Control v3.5 Service Partition installation procedure for SCB2 ATA Promise* RAID)

In addition, modifications are made to existing features to be in compliance with IPMI 1.5 standard. Appropriate changes are made for additional events for power supply, memory and slot information supported in IPMI 1.5 specification.

A new feature for IP Address synchronization with the BMC is implemented in ISC 3.5.x PI.

- IP Synchronization Agent (IPSA). This agent ensures that the network configuration parameters stored in the BMC are consistent with the values specified in the operating system. Hence, BMC MAC addresses should stay in sync with the operating system IP addresses.

The baseboard/chassis instrumentation is based on the DMI 2.0 Service Provider (SP) interface.

Korean GUI Translation

Additional enhancements beyond IPMI 1.5 compliancy include the addition of Korean localization for the PIC GUI, CSSU GUI and DPC GUI. With the addition of Korean GUI support ISC 3.5.x now is translated into Simplified Chinese, German, Spanish, and Korean. Localization applies to the Graphical User Interfaces (GUI) only and related components including ISC Utilities, Firmware, FRU/SDR, PI, and server-side information, will continue to be supported in United States English only.

DPC Status Configuration Dialog Enhancements

The DPC GUI has been streamlined to improve user functionality. Changes in the new GUI affect the “Status and Configuration” dialog only. Figures A - 1 through A - 3 compares ISC 3.0/3.1 dialogs with ISC 3.5 Configuration Status dialogs, shown in Figure A - 4.

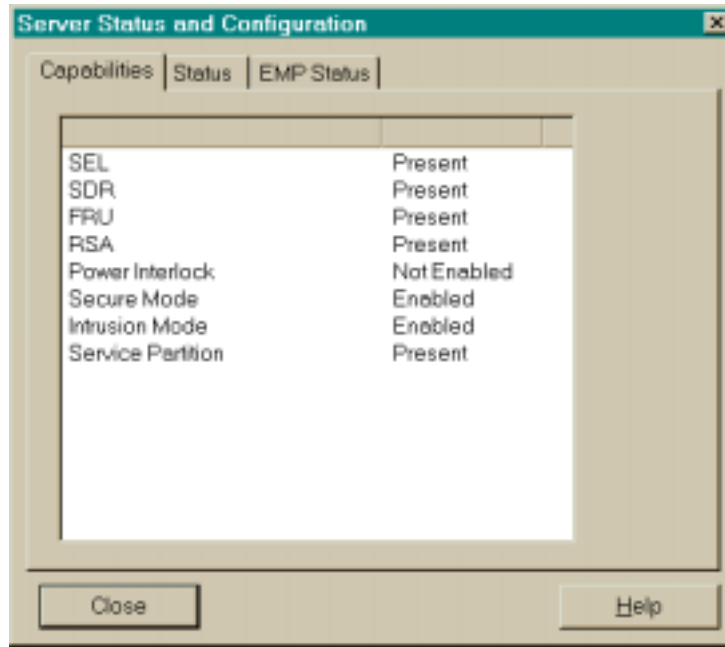


Figure A - 1: ISC 3.0/3.1 DPC Configuration and Status “Capabilities” Dialog

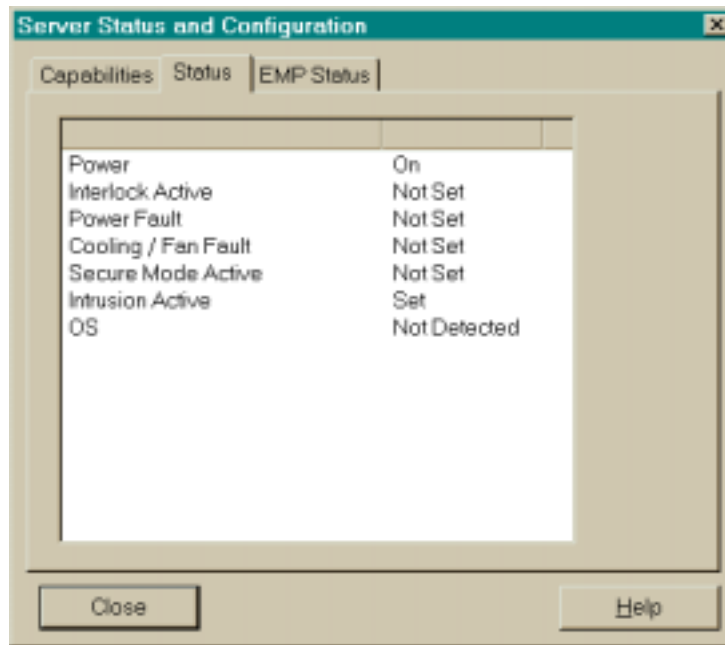


Figure A - 2: ISC 3.0/3.1 DPC Configuration and Status “Status” Dialog

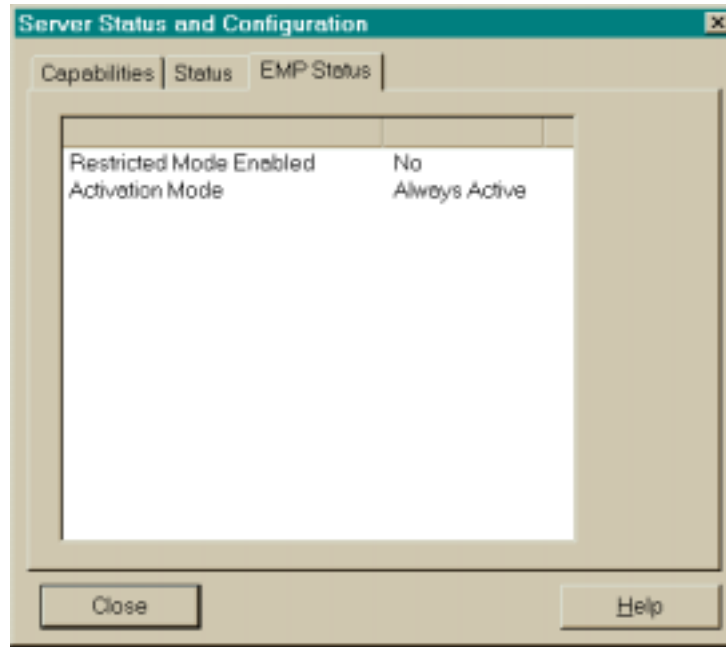


Figure A - 3: ISC 3.0/3.1 DPC Configuration and Status “EMP Status” Dialog

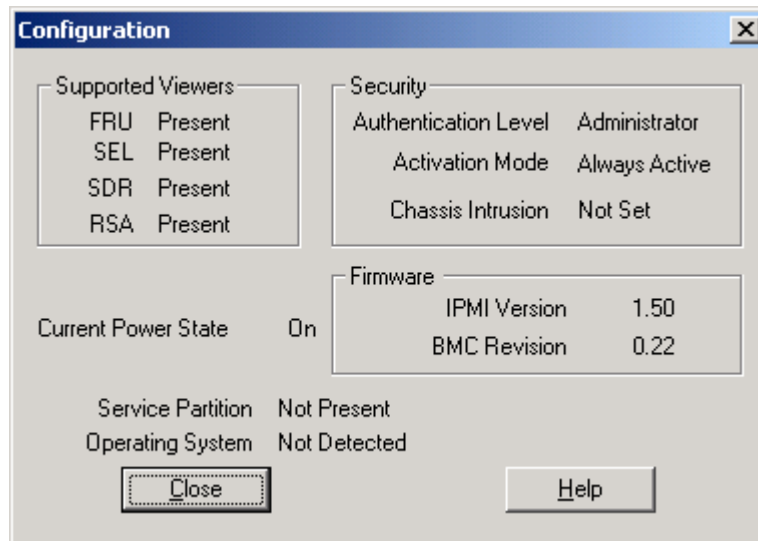


Figure A - 4: Enhanced ISC 3.5.x DPC Configuration Status Dialog

The Configuration Status dialog displays an information dialog that gives the chassis status and configuration of the server. This information is available when the DPC Console successfully connects in EMP or LAN mode.

The Service Partition status is updated automatically whenever a connection is made to the server and whenever the server status and configuration is retrieved.

