



Intel[®] Server Management v5.x

Technical Product Specification

Intel order number C20141-002

Revision 2.0

March, 2004

Enterprise Platforms and Services Marketing

Revision History

Date	Revision Number	Modifications
January 2003	1.0	Initial release.
March 2004	2.0	Added release up to ISM 5.8 for SE7210TP1-E server platform support.

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 Management v5.x 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.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Intel, Pentium, Itanium, and Xeon are trademarks or registered trademarks of Intel Corporation.

*Other brands and names may be claimed as the property of others.

Copyright © Intel Corporation 2004.

Table of Contents

1. Introduction	17
2. Intel Server Management Overview.....	18
3. Platform Management Technology.....	20
4. Platform Instrumentation Control	21
4.1 Product Objectives	21
4.2 Internationalization	21
4.3 Security	22
4.4 Installation	22
4.4.1 Registry Keys.....	22
4.4.2 Class Names	23
4.4.3 Tree Templates.....	24
4.5 GUI Container	25
4.6 Navigation Pane.....	27
4.6.1 Health.....	27
4.7 Group Information	28
4.8 Presentation Pane.....	28
4.8.1 Sensor Settings Tab Page.....	30
4.8.2 Sensor Status Tab Page	31
4.8.3 Inventory Information Tab Page	32
4.9 Sensor Controls.....	32
4.10 Chassis	33
4.11 Fan.....	33
4.12 Memory Array	34
4.13 Memory Device.....	35
4.14 PCI HotPlug Device.....	36
4.15 Power Supply	36
4.16 Power Unit.....	37
4.17 Processor.....	37
4.18 System Information	38
4.18.1 Field Replaceable Unit	38
4.18.2 Operating System	39

4.18.3	System BIOS	39
4.18.4	System Event Log.....	39
4.19	System Slots	40
4.20	Temperature.....	41
4.21	Third Party Instrumentation	42
4.22	Voltage.....	44
4.23	PIC Dialogs.....	45
4.24	Options Dialog.....	45
4.25	Restoring Factory Defaults	45
4.26	Watchdog Timer Dialog	46
4.27	Paging Configuration Dialog.....	46
4.28	Email Alert Configuration Dialog.....	48
4.29	Test Email Dialog.....	48
4.30	ICMB Configuration Dialog	48
4.31	ICMB Remote Server(s) Dialog.....	49
4.32	Intel® SmaRT Tool Interface	50
4.32.1	Launching Intel® SmaRT Tool above the FRU Level.....	50
4.32.2	Launching SmaRT Tool at the FRU Level.....	50
4.32.3	Parameters Passed to SmaRT Tool.....	50
5.	Platform Instrumentation	51
5.1	Functional Specifications for Intel® Server System SHG2.....	51
5.1.1	Baseboard Fan Management	51
5.1.2	System Event Log.....	51
5.2	Functional Specification for the Intel® Server Chassis SC5200.....	52
5.2.1	Sensor Monitoring	52
5.2.2	Ambient Temperature Based Fan Speed Control	52
5.3	Functional Specifications for Intel® Server System SSH4	52
5.3.1	Baseboard Fan Management	52
5.3.2	System Event Log.....	52
5.3.3	Alerting – PEF and Alert Policies	53
5.4	Functional Specifications for Intel® Server Systems SE7500WV2 and SE7501WV2	53
5.4.1	Baseboard Fan Management	53
5.4.2	System Event Log.....	53
5.5	Functional Specification for the Intel® Server Chassis SR1300.....	53

5.5.1	Sensor Monitoring	53
5.5.2	Ambient Temperature Based Fan Speed Control	54
5.6	Functional Specification for the Intel® Server Chassis SR2300.....	54
5.6.1	Sensor Monitoring	54
5.6.2	Ambient Temperature Based Fan Speed Control	54
5.7	Functional Specifications for Intel® Server Board SE7501BR2	54
5.7.1	Baseboard Fan Management	54
5.7.2	System Event Log.....	54
5.8	Functional Specification for the Intel® Server Chassis SC5250-E.....	55
5.8.1	Sensor Monitoring	55
5.9	Functional Specification for the Intel® Server Chassis SR1350-E.....	55
5.10	Functional Specifications for Intel® Server Board SE7501HG2	55
5.10.1	Baseboard Fan Management.....	55
5.10.2	System Event Log.....	55
5.11	Functional Specifications for Intel® Server Board SE7210TP1-E.....	55
5.11.1	Baseboard Fan Management.....	55
5.11.2	System Event Log.....	56
5.12	Functional Specification for the Intel® Entry Server Platform SR1325TP1-E	56
6.	Direct Platform Control	57
6.1	Supported Communication Components.....	57
6.2	Client Configuration	58
6.2.1	Serial Communication	58
6.2.2	LAN Communication.....	58
6.3	Server Configuration.....	58
6.3.1	Serial Communicaton	58
6.3.2	LAN Mode.....	58
6.3.3	Configuring Console Redirection.....	58
6.3.4	Configuring Server Serial Communications	59
6.3.5	Configuring LAN Connections.....	59
6.3.6	Creating a Service Partition	59
6.4	Modes of Operation	59
6.4.1	EMP Mode.....	60
6.4.2	DPC over LAN Mode.....	60
6.4.3	Redirect Mode.....	60

6.4.4	Service Partition Mode	61
6.5	Making a Connection	61
6.6	Security	62
6.7	Server Power Control	63
6.8	User Interface	63
6.9	Title Bar	64
6.9.1	Server	64
6.9.2	Line	64
6.10	Status Bar	64
6.10.1	Mode	64
6.10.2	OS (Operating System)	64
6.11	DPC Console Menu	65
6.11.1	File Menu	65
6.11.2	View Menu	67
6.11.3	Action Menu	68
7.	Client System Setup Utility	72
7.1	Client Application Framework	72
7.1.1	Command Line Options	72
7.1.2	Launching the Client SSU	72
7.2	CSSU Functional Specification	73
7.2.1	Console Redirection Features	74
7.3	CSSU Managers	75
7.3.1	MBM Manager	75
7.3.2	PWM Manager	75
7.3.3	SEL Manager	75
7.3.4	SDR Manager	75
7.3.5	FRU Manager	75
7.3.6	SUM Manager	76
7.3.7	PEP Manager	79
7.3.8	CSR Manager	79
7.3.9	Save Configuration to File Button	79
7.3.10	Restore Configuration from File Button	80
7.3.11	Save Configuration Data	80
8.	ISM Install / Uninstall	81

8.1	Extensibility, Customization.....	81
8.2	Remote Installation of Console/Server Components.....	81
8.3	Supported Operating Systems.....	81
8.4	Internationalization.....	82
8.5	Installation User Interface.....	82
8.5.1	Starting ISM Setup.....	82
8.5.2	Installation Types.....	82
8.5.3	License Agreement.....	82
8.5.4	Feature Selection.....	82
8.5.5	Remote Destination Selection.....	84
8.5.6	Local Destination Selection.....	85
8.5.7	System Shutdown Screen.....	86
8.5.8	Log File.....	86
8.6	Silent Installation.....	86
8.7	Uninstall ISM Features from Local Win32 System.....	88
8.8	Uninstall ISM from Remote System (Win32, OpenUnix, NetWare).....	88
8.9	Recommended Files and Windows Registry Tree Structures.....	88
8.9.1	Source Files.....	88
8.9.2	Windows Registry.....	88
8.10	Creating Configuration Files.....	89
8.10.1	Setup Control File: XXXISCSetup.inf.....	89
8.10.2	Default Install Path.....	89
9.	Security.....	90
9.1	Security Implementation.....	90
9.2	Platform Instrumentation.....	90
9.2.1	New Authentication Scheme.....	91
9.2.2	LRA Notification-Only Control.....	91
9.2.3	SNMP Read-only Access Control.....	91
9.3	DPC/CSSU Security.....	91
9.4	LAN Based Security (IP Filtering).....	92
9.5	Invalid Password Handling.....	92
9.6	Session Expiration.....	92
9.7	System Setup Utility.....	92
9.8	Password Length and Character-set Support.....	92

10. Service Partition	94
10.1 External Dependencies	94
10.2 BMC Firmware	94
10.3 BIOS Support for Service Boot	95
10.4 BIOS Console Redirection	95
10.5 Intel Server Management Console	95
10.6 Service Partition Type	95
10.7 Firmware / BIOS Service Boot Support	96
10.8 Remotely Initiating Service Partition Boot	96
10.9 Local Boot from Service Partition.....	96
10.10 Service Partition Installation	97
10.11 Scan And Present Bits	98
10.12 Service OS / System Resource CD Hidden Partition Support.....	98
10.13 Service OS Initialization.....	98
10.14 TCP/IP Stack for Remote Communication.....	98
10.15 Network Initialization	99
10.16 PPP IP Address Configuration	99
10.17 PPP Serial Port Configuration.....	99
10.18 LAN Controller Configuration.....	100
10.19 Remote Service Agent	100
10.20 RSA Initialization.....	101
10.21 Execution of DOS-based Utilities	102
10.22 Modem-based Security	102
10.23 LAN-based Security (IP Filtering)	102
11. Enterprise System Management Console Integration.....	103
11.1 Supported Enterprise System Management Consoles	103
11.2 Supported Operating Systems.....	103
11.3 Components	103
11.3.1 Console Tools Manager	104
11.3.2 ESMC Agents.....	104
11.3.3 ISM Application Plugins	104
11.4 ESMC Functionality	104
11.5 CTM/Agent Connection	104
11.6 CTM/Plugin Connection.....	105

11.7	Server Discovery.....	105
11.8	Server Health.....	106
11.9	ISM Application Launch.....	106
11.10	Operation.....	106
11.10.1	Hewlett Packard OpenView Network Node Manager Server Health Display And Update	106
11.10.2	Computer Associates Unicenter TNG Server Health Display And Update.....	106
11.11	Levels Of Discovery.....	107
11.11.1	First Level Discovery.....	107
11.11.2	Second Level Discovery.....	107
12.	LAN Alert Viewer	108
12.1	Alert Viewer.....	108
12.2	Simple Network Management Protocol Trap and LANAlert	110
12.3	Header	110
12.4	Protocol Data Unit (PDU)	111
12.5	Variable Bindings Field.....	111
12.6	Alert Configuration	112
12.7	Platform Event Manager.....	112
13.	Platform Event Paging	112
13.1	Page Configuration.....	112
13.2	Platform Event Manager.....	112
14.	Intelligent Chassis Management Bus (ICMB)	112
14.1	ICMB Requirements	112
14.1.1	Setting Up an ICMB Connection.....	112
14.1.2	Configuring the Management Point Server	112
14.2	Setting Up ICMB	112
14.2.1	Discovering Remote ICMB Systems	112
14.2.2	Viewing and Managing Viewing Remote ICMB Systems.....	112
15.	Command Line Interface / Serial Over Lan	112
15.1	Serial Over LAN.....	112
15.2	Command Line Interface.....	112
15.3	SOL/CLI Client Architecture	112
15.3.1	Dpccli Client Program	112
15.3.2	Network Proxy	112
15.4	Dpccli Command Line Syntax.....	112

15.5	.dpccliirc File Format.....	112
15.6	CLI Command Vocabulary.....	112
15.7	Alarm -s	112
15.8	console [-f].....	112
15.9	exit and quit.....	112
15.10	id 112	
15.11	network [mac ip subnet gateway]	112
15.12	Power -s	112
15.13	power on [-c].....	112
15.14	power off [-f].....	112
15.15	reset [-f] [-c]	112
15.16	sel [-c] [-num]	112
15.17	sensors [-v] [-c] [-f ok nc cr nr us] [volt temp power fan].....	112
15.18	diagint [-c].....	112
15.19	boot [-f] [-c] (normal service)	112
15.20	service (console exit ftp (start stop))	112
15.21	set (prompt= <i>text</i> prefix= <i>text</i>)	112
15.22	Identify [-on [# of seconds]] [-off]	112
15.23	version	112
15.24	help [<i>CLI command</i>].....	112
15.25	Network Proxy Command Line Syntax	112
15.26	Operation Environment	112
15.27	Installation.....	112
15.27.1	dpccli.....	112
15.27.2	dpcproxy	112
16.	Native Command Line	112
16.1	Native Command Line Overview.....	112
17.	Standalone SNMP Subagent Introduction	112
17.1	SNMP Subagent Description.....	112
17.2	General Architecture.....	112
18.	Install/Uninstall.....	112
18.1	Preparing for Installation.....	112
18.1.1	Linux Systems.....	112
18.1.2	Windows Systems.....	112

18.2	Install Framework.....	112
18.2.1	Window-based Install.....	112
18.2.2	Install for Linux System	112
18.3	Uninstall.....	112
19.	Functionalities.....	112
19.1	Access Sensor Data	112
19.2	View and Modifying Threshold Settings.....	112
19.3	System Health Status.....	112
20.	MIB Structure	112
20.1	Version Compatibility.....	112
20.2	Compliancy.....	112
20.3	MIB Extensions and Changes	112
20.4	MIB Definitions	112
20.4.1	Base OID.....	112
20.4.2	Event Configuration Settings.....	112
20.4.3	IPMI Information.....	112
21.	SNMP Events	112
21.1	Event Design Methodology.....	112
21.2	Event OID Information	112
22.	Coexistence with ISM DMI Based SMA.....	112
23.	Configurable Settings.....	112
Appendix 1: Server Board SHG2 Sensors.....		112
Appendix 2: Server System SSH4 Sensors.....		112
Appendix 3: Server Board SE7500WV2 Sensors.....		112
Appendix 4: Server Board SE7501WV2 Sensors.....		112
Appendix 5: Server Board SE7501BR2 Sensors.....		112
Appendix 6: Server Board SE7501HG2 Sensors.....		112
Appendix 7: Server Board SE7210TP1-E Sensors.....		112
Appendix 8: DMTF Groups and OIDs.....		112
	Windows/Open Unix/NetWare.....	112
Linux	112	
Intel	112	
DMTF	112	
Appendix 9: ISM Feature Matrix.....		112

Appendix 10: ISM v5.5 Features112
 Command Line Interface Enhancements.....112
 System ID LED Control112
 Native Command Line112
 SNMP v3.0112
Appendix 11: ISM v5.5.6 Features112
Appendix 12: ISM v5.5.7 Features112
Appendix 13: ISM v5.8 Features112
Glossary.....112
Reference Documents.....112

List of Figures

Figure 1. PIC Container.....	26
Figure 2. Navigation Pane	27
Figure 3. DPC Console Main Window	63
Figure 4. User Interface to CSSU	73
Figure 5. Main Window Toolbar Buttons	74
Figure 6. Example .UIF File.....	76
Figure 7. Installable Features	83
Figure 8. Fusion TCP/IP Network Stack.....	99
Figure 9. Remote Service Agent Overview.....	101
Figure 10. LanAlert Viewer	109
Figure 11. LanAlert Details Dialog Box	110
Figure 12. Enabling ICMB Features	112
Figure 13. Displaying Remote Server Information.....	112
Figure 14. CLI Interface Flowchart.....	112
Figure 15. SNMP Agent Architecture	112

List of Tables

Table 1. DMI Class Registry Keys	23
Table 2. Navigation Tree Item Attributes	25
Table 3. Presentation Pane.....	28
Table 4. Parameters Passed to SMaRT Tool.....	50
Table 5 Console Redirection Submenu Options	58
Table 6. Command Line Options	72
Table 7. ASCII Character Codes Supported by the DPC Password.....	93
Table 8. LANAlert Viewer Buttons	108
Table 9. Protocol Data Unit Fields	111
Table 10. Variable Bindings Fields	111
Table 11. MIB Event Configuration Usage	112
Table 12. Managed System Information Below Baseboard Group 5.....	112
Table 13. Predefined Attribute Types in the MIB	112
Table 14. SNMP Events	112
Table 15. OID Event Catagories	112

< This page intentionally left blank. >

1. Introduction

Intel® Server Management (ISM) 5.x is the server management software for IA-32 servers from the Intel Enterprise Product Group's server offerings. This Technical Product Specification (TPS) provides technical details on the implementation of Intel Server Management v5.x. This document does not discuss user operation; the Installation and User Guide that accompanies the software is available for functional information.

The Readme.txt and Errata.txt documents that accompany the software provide the latest information about the software. After release of the software, monthly specification updates are appended to this document and that is the source of ongoing current information.

This ISM 5.8 release of ISM features support for the Intel® Server Board SE7210TP1-E. This platform uses a National Semiconductor* PC87431M mini-Baseboard Management Controller (mBMC) as compared to the other servers supported by ISM which uses a full BMC.

Consequently, managing the Server Board SE7210TP1-E with this version of ISM supports a subset of the management functionality present when managing server platforms that house the full BMC. Throughout this manual, server management features not supported when managing the Server Board SE7210TP1-E are noted. See Appendix 13 for a further description of features supported on the Server Board SE7210TP1-E.

Note: For additional information, see Intel Server Management Installation and User's Guide provided on the ISM CD. See also the readme files and documentation that accompanies your specific release of ISM.

2. Intel Server Management Overview

Intel bundles Intel® Server Management (ISM) with all EPG server systems to provide a differentiated management solution. Intel Server Management software provides a suite of components that inform users of the server health and operational condition. ISM also provides for remote access regardless of the operating system or its condition. Remote access is also independent of server power state (On or Off). The access path to the server can be LAN, modem, or direct connect. The design of ISM 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 Intel® Server Management software
- Single installation framework
- The components within ISM will be modular in nature for easy integration into existing OEM management stacks, with well documented interface points for OEM integration and extensibility
- Each component within ISM plugs into a common ISM framework that allows them to snap into selected Enterprise System Management Console (HP Openview*, CA Unicenter TNG*).
- Each component within ISM supports standalone execution.

Intel Server Management consists of the following user-visible components:

- Platform Instrumentation Control (PIC)
- Direct Platform Control (DPC)
- System Setup Utility (SSU)
- Client System Setup Utility (CSSU)
- LAN Alert Viewer
- Command Line Interface (CLI) / Serial Over LAN (SOL) (System Dependent)

All components rely on a foundation of hardware and firmware support supplied by the Platform Management Technology. An overview of this technology is provided in section 3.

Intel Server Management applications use the following access paths to provide management data to the remote console:

- Platform Instrumentation Control (PIC) communicates through a LAN connection to the Platform Instrumentation (PI) resident on the server. Standard DMI/RPC protocols are used for the communication. See Section 4 for information about Platform Instrumentation Control and Section 5 for information about the Platform Instrumentation.
- Direct Platform Control (DPC) communicates directly to the server's firmware using IPMI messaging. The BMC accepts this connection through the LAN using the NIC TCO port, direct serial interface, or a modem. The NIC TCO port is a special side-band interface from the NIC to the BMC. See Section 6 for information on Direct Platform Control.

- The Client System Setup Utility (CSSU) communicates directly to the server firmware using IPMI messaging. The BMC accepts this connection through the LAN using the NIC TCO port, direct serial interface, or a modem. Once the connection is established, the CSSU will reboot the server to a local Service Partition. When connected to the Service Partition, CSSU uses additional networking (PPP or TCP/IP to provide additional functions.

Note: The Service Partition must be installed during system setup. The Service Partition and CSSU are not supported on the Server Board SE7210TP1-E.

See Section 7 for more information about the CSSU and Section 10 for information about the Service Partition.

- The LAN Alert Viewer is a Java* application that can receive and display IPMI PET traps that are generated by the BMC firmware. These traps are sent over the LAN to the management console. See Section 12 for information about the LAN Alert Viewer.
- Serial over LAN (SOL) is the capability of some servers to redirect serial port B over the LAN. SOL uses the CLI proxy to decode this serial data. See Section 15 for SOL information.