- **Supported Viewers:**
This area gives the SEL, SDR, FRU, and RSA status.
- **Security:**
Displays the Authentication level, Activation mode and Chassis Intrusion setting.
 - **Authentication Level:** User or Administrator. Will be user if you have an EMP (serial) connection and EMP mode set to restricted. For TCO (LAN) connections, will be user if no secure session available (e.g. someone else already connected), or LAN access mode set to restricted.
 - **Activation Mode:** Always active or pre-boot only – reflects
 - **Chassis Intrusion:** Shows chassis intrusion detection setting
- **Firmware:** Displays IPMI and revision information

Removal of Service Partition Remote Diagnostics

Several features of the ISC 3.0/3.1 on SKA4 based systems are not available in ISC 3.5.x systems. Remote Diagnostics run via the Service Partition on SKA4 are unavailable. Refer to "Installing and Remotely Running BYO Platform Confidence Test Software on a SCB2 Service Partition White Paper" for limited remote confidence testing purposes.

Defeature of CSSU SUA Remote BIOS Update

On the SDS2 based systems remote BIOS update is temporarily unavailable. SCB2 based systems support this with initial revisions of BMC firmware and ISC software. Refer to the monthly ISC 3.x Specification Update posted on support.intel.com for details on support changes. Search on iBL for download availability.

DPC over LAN Access / CSSU over LAN Access

ISC 3.5.x-based systems will only allow access via LAN on on-board NIC1. New platforms have NIC redundancy built-in with two addressable NICs. However, ISC 3.5.x does not support CSSU or DPC LAN access over NIC2. Also, add-in NICs will also not support DPC or CSSU functions. This is similar to serial/modem connections that are only available on COM2. Serial/modem access is identical to ISC 3.0/3.1 availability.

This page intentionally left blank

Appendix B: Summary Errata Table

The following tables indicate the Errata and the Document Changes that apply to Intel Server Control v3.x. Intel intends to fix some of the errata in a future releases, and to account for the other outstanding issues through documentation or specification changes as noted. This table is added to at each release. Past items are left in place for historical purposes. See the Revision history table to determine which items have been added the most recently. These tables use the following notations:

Codes Used in Summary Table

Doc:	Intel intends to update the appropriate documentation in a future revision.
Fix:	This erratum is intended to be fixed in a future release of the software.
Fixed:	This erratum has been previously fixed.
NoFix:	There are no plans to fix this erratum.
Investigate	Intel is investigating this issue.

Revision History

8/27/01	First Appendix with Erratas 1-21 added.
12/11/01	Added Errata items 22-38.
6/5/02	Added Errata items 39 - 47

Application Errata

NO.	Plans	ERRATA
1	Fix 3.1	Windows* 2000 console systems will not launch ISC within HP* OpenView* 6.1
2	Fix 3.1	HP OpenView integration health oval stays orange (status alert) even though server Health is okay. It should be a green ISC oval.
3	Fix 3.1	Uninstall ISC after installation of LANDesk® Server Manager (LDSM) and ISC causes the win32sl service to not start. As a result, some LDSM functions are disabled.
4	Fix 3.1	LAN Alerts fail in Chinese because the Java* Runtime Environment is not loaded properly.
5	Fix 3.1	LAN Alert Viewer is not translated in Chinese, German, and Spanish
6	Fix 3.1	Windows registry key DMI2SNMP is not installed.
7	NoFix	On internationalized releases, some text may appear in English.
8	NoFix	For customers using HP OpenView, the files Ezrpcw32.dll, Wcdmionc.dll, Wcrap.dll, Winrpc32.dll, and Wonctcp.dll are not removed during uninstall when HP OpenView is running.
9	NoFix	Intel Server Control objects are not removed from the HP OpenView database and map.
10	NoFix	The ISC Console may lose communication with the server if the server reboots or shuts down.
11	NoFix	Keyboard shortcuts do not always work.
12	NoFix	The "Immediate Hardware Reset" and "Immediate Power Off" features may not work properly during initialization.
13	NoFix	The SEL viewer updates inconsistently if there are a very large number of event records.
14	NoFix	In some configurations, the ISC console inconsistently discovers ISC servers.
15	NoFix	ISC may cause a floppy error message being generated on a Linux* server.

NO.	Plans	ERRATA
16	NoFix	LDSM SNMP Event Viewer cannot run on the same machine as HP OpenView.
17	NoFix	F1 key does not always give help correctly.
18	NoFix	Server hangs when ESC key pressed on server keyboard when server is connected to Client SSU.
19	Fix 3.1	MIB files not loading correctly into HP OpenView.
20	Fix in future release	The "SNMP read-only access" option for Intel Server Control Platform Instrumentation (ISC PI) does not function as desired.
21	Fix 3.1	A Microsoft Windows Event Log SNMP warning message is recorded during system boot when Intel Server Control software is installed. This message also appears every time the SNMP service is stopped and re-started.
22	No Fix	Intel Server Control V3.1 will not launch from CA* Unicenter* TNG 2.4
23	No Fix	Direct Platform Control diagnostics fail with SKA4 final Resource Kit CD
24	Fix in 3.5	Local Response Agent (LRA) may reprocess all SEL events when SEL is approximately 80% full on on ISC 3.0 / 3.1 / 3.1.1 based systems
25	No Fix	Direct Platform Control's FRU Manager Chassis and Board attributes labels are incorrect under ISC 3.5
26	No Fix	Direct Platform Control's FRU Manager (ISC 3.5) only displays baseboard information and the following are not viewable: HSC, power distribution board, power supply 1 and 2 missing
27	No Fix	Direct Platform Control fails to boot to the service partition when connected by DNS (Domain Name Service) under ISC 3.5
28	No Fix	When using CA-TNG Unicenter 2.4 on ISC 3.5 systems, double-clicking on the ISC WorldView may fail.
29	No Fix	Direct Platform Control is unable to connect to a server via modem when the EMP Access Mode is set to "Preboot" in System Setup Utility (SSU).
30	Fix in 3.5.1	ISC 3.5 on SCB2 LAN Alert Viewer chassis intrusion is non-functional.
31	No Fix	The default "Server" install of Red Hat Linux 7.1 does not allow ISC to function.
32	No Fix	BMC/BIOS will not maintain changes to dynamic IP address unless ISC PI component is running.
33	No Fix	Auto refresh with the Intel Server Control GUI application Platform Instrumentation Control (PIC) may not work when monitoring a Windows* based server.
34	No Fix	The Intel Server Control's Platform Instrumentation (PI) agent that synchronizes the Baseboard Management Controller's (BMC) IP/MAC address with the operating system IP address does not synchronize the addresses on non-US English versions of NT 4.0 SP6A.
35	Fix in 3.5.1	Occasionally Intel Server Control 3.5 for SCB2 systems will not successfully launch within HP OpenView 6.2 ISCNode Icon, or may be excessively slow in launching.
36	No Fix	Actions for some hot swappable power supply events may not be set and handled properly on ISC 3.5.1 on SDS2 systems.
37	No Fix	If a Microsoft Windows NT v4.0 operating system has the "Services for Macintosh" enabled the Intel Baseboard Service needed for reporting system health will not start correctly
38		ISC 3.5 User Guide incorrectly states that concurrent DPC modem and LAN connects are not supported in ISC 3.5
39	Fix in 3.5.1	Occasionally Intel® Server Control 3.5 for SCB2 systems will not successfully launch within HP OpenView* 6.2 ISCNode Icon, or may be excessively slow in launching.
40	Fix in 3.5.1	Unable to install ISC 3.5.1 on SDS2 or SCB2 based servers to NetWare 6.0 or Red Hat* Linux 7.2
41	Fix in ISM 5.x	The initial health status of ISC as seen on the Stand Alone console for Red Hat* Linux 6.2 or 7.1 servers may not reflect the current health status.
42	Fix	Installing Promise* FastTrak* Log Service may stop the Promise FastTrak DMI service integrated with ISC 3.5.2.

NO.	Plans	ERRATA
43	Fix	Uninstalling Promise* software components may also remove Promise* FastTrak* DMI service integrated with ISC 3.5.2.
44	Fix	With ISC 3.5.2, ISC objects on the CA-TNG map may not appear.
45	Fix	Application seems to 'hang' after a reboot when serial access mode is set to "Preboot"
46	Investigate	ISC icons Intel Platform Control (PIC) and Intel DMI browser may not appear on ISC Standalone Console
47	Investigate	Booting to the SDS2 service partition from a remote modem connection may cause the server to hang.

1. ISC will not launch from HP* OpenView* 6.1 on Windows* 2000 consoles

Problem: The user installs HP OpenView, then ISC on a Windows 2000 console. ISC does not snap into (Is not accessible from) HP OpenView. It works correctly on Windows* NT* and on Windows 98. When the user selects the HP OpenView node (subnet) in question s/he does not see the normal ISC green oval with the title "ISCnode."

Implication: Only non-Windows 2000 based ISC console systems integrate with HP OpenView 6.1. There is no right-click functionality to launch ISC with HP OpenView 6.1.

Workaround: Launch ISC components from the Start Menu | Programs | Intel Server Control sub-folder only.

Status: Fixed in ISC 3.1

2. HP OpenView Orange (alert) oval is displayed even though the health oval should be green (okay)

Problem: HP OpenView 6.1 status oval stays orange even though ISC Platform Instrumentation Control (PIC) reports no status alerts for failing or potentially failing hardware components.

Implication: Misconstrued and confusion hardware information.

Workaround: None

Status: Fixed in ISC 3.1

3. Uninstall ISC after installation of LDSM and ISC causes the win32sl service to not start

Problem: Install LDSM 6.1 and ISC 3.0, then uninstall ISC 3.0. This correctly removes registry components. However, since LDSM also uses the WIN32SL service, it is incorrect that this element is removed. The WIN32SL service should remain and continue running.

Implication: LDSM 6.1 runs in a limited capacity if ISC 3.0 is de-installed.

Workaround: Manually restart the WIN32SL process in Control Panel | Services. Set it to start automatically on the next system reset.

Status: Fixed in ISC 3.1

4. LAN Alert Viewer fails to launch under Simplified Chinese only

Problem: After installing the Java 2 runtime environment, the "LanAlert viewer" will not launch from the Start menu.

Implication: LAN Alert Viewer is inoperable in Simplified Chinese.

Workaround: Install the Chinese JRE located at <http://java.sun.com/j2se/1.3/jre>

Status: Fixed in ISC 3.1.

5. LAN Alert Viewer is not translated in Chinese, German, and Spanish

Problem: After installing the LAN Alert Viewer on either a Chinese-, German-, or Spanish-based server, the LAN Alert Viewer only appears in English, regardless of country language of the operating system.

Implication: LAN Alert Viewer only runs in English.

Workaround: None.

Status: Fixed in ISC 3.1.

6. Windows Registry key DMI2SNMP is missing after installation of ISC on a SNMP community enabled client-server setup

Problem: The Windows Registry key for \SOFTWARE\INTEL\DMI2SNMP is missing or configured wrong on a Windows server with SNMP and ISC. An error will occur in the Windows event log with the following context: "The SNMP Service is ignoring the extension Software\Intel\DMI2SNMP because it is missing or misconfigured." Though the error is reported, the SNMP service starts and runs.

Implication: SNMP traps are not consistently sent and viewed in HP OpenView 6.1, CA Unicenter 2.2 TNG*, or LANDesk Server Manager 6.1.

Workaround:

- 1) Disable or set to MANUAL the "Intel NIC LAN" service and
- 2) Create a "DMI2SNMP" key in the Windows registry and add value of "pathname and string" to default ISC path put the attached DLL in that path. SNMP errors will not appear continue to appear in the event log and host servers will receive SNMP traps in the correct formats.

Status: Fixed in ISC 3.1 on the SPKA4, SRKA4, and on the ISP4400 systems.

7. On internationalized releases, some text may appear in English

Problem: At the time of release, some user interface and Help strings may not have been translated, or may contain redundant text in English.

Implication: The user may not have a clear understanding of information communicated by the user interface.

Workaround: None.

Status: Intel is investigating the possibility of fixing this erratum.

8. For customers using HP OpenView, the files Ezrpcw32.dll, Wcdmionc.dll, Wcrap.dll, Winrpc32.dll, and Wonctcp.dl are not removed during uninstall when HP OpenView is running

Problem: Because the ISC uninstall program does not have information about other applications that may be running, it does not shut down HP OpenView. Therefore, ISC files that are open while HP OpenView is running cannot be deleted.

Implication: Some files are not removed from the system during uninstall.

Workaround: Close HP OpenView prior to uninstalling ISC

Status: Intel is investigating the possibility of fixing this erratum.

9. Intel Server Control objects are not removed from the HP OpenView database and map

Problem: After uninstalling the Intel Server Console, ISC symbols are left on the HP OpenView map. If the user double clicks on a ISC symbol, HP OpenView throws a Dr. Watson.

Implication: ISC symbols and objects created during ISC integration are not removed from the system during uninstall.

Workaround: Users should copy "c:\Program files\Intel\ServerControl\Bin\UninstlscOv.txt" to "c:\Openview\registration\C\UninstlscOv.txt".

Status: Intel is investigating the possibility of fixing this erratum.

10. The ISC Console loses Communication with the server if the server reboots or shuts down

Problem: The ISC console loses communication with the server if the server reboots or shuts down. The server reboot or shutdown may be caused by several actions, including LRA actions that occur in response to an event condition, or by the user manually resetting or powering down the system. Once the server has powered down, the RPC connection used by the console to communicate with the server is no longer valid.

- Implication:** The ISC console appears to hang, pending a time-out on a DMI request to the server. This time-out may take several minutes to occur. Once ISC detects a time-out condition (loss of communication to the server), it notifies the user and then terminates. The current ISC console session cannot re-establish communications to the server after the server has been restarted. Instead, the current ISC console session must terminate, and a new ISC console session started to manage the server again.
- Workaround:** After the server is restarted, the user must re-launch ISC. The users can wait for the current ISC console session to terminate normally (after the time-out is detected), or s/he can manually stop the ISC console process and then restart ISC.
- Status:** Intel is investigating the possibility of fixing this erratum.

11. Keyboard shortcuts do not always work

- Problem:** The ISC GUI is divided into two windows or panes. The left pane is used for navigation and the right pane is used for presenting information. If the current window focus is in the right pane, keyboard shortcuts will not work. For example, the F5 key will not refresh the screen, the tab key will not navigate, and the Alt-A shortcut will not apply. If the current window focus is in the left pane, then the F5 key will refresh the data including data displayed in the right pane.
- Implication:** The mouse and menu must be used instead of keyboard shortcuts.
- Workaround:** Use the mouse to click in the left pane to change the window focus. This will allow use of the F5 key for refresh. The tab key and Alt-A key do not work.
- Status:** Intel is investigating the possibility of fixing this erratum.

12. The "Immediate Hardware Reset" and "Immediate Power Off" features may not work properly during initialization

- Problem:** During the ISC GUI initialization, if the user selects the power control actions "Immediate Hardware Reset" or "Immediate Power Off", the actions may not work as documented.
- Implication:** The power control actions "Immediate Hardware Reset" and "Immediate Power Off" may not work properly and the server may continue to run without the desired action.
- Workaround:** Users should wait until the ISC GUI has completed initialization (The status bar will display a READY state) before attempting these actions.
- Status:** Intel is investigating the possibility of fixing this erratum

13. The SEL viewer updates inconsistently if there are a very large number of event records

- Problem:** The SEL viewer in PIC and DPC do not consistently display event records when there are more than a few hundred events in the log.
- Implication:** User cannot view all event records consistently.
- Workaround:** User can periodically clear the SEL log through the Direct Platform Control (DPC) console.
- Status:** Intel is investigating the possibility of fixing this erratum.

14. In some configurations, the ISC console inconsistently discovers ISC servers

- Problem:** The ISC console may not discover all servers in a single discovery session.
- Implication:** User does not consistently discover ISC servers.
- Workaround:** Restart the ISC console and again run discovery to display the missing servers.
- Status:** Intel is investigating the possibility of fixing this erratum.