Note: SOL is not supported on the Server Board SE7210TP1-E.

- Platform Instrumentation (PI) components are server operating system resident agents that monitor the server health and provide information and control functions to the ISM management consoles. Platform Instrumentation can be used to manage servers running Windows* 2000 and Windows 2003, Red Hat* Linux, Novell* NetWare and OpenUnix* operating systems. See Section 5 for information about the Platform Instrumentation.

PIC, DPC, CSSU, and the LAN Alert Viewer can be used on a Microsoft* Windows* operating system. CLI can be used on either a Windows operating system or on a Red Hat Linux operating system. The operating systems supported may vary by server and by software release; see the Readme.txt file for each server.

All ISM components support integration under multiple management consoles and under the ISM Standalone framework. OEMs can select one or more individual components to integrate directly into their proprietary management consoles or into an Enterprise System Management Console. The ISM Standalone framework provides a solution for customers who do not wish to integrate into a management console infrastructure.

The integration with management consoles is supported on the Windows versions of the management consoles.

3. Platform Management Technology

All ISM 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)	IPMI is a set of specifications that defines a standardized, message-based interface to platform management controllers. This includes specifications of command (message) sets, interface protocols, and descriptive records for the platform management subsystem. IPMI messaging is used by the platform management controllers to communicate to each other and to the platform instrumentation software. The ISM 5.x release supports version 1.5 of the IPMI specification.
Intelligent Platform Management Bus (IPMB)	This is a set of specifications that define a management bus inside the system chassis. The management bus allows platform management controllers on various system boards to communicate using IPMI messages. The bus provides a standardized way for chassis board management hardware and value-added management devices, such as remote management cards, to connect to the platform management subsystem on the baseboard.
Intelligent Chassis Management Bus (ICMB) ¹	The ICMB is an external management bus that interconnects platform management subsystems in multiple chassis. The ICMB specification defines the characteristics of the bus, how a management controller communicates on the bus, and how to provide a 'bridge' function that allows messages to be sent between the IPMB and ICMB.
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) ¹	This hardware support allows for direct serial (RS-232) access, or remote access (using an external modem) to the platform management subsystem during various stages of system operation, including the times when the system is powered off. This interface and the protocol is part of the IPMI 1.5 specification.
Platform Event Alerting	The Platform Event Alerting features allow the platform management subsystem to proactively alert the administrator of critical system failures. These features are implemented in hardware and firmware and work even when the host operating system is down.
Platform Event Paging ¹ BMC LAN Alert	With Platform Event Paging (PEP), alerts are sent to a numeric pager. Alerts are sent through the LAN.

¹ ICMB, EMP, and Platform Event Paging are not supported on the Intel® Server Board SE7210TP1-E.

4. Platform Instrumentation Control

Platform Instrumentation Control is the server management user interface that provides real time monitoring and alerting for server hardware sensors. PIC uses the standard Desktop Management Interface (DMI) 2.0 framework for managing hardware components.

4.1 Product Objectives

Intel targeted PIC for the departmental LAN environment (file/print/application servers). Platform Instrumentation Control allows system administrators to do the following:

- 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
- Launch Intel® SMaRT Tool, which provides server component (FRU) Remove & Replace (R&R) information and ordering information.

PIC provides software-only, in-band server management for the LAN administrator. PIC is design to manage a single server. Enterprise and workgroup applications provide LAN-based server discovery services. Enterprise System Management Console (ESMC) integration allows Platform Instrumentation to be discovered on the server. A launch point for PIC will be created on the PI enabled servers. See Section 11 for information about Enterprise System Management Consoles and See Section 5 for details about Platform Instrumentation.

PIC will be integrated with the following enterprise/workgroup consoles:

- HP OpenView Network Node Manager v6.2
- CA UniCenter TNG v3.0

4.2 Internationalization

The PIC application has been designed to support easy localization of the resources.

The default resource files are localized in US English and have the file extension “ENU”. PIC is localized into Simplified Chinese with the file extension “CHS”, Spanish with “ESP”, German with “DEU”, and Korean with “KOR”.

4.3 Security

The managed server may be running a DMI 2.0s (or secure) version of the DMI service provider, but PIC does not use or support the DMI 2.0s security enhancements.

When PIC is launched, a dialog will appear during initialization requesting a password for the server being managed. In order to pass the security check, the password entered must be the same as the password stored in firmware on the managed platform. The password is case sensitive. While the password dialog is present, PIC will continue to initialize but will not be usable until the correct password has been entered.

If the user enters in an incorrect password, a new password dialog will appear requesting a password. The user will be allowed three attempts to enter in a correct password. After the third attempt, if the password is incorrect, the PIC application will close and PIC must be relaunched to restart the User Authentication process.

PIC does not support a read-only user. If a correct password has been entered, the user will be allowed to manage the server using PIC. Additional security checks will be executed if the user selects one of the following menu items from the Configure dropdown menu.

- Enable Front Panel Power and Reset
- Power off the server immediately
- Power on the server immediately
- Restore Factory Defaults

These checks will be invisible to the user and will be performed using the stored password that was entered during PIC initialization. If the security check fails, the requested action will not be performed and the user will be notified of the failure.

4.4 Installation

The individual who installs PIC must have Administrator rights on the local and remote servers.

The PIC installation copies the necessary files onto the console machine. Then it registers the ActiveX controls and finally, it makes the registry changes needed for console customization.

4.4.1 Registry Keys

The registry keys described below are defined under the PIC root key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ Intel\Server Control\MI\PIC
```

4.4.2 Class Names

PIC retrieves the DMI class names it uses from the following registry values.

Table 1. DMI Class Registry Keys

Subkey Name: \Paths

Values Type: REGSZ

Registry Subkey Name	DMI Class (as shipped)	Comments
IntelHealthComponent	Intel Corporation, Server Health	SHA component name
ICMBControl	Intel ICMB Control 001	Reclaim Inactive Resources menu option
ServerHealthDetail	Intel Server Health Detail 001	Health event detail
StatusDisplay	Intel Status Display basebrd001; Intel Status Display 002	Semicolon-delimited list of class name(s) for LCD display. PIC queries these in order specified, uses the first which is present.
SystemControl	Intel System Control basebrd001	Used by menu options: Immediate Power Off Server Immediate Hardware Reset Server Enable Watchdog Timer Restore Factory Defaults
SystemHardwareSecurity	DMTF System Hardware Security 001	Enable Front Panel Power & Reset menu option
PagingConfig	Intel Paging Config 001	Paging Configuration dialog
LocalPagingConfig	Intel Local Paging Config 001	Paging Configuration dialog
DisplayCustomization	Intel Display Customization 001	Optional name of server-specific bitmap
Container	DMTF Container 001	Identifies server model for bitmap and tree template selection
SMaRTToolExe		Path of SMaRT Tool application.
EmailAlertConfig	Intel Email Config 001	Email Alert Configuration dialog
Local Email Alert Config	Intel Local Email Config 001	Email Alert Configuration dialog

Registry Value Name	Type	Value	Use
DefaultTree	STRING	Default	Name of default tree

4.4.3 Tree Templates

The structure and content of the instrumentation tree view which PIC displays is defined entirely in the Windows registry. PIC supports multiple, server-specific trees. It attempts to use a tree associated with the server model, if one is defined. If not, PIC uses a default tree.

Tree templates are defined under the registry subkey:

```
\Trees\

```

<tree name> is an arbitrary string that identifies the tree. If <tree name> matches the server model, PIC uses that tree for the server; otherwise PIC uses the tree named by the DefaultTree registry value. See the Container key in the above table for more information on how PIC derives the tree name from the server model.

Each node in a registry tree template has the following form:

```
<item name>
\Attrs = <item attributes>

<item name>\*Groups
<DMI Classn> = <ProgIDn>

<item name>\*Components
\ResID= <component resource ID>
\ProgID= <ProgID>

<item name>\<subitem name>
...
```

4.4.3.1 Subkeys

```
\*Groups
```

Defines the DMI groups that the item contains, if any.

```
\*Components
```

Defines the DMI groups that the item contains, if any.