15. ISC may cause a floppy error message being generated on a Linux server

- Problem:** While starting ISC on a RedHat* Linux server, the user may see the message "end_request: \IO error, dev 02:00 (floppy), sector 0" on the system console. This is caused by ISC attempting to mount the floppy drive to check for configuration files. The mount command results in the above message if there is no floppy in the drive. This message comes from the floppy driver in the kernel and cannot be suppressed.
- Implication:** The user may think an error has occurred.
- Workaround:** None.
- Status:** Intel is investigating the possibility of fixing this erratum.

16. LDSM SNMP Event Viewer cannot run on the same machine as HP OpenView*

- Problem: Conflict between LDSM and HP OpenView.
- Implication: Only one of these applications can receive TRAPs when both are running on the same Windows system.
- Workaround: Run one viewer at a time.
- Status: Intel is investigating the possibility of fixing this erratum.

17. Pressing F1 for help may not work

- Problem: On non-English operating systems, pressing the F1 key may not display the help screen. Instead, the user receives a message that help does not exist.
- Implication: The user may not have F1 access to needed help topics.
- Workaround: The help topics can be accessed through the menu selection.
- Status: Intel is investigating the possibility of fixing this erratum.

18. If the server is connected to the Client SSU, it hangs when the ESC key on the server is pressed

- Problem: The keyboard on the server should be locked to prevent users from interrupting a remote session with Client SSU because using the ESC key may cause the server to hang.
- Implication: The Client SSU cannot communicate with the server if the server's ESC key has been pressed.
- Workaround: Users should not press keys on the server keyboard during a remote session with the Client SSU.
- Status: Intel is investigating the possibility of fixing this erratum

19. Some MIB files will not manually load in some versions of HP OpenView

- Problem:** Some of the MIBs provided with ISC will not load in some versions of HP OpenView.
- Implication:** HP OpenView will not provide all information when displaying a SNMP trap from ISC.
- Workaround:** None.
- Status:** Intel is investigating the possibility of fixing this erratum.

20. The “SNMP read-only access” option for Intel Server Control Platform Instrumentation (ISC PI) does not function as desired

- Problem:** Intel Server Control Version 3.0 provides a security feature that should disable SNMP SET commands on a server with Intel Server Control Platform Instrumentation. This feature is not functioning as expected. During the ISC installation, a “SNMP Read-Only access” option is presented under “Platform Instrumentation”. Selecting this option fails to disable SNMP SET commands. By default, SNMP SET and GET commands are permitted and work correctly. There is no impact to the generation of SNMP traps, which functions normally. SNMP traps are processed and are received by the SNMP consoles as expected.
- Implication:** The user is not able to disable SNMP SET commands through the Intel Server Control installation process.
- Workaround:** The operating system SNMP service can be configured with “Community Rights” set to “Read-only”. This provides the ability to disable SNMP SETS as Intel Server Control was intended to do. This is essentially the same as disabling the SNMP SET commands for all extension agents, including Intel Server Control Platform Instrumentation.
- Status:** Intel is investigating the possibility of fixing this erratum.

21. A Microsoft Windows Event Log SNMP warning message is recorded during system boot when Intel Server Control software is installed. This message also appears whenever the SNMP service is stopped and re-started

Problem:	The message, The SNMP Service is ignoring extension key "SOFTWARE\Intel\DMI2SNMP" because it is missing or misconfigured. The indicated key is not required for normal Intel Server Control operation and can be ignored.
Implication:	The user must click past an erroneous error message when starting or stopping the SNMP service.
Workaround:	None.
Status:	Fixed in ISC 3.1.

22. ISC will not launch from Computer Associates* Unicenter TNG 2.4

Problem	Intel® Server Control V3.x will not snap-in to Computer Associates Unicenter TNG 2.4.
Implication	Neither Platform Instrumentation Control, Direct Platform Control, nor the Client System Setup Utility will launch within CA Unicenter TNG 2.4. ISC 3.x will successfully launch within CA Unicenter TNG v2.2.1. CA Unicenter TNG 2.2 is the officially supported version for Intel Server Control Versions 3.0/ 3.1/3.1.1.
Workaround	Launch Intel Server Control components from the Start Menu Programs Intel Server Control sub-folder.
Status	Will not fix.

23. Direct Platform Control remote service partition diagnostics network connection prematurely fails on SKA4-, SRKA4-, SPRKA-, and ISP4400-based systems if it is run from an installation of SKA4 ECO resource kit CD

Problem One of the features of Intel Server Control v3.x server management software is the ability to remotely run diagnostics on the following Intel server systems: SKA4, SPKA4, ISP4400, and SRKA4. The diagnostic software is located on a special service partition area of the remote server system hard drive and may be used as a confidence test for server system hardware and health. A portion of Intel Server Control called Direct Platform Control is used to remotely connect to the service partition from a client system and run the diagnostic software.

In the current release of Intel Server Control v3.0 and v3.1 an anomaly has been discovered that may cause the Direct Platform Control application to prematurely disconnect from the server system while running remote diagnostics.

When a connection has been established there is on-going low-level “heartbeat” communication between the client running Direct Platform Control and the server system. This communication validates the connection between the client and server system. Some subsystem tests of the remote diagnostic package briefly use large amounts of system resources, which may impact the low level “heartbeat” communication between the client and server systems. While these subsystem tests are running, the Direct Platform Control software may believe the communication with the server system has been lost and terminate the connection with the remote server.

Implication This unexpected loss of the connection may leave the server system in an unknown state and may require a local reboot of the server system.

Workaround To eliminate this problem Intel has updated two files. These files are part of the Remote Diagnostic software that is located on the server system and that controls the server subsystem tests. The file modifications eliminate the subsystem tests that are known to cause premature loss of connection. The user can download the updated files from the same location as SKA4 TA-357-1.pdf and use them to replace the files currently on the system. The updated files that should be used are:

XCOMP.PKG	11KB	8/28/00
XQUICK.PKG	4KB	8/28/00

Use the following steps to replace the files on an existing installation.

1. Download and copy the Xcomp.pkg and Xquick.pkg files to a floppy diskette.
2. On the server system, select a local service partition boot by using the BIOS (F2) setup option.
3. The server system will boot to the service partition command prompt.
4. Change directories to the Rdiags folder of the service partition.
5. Save the current Xcomp.pkg and Xquick.pkg files by renaming them. For example, rename Xcomp.pkg Xcomp.old.
6. Insert the floppy disk and copy the new Xcomp.pkg and Xquick.pkg files into the Rdiag folder on the service partition.
7. Reboot the system to the normal operating system.

Status Intel will investigate.

24. The Local Response Agent may reprocess all System Event Log events when the System Event Log is approximately 80% full

Problem	A problem has been identified with Intel Server control reading the System Event Log area. After the SEL is filled to about 80% capacity, the Platform Instrumentation may reprocess all System Event Log entries from the beginning.
Implication	This may cause configured server audio / visual responses or shutdown / power control actions to be performed by the Local Response Agent. When this occurs, it is reading the last processed System Event Log record from the LASTSEL.DAT file as it was placed into the buffer.
Workaround	<p>Create a file named C:\LRA.NOT. Optionally, use a diskette that has this file already on it and put the diskette in the floppy drive right before the operating system boots.</p> <p>The contents of the file and the way in which it is created are not important. It is the existence of a file by this name that disables the software component that responds to the event. After the system is booted, the user must fix the original problem and then delete the LRA.NOT file to allow the software to operate normally.</p> <p>On UnixWare* systems, the user can either create a LRA.NOT file in the root directory or use a diskette as described above.</p>

To prevent LRA loops, the administrator should clear the System Event Log as routine maintenance. The option to clear the SEL is available from the BIOS Setup Utility screen or by using the System Setup Utility.

Status Fix in Intel Server Control 3.5 and all future releases.

25. Direct Platform Control's FRU Manager Chassis and Board attributes labels incorrect under ISC 3.5

Problem The chassis attributes have a label value mismatch.

Implication Incorrect information is displayed.

Workaround No workaround exists for this issue.

Status Intel will investigate.

26. The Direct Platform Control FRU Manager (ISC 3.5) displays only baseboard information

Problem FRU (Field Replacement Unit) information is available only for the baseboard. The Hot-swap Controller, Ppower Distribution Board, power supply 1 and power supply 2 are missing

Implication Not all FRU information is available from Direct Platform Control.

Workaround No workaround exists for this issue.

Status Intel will investigate.

27. Direct Platform Control fails to boot to the Service Partition when connected by DNS (Domain Name Service) under ISC 3.5

Problem Service Partition functionality is not available if when the user connects with a DNS address.

Implication Direct Platform Control may experience problems if a DNS address is used.

Workaround Use an assigned IP address or use an Emergency Management Port / Modem connection to boot to the Service Partition.

Status Intel will investigate.

28. When using CA-TNG Unicenter* 2.4 on ISC 3.5 systems, double-clicking on the ISC WorldView may fail

Problem	When using CA-TNG Unicenter, double-clicking on the ISC WorldView icon in the 2D map may not create ISC server icons.
Implication	CA-TNG Unicenter 2.4 does not always automatically discover ISC WorldView server systems.
Workaround	<p>If this occurs, there are two actions that can be taken that may remedy the situation. Perform action one first. If that is unsuccessful, attempt action two.</p> <p>Steps for action one:</p> <ol style="list-style-type: none">1. Right click My Computer icon on desktop.2. Select the Manage menu item.3. Expand the Services and Applications folder in the Computer Management dialog box.4. Select the Services item.5. Right click Intel TNG-ISC AutoDiscovery service.6. Select Stop.7. Wait for the service to stop.8. Right click Intel TNG-ISC AutoDiscovery service.9. Select Start.10. Review the 2D map in CA-TNG Unicenter for ISC server icons. <p>Steps for action two:</p> <ol style="list-style-type: none">1. Select Start / Programs / Unicenter TNG Framework / Repository / Import Export.2. Select Repository.3. Select the menu item Actions / Import Repository.4. Select the button Add Scripts from Import Repository dialog.5. Navigate to the folder <local drive>:\TNGFW\Bin.6. Select the IscClass.tng file.7. Click the Start button from the Import Repository dialog.8. Click the OK button from the Import Completed dialog.9. Close the Import Repository dialog.10. Close the Unicenter TNG Repository Import Export dialog.11. Optionally, select Yes to save changes.12. Review the 2D map in CA-TNG Unicenter for ISC server icons.
Status	Intel will investigate.

29. Direct Platform Control is unable to connect to a server via modem when the EMP Access Mode is set to "Pre-boot" in the System Setup Utility in ISC 3.5 on SCB2 systems

Problem	Modem (Serial / EMP 2) connections on SCB2 systems in ISC 3.5 cannot be set to "pre-boot" in the SSU. If set to pre-boot, the modem or serial connection will fail.
Implication	The user will not have access to the modem, or serial connection, when the SSU EMP settings have "Access Mode = pre-boot."
Workaround	Set "Access Mode = Always Active" in SSU.
Status	Intel will investigate.

30. ISC 3.5 SCB2 Chassis Intrusion LAN Alerting is non-functional

Problem	The Chassis Intrusion LAN Alerting feature is not functioning.
Implication	The users will be unable to be notified via LAN Alerts if the chassis is opened.
Workaround	Change the default of filter 4 for event trigger from 0x6f to 0x03 using SSU from the BMC LAN Configuration / Options
Status	Intel will investigate.

31. The default "Server" install of Red Hat Linux 7.1 does not allow ISC to function

Problem:	The default "Server" install of Red Hat Linux 7.1 does not install all of the packages needed for baseboard instrumentation to run properly.
Implication:	ISC will not work on Red Hat Linux 7.1 .
Workaround:	Before installing ISC, the user should install the necessary package (compat-libstdc++-6.2-2.9.0.14). To verify whether the package is already installed, at the command line type: rpm -qa grep compat-libstdc++-6.2-2.9.0.14 If the package is present, it will return the package information. If nothing is returned, the package is not present and needs to be installed.

To install the package, insert the Red Hat Linux 7.1 CD into the system.

Mount it by typing at the command line:

```
mount /mnt/cdrom
```

Change to the package directory and install it as follows:

```
cd /mnt/cdrom/RedHat/RPMS
```

```
rpm -i compat-libstdc++-6.2-2.9.0.14.i386.rpm
```

Then unmount the cdrom by typing at the command line:

```
cd /
```

```
umount /mnt/cdrom
```

Verify the package did install (see above), and if present, install ISC.

Status: Intel is investigating the possibility of fixing this erratum.

32. BMC/BIOS will not maintain changes to dynamic IP address unless ISC PI component is running

Problem: If you configure a DHCP (dynamic) IP address for a server using the SSU or Client SSU, the IP address is maintained by the Baseboard Management Controller (BMC). Ordinarily, a floating IP address will expire from time to time and the server is notified by the DHCP server of the new IP address. However, under certain circumstances the BMC/BIOS will retain the expired address, causing a network conflict with the entity that now has been assigned that IP address. This occurs if:

- The ISC PI component is not installed or is not running on the server (PI will maintain the DHCP communication) or
- The OS is not running (e.g., the server is in standby mode or is running only DOS)

Under these circumstances, the BMC may issue LAN Alerts or Gratuitous-ARP broadcasts (which are enabled by default) using the expired IP address, until the server is brought back to running the OS. This can occur on the SCB2, SDS2, or later platforms.

Implication: Network traffic may be slow or exhibit access problems.

Workaround: Configure the DHCP server to issue only a "fixed" DHCP address to any servers using the BMC. Then the DHCP server will always issue the same IP address to those servers. You cannot use the SSU to do this, but must configure it directly on the DHCP server. Alternatively, you can use SSU to assign a Static IP address to the server, and not use DHCP.

Status: Intel is investigating the possibility of fixing this erratum.

33. The Intel Server Control's Platform Instrumentation (PI) agent that synchronizes the Baseboard Management Controller's MAC address with the operating system IP address does not synchronize the addresses on non-US English versions of Windows NT 4.0, SP6

Problem: Non-English installation of Windows NT 4.0 SP6A will not maintain changes to the DHCP IP address unless the ISC Platform Instrumentation (PI) component is running on the monitored server.

Implication: Network traffic to non-English servers may be slow or appear as a network access issue.

Workaround: Configure the DHCP server to issue only a "fixed" DHCP IP address to any servers being monitored with Platform Instrumentation (PI) which talks to the BMC. This way each time the monitored server requests and DHCP IP address it will receive the same one and a conflict with the BMC IP/MAC address won't occur.

Though you can't set such a guaranteed DHCP IP address in the Server System Setup Utility (SSU), you can alternatively assign a static IP address to the server in the SSU instead of using a DHCP IP address.

Status: Intel is investigating the possibility of fixing this erratum.

34. Auto-refresh with the Intel Server Control GUI application, Platform Instrumentation Control, might not work when monitoring a Windows* based server on ISC 3.x

Problem: Auto refresh on the Intel Server Control's Platform Instrumentation Control may not work when monitoring a Windows* based server in ISC 3.x.

Implication: The Platform Instrumentation Control may not accurately reflect the current health sensors for Windows* based servers.

Workaround: The user has two options if this failure occurs:

1. Map the console network drive to a shared drive on the remotely monitored server and configure broadcast alert messages to occur for any sensors that should be monitored locally on your console.
2. Use the <F5> key to refresh the Platform Instrumentation Control's health status of the remote server.

Status: Intel is investigating the possibility of fixing this erratum

35. Intel Server Control 3.5 for SCB2 systems will sometimes not successfully launch with HP OpenView 6.2's IscNode Icon, or it may be excessively slow in launching

- Problem:** Intel Server control may occasionally not successfully launch within HP OpenView 6.2's IScNode Icon, or it may take several minutes to launch.
- Implication:** ISC snap-in integration with HP OpenView may not function after a right mouse click on the IScNode Icon. The tools menu will launch and you can select Intel, but Platform Instrumentation Control is never launched.
- Workaround:** Upgrade all ISC 3.5 SCB2 servers to ISC 3.5.1. This will improve performance and guarantee that Platform Instrumentation Control will launch from the IScNode Icon.
- Status:** Fixed in ISC 3.5.1.