```
\<subitem name>
```

Specifies a tree item that is contained by the current item. The subitem template is of the same form as the item template. Items can be nested to any depth.

4.4.3.2 Value Entries

<item name>

Specifies the text label displayed for the tree item.

<item attributes>

This double-word value specifies a set of bit flags that determine how PIC displays and processes the item.

<DMI Class>

Specifies the name of the DMI class PIC enumerates to create the contents of a folder item. Any number of class names may be associated with a folder, though typically only one is associated.

<ProgID>

Specifies the programmatic identifier of an ActiveX control. If AttrNeverExpand is specified, PIC displays the control when the user clicks on the folder; otherwise PIC displays the control when the user clicks on any of the DMI rows contained by the folder.

Table 2. Navigation Tree Item Attributes

Attribute Name	Hex value	Meaning
AttrHealthContributor	00000001	PIC periodically polls the health of all DMI table rows contained by the item. PIC only polls servers which do not support Server Health Alerts (SHA).
AttrThread	00000002	PIC creates a unique initialization thread to load this item's subtree. The thread terminates as soon as the subtree is loaded. This feature can improve application initialization time. If this attribute is not specified, PIC loads the subtree in the primary background thread, before processing the next item.
AttrAlways	00000004	PIC displays the item even if it is empty (has no children).
AttrHealthRoot	00000008	This item is the root of the health branch. There may only be one of these; PIC ignores any duplicate health branch definitions.
AttrNeverExpand	00000010	PIC should not query the server for this item. Typically, the associated ActiveX control will do so.
AttrExpandOnDemand	00000020	PIC will not query the server for this item during initialization, but will wait until the user expands the item in the tree view.

4.5 GUI Container

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. See the following figure for an example.

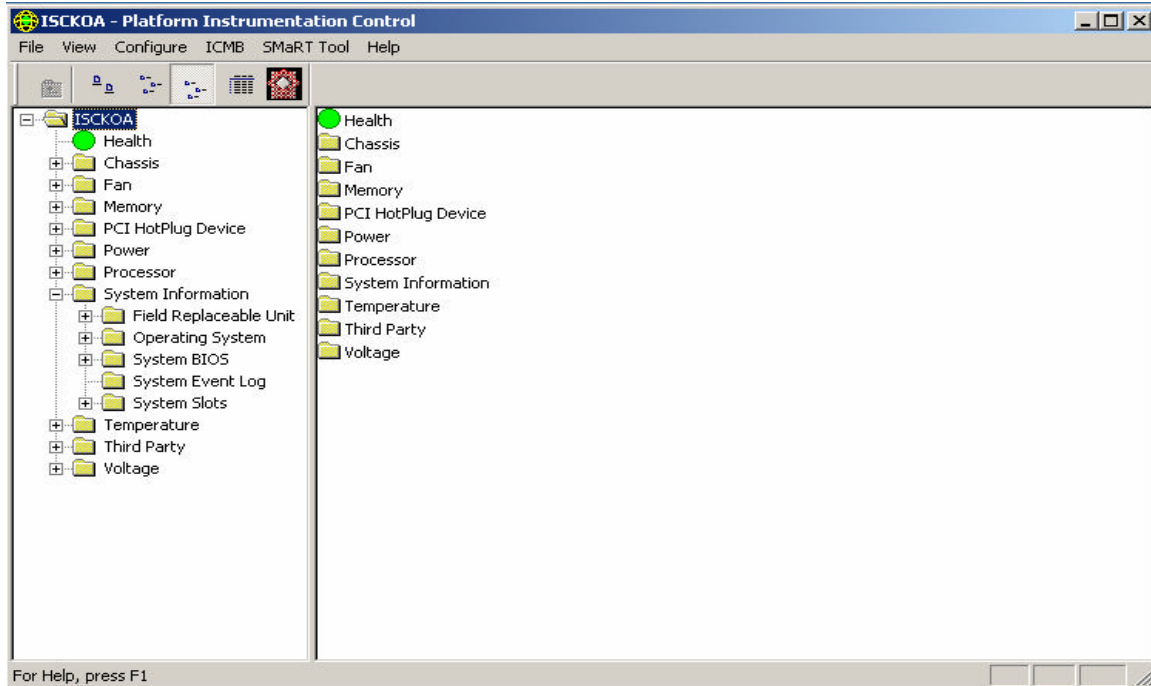


Figure 1. PIC Container

During initialization, PIC takes the following actions:

1. Authenticates the user on the managed server.
2. Communicates with the managed server to determine which sensors are supported on the server.
3. Builds the navigation tree in the main window.
4. Determines the server health status and initializes the Health branch in the navigation tree. Since all unhealthy sensors (current status is not “OK”) are collected under the Health branch, this branch provides the user with a simple view of the current server health.

A blue progress bar at the bottom of the PIC window provides initialization progress. Initialization is complete when the status bar changes to “Ready”.

When the user navigates to a sensor in the tree view, a set of tabbed pages will appear in the presentation pane displaying information specific for that sensor. Using the navigation pane to select a sensor and viewing/updating the sensor in the presentation pane is the general usage scenario of the PIC interface.

4.6 Navigation Pane

The navigation pane appears on the left side of the main dialog and is used to organize the server information.

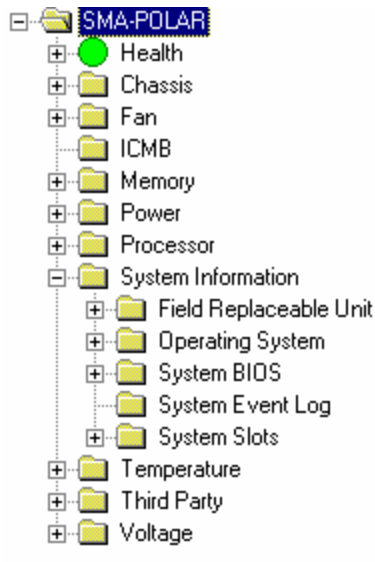




Figure 2. Navigation Pane

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.

4.6.1 Health

Health is 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 (current 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 displayed both under the Health branch and under 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 overall server health icon will display the state of the most severe sensor status. If any sensor is in a critical condition (regardless of other sensors being in a non-critical condition), the server health status will be shown as critical (red). If there are only non-critical sensors, the server health status will be shown as non-critical (yellow). If all sensors report normal conditions, the server health status will be shown as OK (green).

4.7 Group Information

When browsing the tree in the navigation pane, “Group” information displayed in the presentation pane will appear in Large Icon, Small Icon, List or Detail view based on the View option selected in the Main Menu / View pull down menu. The user can arrange these view options by name or by status.

- “Arrange by Name” sorts the list view items alphabetically
- “Arrange by Status” sort items by their current status

The possible values of current status are “Critical”, “Non-Critical”, and “OK”.

4.8 Presentation Pane

The presentation pane appears on the right side of the main dialog and is used to display the server and sensor information selected in the navigation pane.

For sensor objects selected in the navigation pane (such as Temperature, Fan, and Voltage sensors), up to four tab pages are displayed in the presentation pane:

Table 3. Presentation Pane

Sensor Settings or Sensor Status	<p>Displays health status, current readings, error counts and threshold values (if supported).</p> <p>When a user changes a threshold value, s/he can switch between the tab pages of the sensor without pressing the Apply button to save the changes. If the user selects another sensor before pressing the Apply button, s/he will be prompted to save the changes before PIC will display the new sensor information.</p>
Alert Actions	<p>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 AMS events actions are also displayed.</p>
Sensor Information	<p>Displays static sensor information such as normal readings, tolerances, ranges, etc.</p> <p>Note: Not all types of sensors support the Sensor Information tab page.</p>
Inventory Information	<p>Displays Field Replaceable Unit information such as manufacturer, model, serial number, etc.</p> <p>Note: not all types of sensors support the Inventory Information tab page.</p>

For server components selected in the navigation pane (such as Operating System, System BIOS, and System Event Log), one tab page is displayed. The name of the tab page matches the component name in the navigation tree and the data displayed is specific to the server component selected.

4.8.1 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.

This tab page is displayed for the following sensor types:

- Fan
- Temperature
- Voltage

Depending on the individual sensor displayed, some thresholds maybe unsupported and therefore appear as disabled (grayed out) in the control.

The status bitmap at 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”
- A blue question mark means “Unknown”

The Apply button is enabled when a threshold value is changed. PIC validates user entries for threshold values when the Apply button is pressed. Threshold values must conform to the following rule:

MIN <= Lower Critical <= Lower Non Critical < Upper Non Critical <= Upper Critical <= MAX.

For each sensor, there is a minimum (MIN) and a maximum (MAX) threshold value. 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).

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

4.8.1.1 Threshold Value Rounding

When setting thresholds, the values entered may not be the exact values set by the software, due to hardware rounding. To view the value set by the software, it is necessary to redisplay the page.

4.8.1.2 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 a threshold value or alert action is changed in PIC, it is possible to create an environment in which an event is immediately generated, such as if the Upper Non-critical Threshold value is set 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. Changes are valid immediately in the active instrumentation, but PIC waits five minutes before writing user changes to the hard drive.
2. If the change causes the server to reboot, the previous value is restored from disk when the server reboots. PIC uses and displays the previous value, avoiding the 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.

4.8.1.3 Recovering from a Reboot-Fail Retry Loop

In addition to the built-in protection designed to prevent a Reboot-Fail Retry Loop, the Platform Instrumentation includes a method to recover from such a situation. When the Platform Instrumentation services start on the server, the PI looks for the presence of a file with the filename of LRA.NOT in the floppy drive (A:). The LRA.NOT file can be created as a simple text file and can be a zero-byte file; the PI is looking only at the file name, not the contents of the file.

If LRA.NOT is present in the server floppy drive, then the PI will not take any automated actions, including power control, for that server boot only. This allows a user to change the action or threshold that is causing the reboot action.

Note: The Platform Instrumentation performs a check for LRA.NOT at every system boot. On some operating systems, such as Red Hat Linux, this can generate a floppy drive error if no floppy disk is in the drive when the PI attempts to mount the floppy.

4.8.2 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

4.8.3 Inventory Information Tab Page

The Inventory Information tab page displays Field Replaceable Unit information such as manufacturer, model, serial number, etc. for the sensor. The values displayed in the Inventory Information tab page are read-only; information cannot be modified through PIC. The Inventory Information tab page is displayed for the following sensor types:

- Chassis
- Field Replaceable Unit
- Memory Array
- Processor

4.9 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 have only critical error counts, not non-critical
- Some sensors support only one threshold value
- Some sensors support only 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, and Redundant. Example uses: for rotation-sensing fan, chassis door, and power unit.

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

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

4.10 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 and Inventory Information.

On the Sensor Status tab page, the current status can be one of the following values:

- Ok
- Critical
- Unknown

On the Alert Action tab page, event actions can be configured 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.

Note: Some servers do not support chassis sensors.

4.11 Fan

Note: The FRUSDR utility must be run on the server after system integration before PIC will properly display the fan sensors.

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 and Sensor Information.

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 0 and is read-only.

On the Alert Action tab page, event actions can be configured 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. This is RPM, CFM or OK/Fatal. Ok/Fatal is supported only 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.

4.12 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 and Inventory Information.

On the Sensor Status tab page, the current status can be one of the following values:

- Ok
- Non-Critical
- Critical
- Unknown

On the Alert Action tab page, it is possible to 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: The purpose of this memory array.

- **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:** The 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.

Note: Some servers do not support memory array sensors.

4.13 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, and Sensor Information.

On the Sensor Status tab page, the current status can be one of 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 indicate that the device is being used solely 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: The system state during which the last error status was collected.

Note: Some servers do not support memory device sensors.

4.14 PCI HotPlug Device

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

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 occupying the PHP slot.
- Device Type: Displays what type of device is occupying the PHP slot.
- Device Revision: Revision ID of the device that is occupying the PHP slot.

Note: When a PCI device does not exist in the slot, the corresponding device entry is still shown in the tree under the PCI HotPlug Device group in the navigation pane. The corresponding Sensor Information tab page displays the information for Manufacturer, Device Type, and Device Revision as “unknown”.

4.15 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, and Sensor Information.

On the Sensor Status tab page, the current status can be one of 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, such as Linear, Switching, Battery, etc.
- Total Output Power: The total output power of this power supply.

Note: Some servers do not support power supply sensors.

4.16 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, and Alert Actions.

On the Sensor Status tab page, the 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

Note: Some servers do not support Power Unit sensors. The Server Board SE7210TP1-E does not support redundant power supplies.

4.17 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, and Inventory Information.

On the Sensor Status tab page, the current status can be one of 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 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.

Note: Some servers do not support processor sensors.

4.18 System Information

A logical grouping of system related components.

4.18.1 Field Replaceable Unit

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

Note: The information displayed in the FRU is of the System Information group can be programmed using the FRUSDR utility during the initial setup of the system.

4.18.2 Operating System

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

4.18.3 System BIOS

The System BIOS control displays a list of BIOS attributes for the system BIOS installed on the managed system. The System BIOS tab page displays the following information:

- BIOS Manufacturer: The name of the company that wrote the system BIOS.
- BIOS Version: The version number or version string of the BIOS.
- BIOS ROM Size: The physical size of this BIOS ROM device in kilobytes.
- BIOS Starting Address: The starting physical address for the memory that the BIOS occupies.
- BIOS Ending Address: The ending physical address for the memory that 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.

4.18.4 System Event Log

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

4.19 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 64bit” identify PCI Hot Plug or PHP slots. For PHP type slots, three tab pages are 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.

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 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)

4.20 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 and Sensor Information.

On the Sensor Settings tab page, the current status can be one of 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.

Temperature information can be displayed in either Celsius or Fahrenheit. The display format can be changed on the Options dialog by selecting the Main Menu / View / Options pull down 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 is in 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.

4.21 Third Party Instrumentation