36. Action for some hot swappable power supply events on SDS2, may not be set or handled properly

- Problem:** The ISC Platform Instrumentation Control (PIC) does not support setting any of the control actions, such as "Shutdown the OS, Shutdown the OS and Power off" for the "Power Supply Inserted," "Power Supply Removed," "Power Supply AC lost," "Power Supply AC lost or out-of-range," "Power Supply AC out-of-range, but present" events. In addition, the ISC Platform Instrumentation (PI) may not handle the power supply-related events properly after the removal or insertion of a power supply unit.
- Implication:** The system may not perform the requested control actions set for the power supply sensors.
- Workaround:** None
- Status:** Intel is investigating the possibility of fixing this erratum

37. If a Microsoft Windows NT 4.0 system has the “Services for Macintosh” enabled the Intel Baseboard Service needed for reporting system health will not start correctly

Problem: Intel Baseboard services won't correctly launch on ISC 3.x based systems if the “Services for Macintosh” are enabled under Windows NT services.

Implication: As the operating system is loading the user will see an error message similar to the following:

Event ID 50 – RPC server start failure before baseboard agent hung. The DMI Service Provider v2.62 fails to start DCE (WSDMIDEC.DLL). Without the DMI running, the Intel Baseboard Service is also unable to start.

Workaround: Use the regedit32.exe to edit the following registry keys:

Change the operating system registry as follows.

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\1.20]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Client]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Client\Remoting]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Client\Remoting\DCE RPC]

"Module"="WCDMIDCE.DLL"

"Type"="dce"

"Transports"=hex(7):6e,63,61,6c,72,70,63,00,6e,63,61,63,6e,5f,69,70,5f,74,63,\70,00,6e,63,61,63,6e,5f,73,70,78,00,6e,63,61,64,67,5f,69,70,5f,75,64,70,00,\6e,63,61,64,67,5f,69,70,78,00,6e,63,61,63,6e,5f,6e,62,5f,6e,62,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Client\Remoting\Local]

"Module"="WDMI2API.DLL"

"Type"="local"

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Service Provider]

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current Version\Service Provider\Remoting]