The Third Party control displays event configuration information for supported third party instrumentation on the managed server. For third party instrumentation, there is one tab page available in the presentation pane: Alert Actions.

The following third-party instrumentation is supported by PIC:

- Adaptec* SCSI
- Adaptec* CI/O Standard Group MIF
- Symbios* 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, the user 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, the user 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, the user 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

Note: Some servers do not support all third party instrumentation.

4.22 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 and Sensor Information.

On the Sensor Settings tab page, the current status can be one of 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 in 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.

4.23 PIC Dialogs

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

4.24 Options Dialog

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

PIC has several configurable options. The user can set the PIC console refresh rate to specify 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 can specify whether temperatures values display in degrees Celsius or degrees Fahrenheit.

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 SDR file

When configuring the console refresh interval, selecting a frequent refresh interval impacts system performance on both the console and the managed server 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 how quickly 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.

4.25 Restoring Factory Defaults

To restore default PIC settings for threshold values, console refresh interval, and the watchdog feature:

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

Note: Event actions the user has configured and the temperature display format are not affected by the Restore Factory Default option.

Default threshold values are stored in Sensor Data Records (SDR) in nonvolatile storage on the motherboard. These values are determined and configured during motherboard 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, under the following conditions:

- 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, the restoration of the default thresholds may trigger 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 that for each sensor where indications are not wanted, before the user selects the Restore Default Settings action, he/she must adjust the user-defined threshold value so that the current sensor value is not between the user-defined threshold value and the default threshold value.

4.26 Watchdog Timer Dialog

Each motherboard supported by PIC has a watchdog timer implemented in the hardware; the timer is disabled by default. When enabled, the timer continually decrements to test the response of the server operating system. Under normal operating conditions, the PIC server instrumentation software will periodically reset the timer; it will not reach a value of zero. Only if the operating system hangs will the timer count down to zero.

If the timer reaches a value of zero, indicating an operating system hang, 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 pull down menu selection.

4.27 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 actual paging function is implemented by the Baseboard Management Controller and uses a system modem on the managed server. Although PIC supports paging as an event action, PIC does not provide any user interface to configure the system modem. PIC does provide a dialog to configure the pager number, repeat counts, or 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 pull down menu selection. If paging is not supported on the managed server, this menu option will be grayed out.

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 should be dialed, including:
 - Modem dial commands
 - Paging service phone number (including initial numbers to get 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
-
- **Paging Properties:** The Repeat Paging feature allows administrators to be notified multiple times for any paging event. The user can configure how many times and how 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 one minute 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.

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

Note: The Test Page function is supported only for the default pager number. Paging is not supported on the Server Board SE7210TP1-E.

4.28 Email Alert Configuration Dialog

Sending an email is an alert action configurable for any sensor event if the email alert feature is supported on the managed server. The ISM Platform Instrumentation on the server implements the actual email sending function. The Email alert feature assumes that the server that is running the ISM Platform Instrumentation is connected across the network, and the SMTP service is running either on the local server or on another server in the network environment.

PIC provides a dialog to configure the Email IDs (source and destination) and SMTP Server relevant to the email event action. This email alert configuration is global to the server and is therefore not sensor specific.

The Email Alert Configuration dialog is available from the Main Menu / Configure / Email Alert Configuration pull down menu selection. If email option is not supported on the managed server, this menu option will be grayed out.

The Email Alert Configuration dialog allows the user to configure the following email information:

- **Email Settings:** The From Email ID is the Email ID of the sender. The To Email ID includes the list of destination email IDs for the alert (multiple email IDs separated by commas or semicolon. SMTP Server is the name of the mail server.
- **Test Email:** Allows the user to generate and validate a test email request based on the From and To email IDs.

Use the Test Email function to validate the information entered.

4.29 Test Email Dialog

Test Email allows the administrator to verify the system is properly configured to send emails using the To Address and From Address listed in the Email Configuration Data. After validation is confirmed, it can also be used to send emails from the managed Intel server running email-enabled ISM software.

- **Email Subject:** The Email Subject field is usable only when sending a Test Email. Typically, this field contains a summary or keyword indicating the topic of the message. It is not user definable when the system sends an alert email; in that case, the system automatically fills this field in with alert-related information.
- **Email Message:** The Email Message field is usable only when sending a Test Email. This field contains the body of the message to be sent. It is not user definable when the system sends an alert email; in that case, the system automatically fills this field in with alert-related information.

4.30 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 as an ICMB primary server and report management information on other ICMB devices connected to it. Using ICMB, PIC can manage the power state of remote ICMB devices

and view the SEL and FRU information about those devices. The amount of FRU information available depends on the type of ICMB device being managed.

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.

Through the PIC software, user can configure the ICMB management features of the primary managed server and the remote ICMB managed devices. The ICMB dialog allows the user to 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. 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.

4.31 ICMB Remote Server(s) Dialog

Once the primary server has been configured to be a 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) pull down menu selection. If ICMB is not enabled on the managed server, this menu option will be grayed out.

This dialog will display a list of all the servers being managed via ICMB. Users 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 new servers 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 information
- System event log

Note: ICMB is not supported on the Server Board SE7210TP1-E.

4.32 Intel® SMaRT Tool Interface

4.32.1 Launching Intel® SMaRT Tool above the FRU Level

When the user has not yet drilled down to the specific FRU that causes an alert (for example: the user has highlighted the server name or Health branch in the navigation pane clicking the “Launch SMaRT Tool” Menu option or “SMaRT Tool” toolbar button causes the SMaRT Tool to open on the particular server systems home page.

4.32.2 Launching SMaRT Tool at the FRU Level

When the user has drilled down to the FRU level (for example: the user has highlighted a critical sensor or normal sensor, clicking the “Launch SMaRT Tool” Menu option or “SMaRT Tool” toolbar button causes the SMaRT Tool to open on that particular FRU’s listing in the FRU database.

By clicking on the associated options in the SMaRT Tool screen, the user can give a graphical step-by-step replacement procedure for the selected FRU.

4.32.3 Parameters Passed to SMaRT Tool

When ISM PIC calls the SMaRT Tool executable, ISM PIC will provide some or all of the following command line parameters.

Table 4. Parameters Passed to SMaRT Tool

SNo	Parameter	Description
1	language	The console operating system language in which ISM is running is passed to the SMaRT Tool to ensure the SMaRT Tool is opened in the same language if available. (Mandatory field)
2	board	The managed server baseboard identifier. (Mandatory field)
3	chassis	The managed server chassis identifier. (Mandatory field)
4	fru	FRU data item associated with the selected sensor. (Optional field)

5. Platform Instrumentation

Platform Instrumentation provides an administrator with the ability to use standards-based management tools to gather information from a server and to perform various control functions on the server.

These control functions provide a user with administrative rights with the ability to make significant changes to the server's status, such as causing it to power down or reset. The fact that this functionality is available via a standards-based interface means it is easy for many tools to perform these actions.

The ISM 5.x PI provides support for IPMI 1.5 platforms and is backward compatible with IPMI 1.5, IPMI 1.0, and IPMI 0.9 platforms.

5.1 Functional Specifications for Intel® Server System SHG2

Only the functionality that is specific to the Intel® Server System SHG2 is described in this section. Appendix 1 shows the list of all sensors supported by ISM 5.x for SHG2 platform.

5.1.1 Baseboard Fan Management

The Server Board SHG2 supports a maximum of eight fans. There are two fans per processor and four fans dedicated for the chassis. The BMC has six fan speed (boost) sensors:

- Fan Boost Base Board Temperature
- Fan Boost HSPB 1 Temperature
- Fan Boost HSPB 2 Temperature
- Fan Boost Front Panel Temperature
- Fan Boost Proc 1 Temperature
- Fan Boost CPU 2 Temperature

5.1.2 System Event Log

SEL entries are kept in a 64K parameter block of the flash device, allowing for approximately 3,276 entries.

5.2 Functional Specification for the Intel® Server Chassis SC5200

The BMC supports the Intel® Server Chassis SC5200 by monitoring the power subsystem, in addition to providing FRU access to the power distribution board, each of the three power supplies, and the hot swap controller.

5.2.1 Sensor Monitoring

The BMC monitors the following sensors in the Server Chassis SC5200. The sensors that are specific to the Server Chassis SC5200 are listed in the sensor table.

- Tachometer fan counts for each power supply.
- Power supply presence for each power supply.
- Access to the FRU Inventory for each power supply.
- Access to the FRU Inventory for the Power Distribution Board.
- Hot-swap Back-plane temperature sensor.
- External tachometer fan connector counts.

5.2.2 Ambient Temperature Based Fan Speed Control

When used in the Server Chassis SC5200, the BMC implements an ambient temperature-based sensor that is used to control the nominal fan speed. The ambient temperature sensor allows the BMC to control the fan speed in order to lower the acoustic noise level of the Server Chassis SC5200 system.

The thresholds used by the ambient temperature sensor do not correspond to the non-critical thresholds used by the baseboard, processor, PDB temperature sensors, or the associated boost sensors.

Note: The SC5200 chassis monitoring features described in paragraph 5.2 are not supported by the Server Board SE7210TP1-E.

5.3 Functional Specifications for Intel® Server System SSH4

Only the functionality that is specific to Intel® Server System SSH4 is described in this section. Appendix 2 shows the list of all sensors supported by ISM 5.x for the SSH4 platform.

5.3.1 Baseboard Fan Management

The Server System SSH4 supports a maximum of six fans.

5.3.2 System Event Log

SEL entries are kept in a 64K parameter block of the flash device, allowing for approximately 3,276 entries.

5.3.3 Alerting – PEF and Alert Policies

SSH4 platform supports a maximum of 20 PEF Event Filter Table entries.

5.4 Functional Specifications for Intel® Server Systems SE7500WV2 and SE7501WV2

Only the functionality that is specific to the Intel® Server System SE7500WV2 is described in this section. Appendix 3 and 4 respectively show the list of all sensors supported by ISM 5.x for SE7500WV2 and SE7501WV2 platforms.

5.4.1 Baseboard Fan Management

The Server Board SE7500WV2 supports a maximum of six fans. There are four fans for the Intel® Server Chassis SR2300 (two for the chassis and two for processors) and two fans are reserved. Five fans dedicated for the Intel® Server Chassis SR1300; one fan is reserved for the Server Chassis SR1300.

The BMC has six fan speed (boost) sensors:

- Fan Boost Base Board Temperature
- Fan Boost ATA Temperature
- Fan Boost Front Panel Temperature
- Fan Boost PDB Temperature
- Fan Boost Proc 1 Temperature
- Fan Boost CPU 2 Temperature

5.4.2 System Event Log

SEL entries are kept in a 64K parameter block of the flash device, allowing for approximately 3,276 entries. The approximate completion time to clear a full SEL is 1 second.

5.5 Functional Specification for the Intel® Server Chassis SR1300

The Intel® Server Chassis SR1300 is a high-availability server chassis available in 1U rack mount configuration. Monitoring of the power subsystem in addition to providing FRU access to one power supply, and the hot swap controller are available in this chassis.

5.5.1 Sensor Monitoring

ISM 5.x PI monitors the following sensors specific to the Server Boards SE7500WV2 / SE7501WV2 with the Server Chassis SR1300:

- Front panel ambient temperature
- Power unit status
- Hot-swap backplane temperature

5.5.2 Ambient Temperature Based Fan Speed Control

ISM 5.1 PI monitors the ambient temperature-based sensor that is used to control the nominal fan speed. The ambient temperature sensor allows the BMC to control the fan speed in order to lower the acoustic noise level of the Server Board / Chassis SE7500WV2 / SE7501WV2 / SR1300 system.

5.6 Functional Specification for the Intel® Server Chassis SR2300

The Intel® Server Chassis SR2300 is a high-availability server chassis available in a 2U rack mount configuration. The server provides power supply monitoring, and provides FRU access to the power distribution board, both power supplies, and the hot swap controller.

5.6.1 Sensor Monitoring

The BMC provides monitoring of the following sensors implemented in the Server Chassis SR2300. The sensors that are specific to the Server Chassis SR2300 are listed the sensor table.

- Tachometer fan counts for the power supply
- Power supply presence for the power supply
- Front panel ambient temperature sensor
- Hot-swap Back-plane temperature sensor

5.6.2 Ambient Temperature Based Fan Speed Control

When used in the Server Chassis SR2300, the BMC implements an ambient temperature-based sensor that is used to control the nominal fan speed. The ambient temperature sensor allows the BMC to control the fan speed in order to lower the acoustic noise level of the SE7500WV2 / SE7501WV2/SR2300 system.

5.7 Functional Specifications for Intel® Server Board SE7501BR2

Only the functionality that is specific to the Intel® Server Board SE7501BR2 is described in this section. Appendix 5 shows the list of all sensors supported by ISM 5.x for the Server Board SE7501BR2 platform.

5.7.1 Baseboard Fan Management

The Server Board SE7501BR2 supports a maximum of eight fans.

5.7.2 System Event Log

SEL entries are kept in a 64K parameter block of the flash device, allowing for approximately 3,276 entries.

5.8 Functional Specification for the Intel® Server Chassis SC5250-E

The BMC supports the Intel® Server Chassis SC5250-E by providing monitoring of the power subsystem, in addition to providing FRU access to one power supply, and the hot swap controller. The Server Board SE7501BR2 is supported in the Server Chassis SC5250-E.

5.8.1 Sensor Monitoring

The BMC provides monitoring of the following sensors implemented in the Server Chassis SC5250-E.

- Hot-swap Back-plane temperature
- Tachometer fan counts for the power supply

5.9 Functional Specification for the Intel® Server Chassis SR1350-E

The BMC supports the Intel® Server Chassis SC1350-E by providing monitoring of the power subsystem, in addition to providing FRU access to one power supply, and the hot swap controller.

5.10 Functional Specifications for Intel® Server Board SE7501HG2

Only the functionality that is specific to the Intel® Server Board SE7501HG2 is described in this section. Appendix 6 shows the list of all sensors supported by ISM 5.x for the Server Board SE7501HG2.

5.10.1 Baseboard Fan Management

The Server Board SE7501HG2 supports a maximum of eight fans.

5.10.2 System Event Log

SEL entries are kept in a 64KB parameter block of the flash device, allowing for approximately 3,276 entries.

5.11 Functional Specifications for Intel® Server Board SE7210TP1-E

Only the functionality that is specific to the Intel® Server Board SE7210TP1-E is described in this section. Appendix 7 shows the list of all sensors supported by ISM 5.x for the Server Board SE7210TP1-E.

5.11.1 Baseboard Fan Management

The Server Board SE7210TP1-E supports a maximum of seven fans.

5.11.2 System Event Log

SEL entries are kept in block of the flash device, allowing for approximately 92 entries.

5.12 Functional Specification for the Intel® Entry Server Platform SR1325TP1-E

The Intel® Entry Server Platform SR1325TP1-E comes complete with the Intel® Server Board SE7210TP1-E board installed.

6. Direct Platform Control

The Direct Platform Control server management application supports remote system management via LAN, or a RS232 serial connection to the server's serial 2 port over a modem or a direct serial cable. The DPC Console provides remote management of Intel servers via modem or across a LAN with a capability to run DOS-based programs and platform confidence tests (system dependent).

The DPC Console application provides state-independent access to a server. DPC can connect to a server independent of its power state or operating system status. This connection can be made via a LAN, modem, or direct RS 232 serial line connection. DPC Console provides a user-friendly interface for monitoring and controlling the platform management features of the system. DPC Console consists of a Windows32* graphical user interface (GUI) that communicates directly to the Emergency Management Port (serial) or DPC (LAN) ports resident on the server.

DPC shares the on-board network adapter and the Emergency Management Port (EMP) hardware with the server operating system. Since the DPC Console 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 EMP/DPC is available on 5V standby power, DPC Console can be used to communicate with and control a powered down server.

The DPC Console is integrated into Intel® Server Management, Intel's standalone utility. It provides the following features:

- Establish connection to remote servers
- Server Control: Power On, Power Off and, Reset operations of server
- SEL Manager: Retrieve and display System Event Log (SEL) entries
- SDR Manager: Retrieve and display Sensor Data Records (SDR)
- FRU Manager: Retrieve and display Field Replaceable Unit (FRU) information
- RSA Manager: Retrieve and display current Remote Sensor Access information
- Phonebook for remote connection management
- Modes of operation: EMP, DPC over LAN, Redirect, and the Service Partition. See Section 6.4 for details regarding the DPC Console access modes.
- Remote control of Service Partition
- File transfer from / to server

Note: Some features are not available on some platforms. that the Server Board SE7210TP1-E does not support serial communications. The Service Partition, RSA, and EMP is not supported on the Server Board SE7210TP1-E.

6.1 Supported Communication Components

The DPC console supports communication over:

- LAN
- Microsoft* Windows* compatible modem

- RJ45 adapter Cat5 cable, RS232 serial cable

6.2 Client Configuration

The client system is the computer where the DPC console software is installed. The software is used to connect to one of the supported Intel® server systems.

6.2.1 Serial Communication

The DPC Console supports all COM ports on the client system for direct serial connections, along with any Microsoft Windows compatible modem for modem connections. The DPC Console will use the Windows API to determine if a modem is connected and available. The DPC Console will not do modem configuration, but will depend on Windows to have pre-configured the modem.

6.2.2 LAN Communication

DPC supports LAN connections; no client configuration is required for this feature.

6.3 Server Configuration

6.3.1 Serial Communicaton

DPC uses the Emergency Management Port to communicate with the server over a serial connection via the serial 2 port on the server. The EMP must be configured on the server to allow the DPC Console to connect to the server in serial mode. See the *ISM Install and User Guide* for BIOS / SSU settings required for enabling DPC Console connections over EMP.

6.3.2 LAN Mode

In LAN mode, the client communicates with the server via the on-board LAN port. As with a serial connection, the server must be configured to allow the DPC Console to communicate with the server via a LAN connection. See the *ISM Install and User Guide* for BIOS / SSU settings required for enabling DPC Console connections over the LAN.

6.3.3 Configuring Console Redirection

To use the DPC Console with a serial connection, use the Console Redirection Submenu to configure the serial communications as follows:

Table 5 Console Redirection Submenu Options

COM Port Address	Select 2F8. This is the COM2 port that the Emergency Management Port must use. The IRQ setting is automatically assigned with the correct number based on the COM port address choice.
Baud Rate	Refer to the managed server's Product Guide for the maximum baud rate supported for the server. If in doubt, about the correct setting, select 19.2k.
Flow Control	Choose CTS/RTS + CD.

6.3.4 Configuring Server Serial Communications

The DPC Console requires that the server's serial 2 port be connected to an external modem or directly connected to a serial (RS 232) cable. Some server systems may require a RJ45 adapter for connecting the Cat 5 wire (which connects to the server) to the modem cable (which connects to the external modem).

Note: Some servers have a Serial 2 port header on the board. This header is the system's EMP port. These servers require additional cabling to the header. Refer to the Technical Product Specification for that server for information about configuring serial ports and the cabling requirements for the server.

6.3.4.1 Configuring Direct Connections

A null modem serial (RS 232) cable is needed. Connect one end of the cable to the COM2 port of the server and the other to a port on the client workstation.

6.3.4.2 Configuring Modem Connections

For modem support, the server must use a Hayes*-compatible modem. The modem must be on the hardware compatibility list provided by Microsoft.

6.3.5 Configuring LAN Connections

Before connecting to the server via the LAN, the user needs to use the System Setup Utility to configure the server. Then when the server is connected to the LAN, the user will be able to connect to it with the DPC Console software. Refer to the *ISM Install and User Guide* for BIOS / SSU settings required to enable DPC Console connections over the LAN.

6.3.6 Creating a Service Partition

While not a requirement for Direct Platform Control, a Service Partition may be installed to add to the functionality of the DPC connection. If used, the Service Partition needs to be created on the server with the System Resource CD before installing the operating system.

The Service Partition allows the user to run DOS-based utilities and platform confidence tests (system dependent) that are resident on this area of the server hard drive, as well as perform file transfer services.

Refer to the managed server's product guide for information on creating and configuring a Service Partition.

Note: The sService Partition is not supported on the Server Board SE7210TP1-E.

6.4 Modes of Operation

The DPC Console displays the current mode in the status bar. The following is the list of modes. Mode descriptions are provided in the sections that follow.

- EMP mode
- DPC over LAN mode

- Redirect mode
- Service Partition mode - not available over Direct Connect

6.4.1 EMP Mode

The DPC Console always initiates a serial connection in this mode.

Note: EMP mode is not supported on the Server Board SE7210TP1-E.

6.4.2 DPC over LAN Mode

The DPC Console always initiates a LAN connection in this mode.

6.4.3 Redirect Mode

The DPC Console user can enter redirect mode by rebooting or powering up the server with console redirection enabled.

Redirect mode is active when the server is running BIOS console redirection. The DPC Console emulates an ANSI terminal and the redirected data is decoded and displayed in a separate window. Keystrokes are redirected to the BIOS running on the server, including Alt + any key except for system keys such as Alt + Tab.

The Console Redirection control enables the display of “redirected” data from server when the server switches over to BIOS console redirection. In this mode, the DPC Console launches a separate window, which emulates an ANSI terminal.

The redirect window display will be exactly the same as the server console display and will operate like a remote terminal. User keystrokes are translated and transmitted to remote server and the corresponding responses from the server are displayed.

Console redirection is active only when the server is operating in “real” mode. When the server is running in DOS or EFI, redirection is available because DOS and EFI are each considered real mode. When an operating system like Microsoft Windows is running on the server, console redirection is not available because the machine is in protected mode.

The operation of server switching between EMP and Redirect modes depends upon the connection type. With a LAN connection all EMP actions are available while in Redirect mode. With a serial connection switching between EMP and Redirect mode will depend on the setting of the EMP access mode in the BIOS/SSU setup of the server. This mode can be one of the following:

- Pre-boot only
- Always active
- Disabled

6.4.4 Service Partition Mode

The Service Partition mode is entered when user selects reboot from the Service Partition and a successful PPP (Serial) or TCP (LAN) connection is established. This mode allows the user to run DOS or EFI based utilities and platform confidence tests (if supported) that are resident on the Service Partition as well as the File Transfer services.

This mode is similar to Redirect mode, but uses the TCP/IP stack for the data transfer. The DPC Console supports two methods of executing DOS or EFI based utilities:

- The first method is selecting a utility from the program list.
- The second method is to use the DOS or EFI command shell to get the command prompt and execute the utilities.

For each method, the DPC Console opens a redirection window and starts a protocol-based console redirection process with the server.

Only one DOS or EFI based utility or command shell may be running at one time. Because DOS and EFI are single-threaded operating systems, DOS and EFI programs cannot be executed concurrently with the File Transfer Service.

Users are allowed to boot to the Service Partition only if a Service Partition exists on the server. The BIOS console redirection is enabled by the server to display the status of the BIOS boot on the DPC Console.

With a serial connection, after establishing a PPP connection, the DPC Console stops communicating to the firmware and the actions that are supported in EMP mode will be disabled. After switching to a PPP connection, the user needs to disconnect and re-connect for operation in EMP mode.

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

Note: The reboot from Service Partition is NOT supported on a direct line connection. Note also that Service Partition is not supported on the Server Board SE7210TP1-E.

6.5 Making a Connection

DPC Console can initiate a connection via LAN, RS 232 Serial line, or Modem. DPC Console initially expects the server to be in EMP mode.

After a successful connection, all EMP mode supported actions, such as Power on/off, Reset and SEL / SDR /FRU / RSA, are enabled, depending on the server configuration. Additionally, the Power off and Reset operations ensure a graceful shutdown in case any operating system is already running (PI must be running on the server). The Power Off and Reset operations may take more time depending on the number of applications running on the server.

In EMP mode, the user can request a reboot of the server to Service Partition at any time either selecting the option from menu or toolbar. The Service Partition must be installed on the server for this functionality to be available.

Note: A connection to via LAN must be secure before the power actions will be made available. If the connection is not a secure connection, the title bar will display “LAN – User” and the power actions will be disabled. In the case of multiple LAN connections, only the first LAN connection established is considered secure. Additional connections will be made with User level privileges. Power control actions and the SEL clear option will be disabled. A serial “user” connection can be established when a LAN connection is in session.

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 the user wishes to connect to.