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current
Version\Service Provider\Remoting\DCE RPC]
"Module"="WSDMIDCE.DLL"
"Type"="dce"
"Transports"=hex(7):6e,63,61,6c,72,70,63,00,6e,63,61,63,6e,5f,69,70,5f,74,63,\
70,00,6e,63,61,63,6e,5f,73,70,78,00,00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\DMI 2.0 SDK\Current
Version\Service Provider\Security]
"LocalSecurity"=dword:00000001
"RemoteSecurity"=dword:00000001
"MinConnectLevel"=dword:00000002
"AdminGroupName"="Administrators"
```

Status: Intel is investigating the possibility of fixing this erratum.

38. ISC 3.5 User Guide incorrectly states that concurrent DPC modem and LAN connects are not supported in ISC 3.5

Problem: ISC 3.5 SCB2 supports simultaneous modem and LAN connections with DPC. The documentation is incorrect on SCB2 platforms only.

Implication: Users may think they need to run modem and LAN connections separately with DPC.

Workaround: No workaround exists for this issue.

Status: Intel is investigating the possibility of fixing this erratum.

39. Intel® Server Control 3.5 for SCB2 systems will sometimes not successfully launch with the HP OpenView* 6.2 IscNode Icon, or it may be excessively slow in launching

Problem: Intel Server control may occasionally not successfully launch within the HP OpenView 6.2 IScNode Icon, or it may take several minutes to launch.

Implication: ISC snap-in integration with HP OpenView may not function after a right mouse click on the IScNode Icon. The tools menu will launch and you can select Intel, but Platform Instrumentation Control is never launched.

Workaround: Upgrade all ISC 3.5 SCB2 servers to ISC 3.5.1. This will improve performance and guarantee that Platform Instrumentation Control will launch from the IScNode Icon.

Status: Fixed in ISC 3.5.1.

40. Unable to install ISC 3.5.1 on SDS2 or SCB2 based servers on NetWare 6.0 or Red Hat* Linux 7.2

Problem	I try to install ISC 3.5.1 Platform Instrumentation (PI) on both NetWare 6.0 or Red Hat* Linux 7.2, but neither succeeds. With NetWare* I get TIRPC.NLM errors and the PI on Red Hat* fails to install with the “rpm -I” commands.
Implication	Red Hat* Linux 7.1 and NetWare 5.1 Platform Instrumentation is only supported with original factory released resource CDs.
Implication	None.
Status	Fixed in ISC 3.5.2 for SCB2. Intel plans to add support for Red Hat* Linux 7.2 support and NetWare 6.0 support with the ISC 3.5.2 ECO release for SDS2.

41. The health status displayed in the ISC 3.x Stand Alone Console for Red Hat* Linux 6.2 SBE2 or 7.1 kernel 2.4.7 SMP servers may not properly reflect current health status

Problem	ISC Stand Alone Console information may be incorrect from the server side PI unless a proper /etc/hosts “hostname IP address” setting is configured. However, the Platform Instrumentation Control (PIC) information is updated and correct.
Implication	The ISC Stand Alone console may not accurately reflect the current health status of ISC 3.x for a Red Hat Linux 6.2 SBE2 or 7.1 server. If the server health showed green, or OK status, at discovery, the ISC Stand Alone console icon for the will continue to show an OK status. It will continue to show an OK status even if subsequent server hardware failures occur that would normally be displayed at ISC Stand Alone console. In this case, the ISC Stand Alone console in this case does not see any events, even though an event may have occurred. Information does get written to the /var/log/messages on the server. The ISC PIC GUI status information is updated correctly.
Workaround	Write a cron job that parses /var/log/messages file for PI updates. This information can then be sent to the system administrator for period maintenance. OR Use the contents of the PIC GUI as current information for Linux-based servers. OR

If the Linux server is configured with a static IP address, the following steps are necessary to resolve this issue:

1. Edit the /etc/hosts file on the Linux server with vi, emacs, or an appropriate linux editor.
2. Add the static IP address of the server along with the server hostname, if it not already listed. (i.e. "10.1.1.2 IntelServerHost")
3. Save the file.
4. Restart the "network services" on the server (i.e. "./etc/rc.d/init.d"); A reboot will do this too.

Status Intel is investigating a fix for this erratum.

42. Installing Promise* FastTrak* Log Service may stop the Promise* FastTrak* DMI service integrated with ISC 3.5.2

Problem During the installation of ISC 3.5.2 on the SCB2 server board, ATA SKU, the Promise FastTrak DMI service is installed to provide management information for the on-board Promise ATA-100 controller and disk drives. If the Promise FastTrak Log service is installed following the installation of ISC 3.5.2, the Promise FastTrak DMI service is stopped.

Implication If the Promise FastTrak DMI service is stopped, alerts and information in the CMI database related to the Promise ATA-100 controller and disk drives will be unavailable.

Workaround Restart the Promise FastTrak DMI service.

Status Intel is investigating a fix for this erratum.

43. Uninstalling Promise* software components may also remove Promise* FastTrak* DMI service integrated with ISC 3.5.2

Problem	During the installation of ISC 3.5.2 on SCB2 server board, ATA SKU, the Promise FastTrak DMI service is installed to provide management information for the on-board Promise ATA-100 controller and disk drives. If Promise software components are installed and then uninstalled, the Promise FastTrak DMI service integrated with ISC 3.5.2 may also be uninstalled.
Implication	Without the Promise FastTrak DMI service, alerts and information in the DMI database related to the Promise ATA-100 controller and disk drives will be unavailable.
Workaround	Remove and reinstall ISC 3.5.2.
Status	Intel is investigating a fix for this erratum.

44. With ISC 3.5.2, ISC objects on the CA-TNG 2.4 map may not appear

Problem	After ISC 3.5.2 is installed, the user is unable to see ISC objects on the CA-TNG map.
Implication	User will be unable to see ISC objects on the CA-TNG map.
Workaround	This problem can be fixed by first stopping and then restarting the Intel TNG-ISC Autodiscovery service. If that fails to fix the problem, a system reboot may be necessary. After the second reboot, everything should work properly.
Status	Intel is investigating a fix for this erratum.

45. Application seems to hang after a reboot when serial access mode is set to "Preboot"

Problem	The DPC console may appear to be awaiting BIOS redirection data after a power up or reset over a serial connection if the EMP Access mode is set to "Preboot". This will occur after BIOS has finished POST.
Implication	Users will be unable to continue to access the various managers, there is no indication that redirection is over or that the operating system has booted. With a direct connection, the user will see a blank black screen. With a modem connection, the connection will be lost and the user will be notified.
Workaround	None.
Status	Intel is investigating a fix for this erratum.

46. ISC icons Intel Platform Instrumentation Control (PIC) and Intel DMI Browser may not appear on the ISC Standalone Console connected to Red Hat* Linux 7.1 servers

Problem	The managed computer operating system was installed with a firewall option
Implication	Users will be unable to access PIC and the DMI browser.
Workaround	Select no firewall when installing the operating system.
Status	Intel is investigating a fix for this erratum.

47. Booting to the SDS2 service partition from a remote modem connection may cause the server to hang

Problem	When a modem connection is established from the DPC console and the server is booted to the service partition, the server will hang at the start of ROMDOS. "123456" is displayed at the server and "123" is displayed at the ISC console. This only happens if the LAN cable is attached.
Implication	User will be unable to boot to service partition from a modem connection when the LAN cable is installed.
Workaround	Unplug the LAN cable from the SDS2 server. Or select "F4" at the server console during POST to boot to the service partition.
Status	Intel is investigating a fix for this erratum.

Documentation Changes

Revision History

12/11/01	Added Document items 1 – 6.
6/5/02	Added Errata items 7 – 10

NO.	Plans	DOCUMENT CHANGES
1	Doc. 3.1	Linux setup procedure in the Installation Guide will be enhanced in ISC 3.1
2	Doc. 3.1	ISC translated documents will appear under a documents folder with sub- folders of Chinese, English, German, and Spanish.
3	Doc. 3.1	ISC Install Guide with ISC 3.1 will contain a matrix of the features, based on the server platform.
4	Doc. 3.1	A pull-out Quickstart Guide will be added into the installation of ISC.
5	Doc. 3.1	Context for TCO port error resolution fixed in readme.txt.
6	Doc. 3.1.x Doc. 3.5.x	A clear explanation of the Client System Setup Utility System Setup Manager's User Information File is not documented in the Intel Server Control V3.x TPS, Revision 2
8	Fix ISC TPS Rev 4	Server Management network messages routed through the on-board Network Interface Controller (NIC) may not work if the management port of the NIC is configured as part of a teaming or failover pair that uses DHCP
9	Fix ISC TPS Rev 1.4	By default the watchdog timer is disabled. The TPS incorrectly states it is enabled
10	Fix at next update of Install and PIC guide	ISC v3.5.2 supports Red Hat* Linux 7.1 and 7.2

1. ISC Install Guides Linux installation instructions are confusing

Problem: In ISC 3.0 the Linux installation instructions request several unnecessary reboots. The installation does not mention the `./installme` script, which installs multiple rpms at once.

Implication: Linux server will be reboot unnecessarily and result in an extended downtime during ISC installation.

Workaround: Install ISC as directed but reboot only at the end of the process.

Status: Concise steps will be updated in the ISC 3.1 Installation Guide.

2. ISC Document directory structure is confusing

- Problem:** In ISC 2.x and ISC 3.x, the addition of language support for Chinese, Spanish, and German created confusion in determining the correct readme.txt, errata.txt, Install Guide, and product guide to open.
- Implication:** The user may open the file for the wrong language.
- Workaround:** Understand the difference between the Language Resource prefix of ENU (US English), ESP (Spain Spanish), CHS (Simplified Chinese), or DEU (Germany German).
- Status:** To be fixed in ISC 3.1

3. Server system / ISC functionality confusion

- Problem:** Users are confused about the functionality available with the different server systems. They do not know if they need a service partition, or if they can use EMP, paging, LAN Alerts, DPC over LAN, and Out of Band Management. Functionality varies greatly between systems, from SKA4-based systems that have all functionality and SBT2/SLT2-based systems, which provide none of the above features.
- Implication:** The user may waste time trying to implement a feature that is not available on their system.
- Workaround:** None.
- Status:** Documentation will be added to the readme.txt and the ISC Installation Guide to summarize system features in ISC 3.1.

4. ISC no longer includes a Quick Start Guide

- Problem:** Users report that it was easier and faster to install ISC when a Quick Start Guide was included with the product.
- Implication:** ISC installations are time-consuming due to the lack of a Quick Start Guide.
- Workaround:** None.
- Status:** An ISC Quick Start Guide insert will be included with ISC 3.1 and will also be available at <http://support.intel.com>.

5. The readme.txt does not properly express/remedy DPC over LAN system hangs with excessive TCO port traffic over the SKA4 based system onboard NICs in NetWare and Linux 6.2 SBE2

Problem: The readme.txt does not correctly describe that, under certain situations, running DPC over LAN to perform a system reset may cause a system timeout (hang) if enhanced TCO (Total Cost of Ownership) drivers are not loaded. This applies to RedHat 6.2SBE2 and NetWare* 4.x/5.x SKA4 based systems.

Implication: The system hangs due to inefficient NIC drivers.

Workaround: Download and upgrade drivers for all SKA4-based systems, including systems running Windows operating systems. The drivers are available from <http://support.intel.com/support/motherboards/server/isc/software.htm>

Status: The readme.txt file will be updated in ISC 3.1 documentation.

6. A clear explanation of the Client System Setup Utility System Setup Manager's User Information File is not documented in the Intel Server Control V3.x TPS, Revision 2

Problem: The Intel Server Control V3.x Technical Product Specification contains no explanation on the use of a User Information File (.UIF). When a .UIF file is run remotely via the Service Partition from the Client System Setup Utility, it concurrently loads the BMC firmware, HSC firmware, and the BIOS. This streamlines the process by saving the time of connecting and upgrading each component individually. With no documentation available, it is necessary to load each component individually.

Implication: Without this documentation, it is difficult to determine the format of the UIF file.

Workaround: The UIF text file is used by the SUM to determine the order and type of update for each .HEX file. The .UIF contains four lines in each section. The first is a platform line, delimited by brackets. The second line, also in brackets, is the version number of the package being used. The last line is a data line in the format:

```
Hex<number of file>=<filename>
Update<number of file>=<type of update>
```

The only type of update available is OP, which represents the operational code.