```
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 DNS Name of the server.

For example:

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

```
DPCConsole /direct=1
```

```
DPCConsole /lan=255.255.255.0
```

6.6 Security

When connecting to the server, the DPC Console ensures security of the server via a password. The DPC Console prompts for a password before initiating a connection, regardless of whether a password was configured in BIOS/SSU. If a password was not configured in BIOS/SSU, the user does not enter one for the DPC Console. The password is not stored in the machine running the DPC Console, and therefore must be entered each time the user begins the connection process. The maximum size allowed for the password is 16 alphanumeric characters.

When connecting to the server, the user is prompted to enter this 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.

When connecting to the server over a serial connection, the password entered by the user is sent to the server in clear text.

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 the 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.

6.7 Server Power Control

The Server Power Control features provide 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 operates on standby power. The reset function can be used to generate a reset on the server with a post-reset option similar to the power up function. The power up, power down and reset functions are disabled, if the server is in “restricted” mode for EMP operations.

If the Intel Server Management Platform Instrumentation is installed on the managed server, then DPC console will communicate with the instrumentation when a reset or power down command is sent. In this case, DPC console commands the instrumentation to gracefully shut down the operating system before performing the power down function. If the operating system is unknown, or is not supported by ISM, then any power control command will be immediate.

6.8 User Interface

At start-up, the DPC Console displays the main menu, toolbar and a status bar. These can be used for start-up actions such as making connection or launching a plug-in, among others.

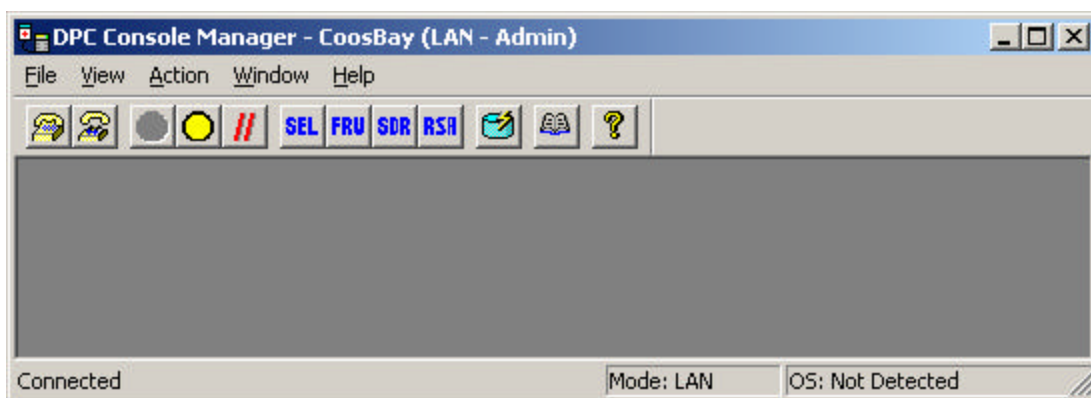


Figure 3. DPC Console Main Window

6.9 Title Bar

The title bar provides information about the server that DPC Console is connected to and the type of line that is used.