```
*****START EXAMPLE UIF FILE*****
[L440GX+]
[05]
Hex0=LWBMC01.HEX
Update0=OP
```

```
Hex1=LWHSC12.HEX
```

```
Update1=OP
```

```
Hex2=LWFPC12.HEX
```

```
Update2=OP
```

```
Hex3=B-0015.BIO
```

```
Update3=BIO
```

```
*****END EXAMPLE UIF FILE*****
```

Status: Concise steps will be included in future releases of the Intel Server Control V3.x Technical Product Specification.

7. In the errata.txt file, item 14 under section K is not an issue in ISC 3.5

Problem Errata.txt item 14 under section K has been fixed in production ISC 3.5. The errata.txt indicated that the string in the PEP screen of CSSU is not pulled into Paging Configuration in ISC PIC.

Implication Users may think the paging string is being read incorrectly, but the software is now working as designed.

Workaround No workaround exists for this issue.

Status The errata.txt was frozen prior to the production software release. This content will be removed from future errata.txt content.

8. Intel Server Management network messages routed through the onboard Network Interface Controller (NIC) may not work if the management port of the NIC is configured as part of a teaming or fail-over pair that uses DHCP

Problem You can configure the server Baseboard Management Controller (BMC) to use an IP address for server management network messages. ISC software on the sever will ordinarily synchronize the operating system IP address with the BMC IP address. However, if the NIC is part of a teaming or fail-over pair that uses DHCP (Dynamic Host IP addressing), ISC may not be able to synchronize the BMC with the operating system network configuration information.

Implication Without the proper network configuration information, the BMC may not recognize valid server management network messages.

Workaround	Do not use the server management assigned NIC as part of the teaming pair. Install an add-in NIC for use as the part of the teaming or fail-over pair. OR Use a static IP address for the server's server management assigned NIC if it is to be included in a teaming or fail-over pair.
Status	Corrected in ISX 3.x TPS, revision 1.4. See Section 1, paragraph 2.2.2 and Section 11, Chapter 3.

9. By default the watchdog timer is disabled

Problem	By default the watchdog timer is disabled. Section 8, paragraph 3.1.3 incorrectly states that the watchdog timer is enabled by default.
Implication	None
Workaround	None
Status	Corrected in ISC 3.x TPS, revision 1.4. See Section 8, paragraph 3.1.3

10. ISC v3.5.2 supports Red Hat* Linux 7.1 and 7.2

Problem	The ISC v3.5.2 Install Guide and Platform Instrumentation Control Console User's Guide calls out support for Red Hat Linux 6.2 SBE and 7.1. These references should be changed to Red Hat Linux 7.1 and 7.2.
Implication	ISC v3.5.2 supports Red Hat Linux 7.1 and 7.2
Workaround	None
Status	To be updated in the next revision of the ISC v3.5.2 Install Guide and Platform Instrumentation Control User Guide.

Glossary

Term/Acronym	Description
82559	Intel 10/100 Mbps Ethernet controller.
AF	Application Framework
AIP	Advanced Integrated Peripheral
AMS	Alert Management System
ANSI	American National Standard Institute
API	Advanced Programmable Interrupt
APM	Advanced Power Management
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
ASPI	Advanced SCSI Programming Interface - An interface specification developed by Adaptec, Inc., Milpitas, CA, that provides a common language between drivers and SCSI host adapters. Drivers written to the ASPI interface can access peripherals that reside on different versions of SCSI host adapter hardware.
BCV	Boot Connection Vector
BIOS	Basic Input Output System
BLA	BMC LAN-Alerts
BMC	Baseboard Management Controller – provides monitoring, alerting, and logging of critical system information obtained from embedded sensors on the baseboard.
BPS	Bits Per Second
BYO	Build Your Own
CAF	Client Application Framework
CD	Carrier Detect
CHAP	Challenge Handshake Authentication Protocol
CMOS	Complementary Metal-Oxide Semi-Conductor
CPU	Central Processing Unit
CR	Carriage Return
CSR	Configuration Save/Restore
CSSU	Client System Setup Utility
CTS	Clear To Send
DCE	Distributed Computing Environment - A set of programs from The Open Group that allows applications to be built across heterogeneous platforms in a network. DCE includes security, directory naming, time synchronization, file sharing, RPCs and multithreading services. DCE source code is licensed to major vendors, who sell the executable programs to their customers.
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-Line Memory Module
DMA	Direct Memory Access
DMTF	Desktop Management Task Force
DMI	Desktop Management Interface
DNS	Domain Name System
DPC	Direct Platform Control
ECC	Error Correcting Code
EFI	Extensible Firmware Interface
EMP	Emergency Management Port
ESCD	Extended System Configuration

Term/Acronym	Description
ESG	Enterprise Server Group
ESMC	Enterprise Server Management Console
FDC	Floppy Disk Controller
FPU	Floating Point Unit
FRB	Fault Resilient Boot – a set of BIOS and BMC algorithms and hardware support that allows an MP system to boot in case of failure of the bootstrap processor under certain circumstances.
FRU	Field Replaceable Unit
FSB	Front-Side Bus
FTP	File Transfer Protocol
GUI	Graphical User Interface
GUID	Global Unique Identifier
IA	Intel Architecture
IANA	Internet Assigned Numbers Authority
ICMB	Intelligent Chassis Management Bus – a character-level transport for inter-chassis communications between smart chassis
IDE	Integrated Drive Electronics – an interface for mass storage devices in which the controller is integrated into the device.
IMB	Intelligent Management Bus
IP	Internet Protocol
IPL	Initial Program Load
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
IPX	Internetwork Packet Exchange - A NetWare communications protocol used to route messages from one node to another.
ISA	Industry Standard Architecture
ISC	Intel® Server Control
LAN	Local Area Network
LCD	Liquid Crystal Display
LDSM	LANDesk® Server Manager
LED	Light Emitting Diode
LF	Line Feed
LRA	Local Response Agent
LSC	LANDesk® Server Control
LUN	Logical Unit Number
MAC	Media Access Control
MBM	Multiboot Manager
MD2	Message Digest Version 2
MDI	Multiple Document Interface - a Windows API that enables programmers to easily create applications with multiple windows.
MIB	Management Information Base
MIF	Management Information Format
MRU	Most Recently Used
MTA	Modular Test Architecture
MUX	Multiplexer
NIC	Network Interface Controller
NLM	Software that runs in a NetWare server. Although NetWare servers store DOS and

Glossary

Term/Acronym	Description
	Windows applications, they do not execute them. All programs that run in a NetWare server must be compiled into the NLM format. They are typically written in C and use Novell's libraries. NLMs began with NetWare 3.x. The earlier NetWare 2.x counterpart was known as a Value Added Process (VAP).
NMI	Non-Maskable Interrupt – The highest priority interrupt in the system, after Platform Management Interruption (PMI). This interrupt has traditionally been used to notify the operating system of fatal hardware errors, such as parity errors and unrecoverable bus errors.
NV	Non Volatile
OEM	Original Equipment Manufacturer
OID	Object Identifier
ONC	Open Network Computing - A family of networking products from SunSoft for implementing distributed computing in a multivendor environment. Includes TCP/IP and OSI protocols, NFS distributed file system, NIS naming service and TI-RPC remote procedure call library. ONC+ adds Federated Services, which is an interface for third-parties to connect network services into the Solaris environment.
OS	Operating System
PBC	Processor Board Controller
PCI	Peripheral Component Interconnect
PCXB	PCI to Xpress Bus Bridge
PDU	Protocol Data Unit
PEF	Platform Event Filtering. Name for the feature where the BMC implements a table of Event Filters, compares incoming platform events against the filters, and generates an action - such as a page – when a match is found.
PEM	Platform Event Manager
PEP	Platform Event Paging. Name for the feature where the platform management hardware built into the baseboard uses an external modem to autonomously page when selected platform events occur.
PET	Platform Event Trap
PI	Platform Instrumentation
PIC	Platform Instrumentation Control
PIT	Programmable Interval Timer
POST	Power On Self Test
PPP	Point-To-Point Protocol
PWM	Password Manager
PXE	Preboot Execution Environment
RAM	Random Access Memory
RAMDAC	RAM Digital-To-Analog Converter
RAP	Remote Access Protocol
RCM	Resource Configuration Manager
RPC	Remote Procedure Call - A programming interface that allows one program to use the services of another program in a remote machine.
RSA	Remote Sensor Access
RTC	Real Time Clock
RTS	Request To Send
SCSI	Small Computer Systems Interface
SDR	Sensor Data Records
SDK	System Design Kit
SDMS	Scientific Data Management System

Term/Acronym	Description
SEL	System Event Log
SIMM	A memory insert for system RAM (older technology).
SIO	Super I/O
SMB	Server Management Bus
SMBIOS	Server Management BIOS
SMI	Server Management Interrupt
SMM	Server Monitor Module
SMS	Server Management Software
SNMP	Simple Network Management Protocol.
SSU	System Setup Utility
SUM	System Update Manager
SVGA	Super Video Graphic Array
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol / Internet Protocol
TPS	Technical Product Specification
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol.
UI	User Interface
UDP	Universal Datagram Packet
USB	Universal Serial Bus
UTC	Universal Time Coordinated
UUT	Unit Under Test
VGA	Video Graphic Array
VID	Voltage ID
VMU	Visual Memory Unit
VRM	Voltage Regulating Modules
WAN	Wide Area Network
WE	Write Enable
WfM	Wired-for-Management
WOL	Wake-On-LAN
XPC	X Performance Characterization - A graphics benchmark that tests X Window performance. In 1993, the XPC project group created Xmark93, which rates a broad set of X functions in Xmarks.