6.9.1 Server

When connected, the server name is shown after the application title, separated by a hyphen. This is updated for LAN or modem based connections only and remains blank for direct connections. The name displayed here is the same as the name selected from the phonebook on connection.

6.9.2 Line

When connected, the type of line used is shown in parentheses after the server name. The value displayed is the current type of connection LAN, direct, or dial-up followed by Admin or User. If an un-secure LAN connection is active the title bar displays “LAN – User”.

6.10 Status Bar

The status bar provides information about the mode of operation, the operating system running on the server, and the status of the line.

6.10.1 Mode

This displays the current mode of the connection. This is EMP, Redirect or PPP (Service Partition) for serial connections and LAN for a LAN connection.

6.10.2 OS (Operating System)

OS displays whether an operating system was detected on the server. It can be Unknown, the version number, or Not Detected.

Unknown is displayed when DPC Console is gathering information from the remote server, attempting to determine if the operating system is running or not on the remote server. If the server operating system is Unknown or Not Detected, then any power control actions will be immediate. See Section 6.7 for more information.

The version number is displayed when DPC Console has determined that the operating system is running on the remote server; Not Detected is displayed when DPC Console was unable to detect an operating system running on the remote server.

6.11 DPC Console Menu

The main menu is displayed when there is no active connection or when the console is connected in EMP mode and there is no active view. In addition, each Manager (FRU, SEL, SDR and RSA) adds a menu item when active to the Main menu between the Action and Window menu items. The main menu options are:

- File Menu
- View Menu
- Action Menu
- Window Menu
- Help Menu

6.11.1 File Menu

The File menu contains the following options:

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

6.11.1.1 Connection

The Connection menu item is a cascading menu that provides the options New... and Disconnect. These are used to connect and disconnect from a. A menu separator appears after this item.

New...

The New 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.

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.

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 the user is disconnected from the server.

Disconnect

The Disconnect 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 the Service Partition.

6.11.1.2 Open...

The Open menu item displays the standard Windows File Open Dialog.

6.11.1.3 Close

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

6.11.1.4 Save As...

The Save As... menu item saves information for the FRU, SEL and SDR Managers. If the FRU, SEL, RSA, or SDR Manager is not the active view this item is grayed.

The 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 and cannot be changed.

6.11.1.5 Print...

The Print menu item prints information for the FRU, SEL and SDR Managers. If the FRU, SEL, RSA, or SDR Manager is not the active view this item is grayed.

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.

6.11.1.6 Phonebook

The phonebook contains names of servers and their corresponding phone number and/or, IP Address or DNS name. The phonebook is shared by several applications and therefore has a common, shared user interface. The phonebook is used when connecting by LAN or by modem. The user selects a server name from the phonebook during the connect process.

6.11.1.7 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).

6.11.1.8 Exit

This option gracefully disconnects and cleans up and then terminates the execution of the DPC Console application. This option raises a confirmation dialog before closing the application.

6.11.2 View Menu

The View menu contains the following options:

- SEL Manager
- SDR Manager
- FRU Manager
- RSA Manager
- Toolbar
- Status bar

Each manager has a tool bar with the appropriate menu items represented.

6.11.2.1 SEL Manager

The SEL Manager plug-in provides access to the System Event Log on the server. Clicking the SEL manager menu item will launch the SEL Manager management plug-in and allows the user to view the SEL records.

6.11.2.2 SDR Manager

The SDR Manager plug-in provides access to the Sensor Data Records. Clicking the SDR manager menu item allows the user to view Sensor Data Records. The menu item will be enabled before connecting to the server. This allows the user to view the saved SDR files.

6.11.2.3 FRU Manager

The FRU Manager allows the user to display Field Replaceable Unit data. The information displayed includes chassis information, baseboard information, and product information. Clicking the FRU manager menu item allows the user to view this information from the server's baseboard FRU information area. The menu item will be enabled before connecting to the server. This allows the user to view the saved FRU files.

6.11.2.4 RSA Manager

This menu provides the user with Remote Sensor Access (RSA) data from the server's baseboard FRU and SDR information area.

The RSA Manager will access sensor reading data after connecting via LAN or EMP. All readings and display will be completely decoded based on the IPMI 1.0 and 1.5 specifications. 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 and will not update dynamically, there will, however, be an RSA/Reload menu item to update the values.

The RSA menu item is between the Action and Window menu items when the RSA Manager is the active view (the same as for SEL, FRU and SDR). The RSA menu consists of Reload and Options. Reload behaves similar to the FRU and SDR Reload menu item. The Options menu item displays the dialog shown below.

The options dialog allows the user to choose Celsius or Fahrenheit. Upon pressing OK in the RSA Manager Options Dialog the Manager updates values based on the selections made.

If the server is powered down most sensors cannot be read. If a sensor cannot be read, the Current Status will display "Unknown". The BMC stores an historical reading of some sensors to show the state of the system as it was when it was powered off. For example, the fan sensors may read "full speed" even though the system power is off.

Note: RSA Manager is not supported on the Server Board SE7210TP1-E.

6.11.2.5 Toolbar

Check this item to display the applications toolbar; uncheck this item to hide the toolbar. The state of the toolbar (shown or hidden) is saved with the application data in the user portion of the registry.

6.11.2.6 Status Bar

Check this item to display the applications status bar or uncheck this item to hide the status bar. The state of the status bar (shown or hidden) is saved with the application data in the user portion of the registry.

6.11.3 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.

- Power On
- Power Off
- Reset
- Reboot to Service Partition
- Configuration Status

6.11.3.1 Power On...

This menu item allows the user to power the server on with one of the following post power-on options.

Power On with a Serial Connection

This option allows the user to power the server on in either EMP Mode or BIOS Redirection Mode.

Power On with a LAN Connection

This option allows the user to indicate that when the server is next powered on, it should be in BIOS Re-direction Mode.

6.11.3.2 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.

6.11.3.3 Reset...

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

Reset with a Serial Connection

This option allows the user to power the server on in either EMP Mode or BIOS Redirection Mode.

Reset with a LAN Connection

This option allows the user to indicate that when the server is next powered on, it should be in BIOS Re-direction Mode.

6.11.3.4 Reboot to 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 operating system and a reboot will cause the operating system 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 or LAN 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', refer to Section 10.

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. If the 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 DPC Console establishes a PPP connection with the server and the status bar is updated accordingly. The menu options available are also updated based on the functionality available from the Service Partition.

When the user is finished using the Service Partition, s/he must select the Reset (only for LAN connection) menu item (or toolbar button) or Disconnect (LAN or Dial-up), to reboot the server out of the Service Partition. A confirmation dialog will be shown prior to resetting the server. If this is a LAN connection, the user will be given the option to reset the server with BIOS redirection enabled. If this is a serial connection the connection to the server is terminated upon confirmation.

While booted to the Service Partition, the Service Partition menu is displayed with the following items:

- Run DOS/EFI Shell
- Run Program
- Run Platform Confidence Tests (on supported servers)
- File Transfer
- Redirection View

Note: The Server Board SE7210TP1-E does not support a Service Partition. Consequently, the user cannot reboot to a Service Partition on these platforms.

6.11.3.4.1 *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 platform confidence tests (system dependent) or use the Action menu item.

6.11.3.4.2 *Run Program*

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

- **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, platform confidence tests or perform any file transfer operations. User can open the redirection window by selecting "Redirection View" under the Service Partition pull down menu.
- **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.

6.11.3.4.3 *Run Platform Confidence Tests (System Dependent)*

This menu item is selected to run the platform confidence tests 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 platform confidence test program, which launches the initial screen.

6.11.3.4.4 *File Transfer*

This is a cascading menu used to transfer files between the client and the server in binary mode. This menu allows the user to transfer files to / from the client in binary mode. When the user selects the Upload or Download options, s/he is presented with a screen to select information such as the path and file name on both the client and server or to browse the client and/or server for the file.

6.11.3.4.5 *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.

7. Client System Setup Utility

The Client SSU (CSSU) application provides a Windows based interface running on a client workstation to an SSU server running on a remote server system. The application allows the user to perform a variety of configuration and setup tasks that normally would only be available on the local server platform.

Note: The CSSU is not available for use when managing the Server Board SE7210TP1-E. To configure the Server Board SE7210TP1-E, the user must use the SSU locally from the server. To execute any server-resident utilities the user must execute them locally from the server.

7.1 Client Application Framework

The Client Application Framework is a 32-bit Windows application that provides the general environment for remote SSU operation. The CSSU integrates SSU-based features through a set of management plug-ins called managers. These managers allow the user to perform remote system management tasks from the client workstation.

Functionality provided by the manager may vary, depending on the server platform. The managers may include support for configuration of system resources, selection of boot options, specification of the password, and viewing of system information such as the system event log, the sensor data records, and the field replaceable unit information. Within this architecture the CSSU is implemented as a MDI container application and each manager is implemented as an ActiveX control.

7.1.1 Command Line Options

The CSSU supports the following command-line options:

Table 6. Command Line Options

Option	Meaning
/P phone_number	Specifies the telephone number to be used to establish a connection with the SSU server.
/I IP address	Specifies the IP address to be used to establish a connection with the SSU server.
/D DNS name	Specifies the DNS name to be used to establish a connection with the SSU server.

7.1.2 Launching the Client SSU

Only a single instance of the CSSU may be launched on the client platform. The instance may connect to a single SSU server. A single CSSU connected to multiple SSU servers or multiple CSSUs connected to multiple SSU servers is not supported.

If the Client SSU is launched with a telephone number or an IP address specified on the command line, it will attempt to establish a connection with a SSU server at the given phone number, IP address, or DNS name. This will include prompting for a password as required. While the connection is being established, the Client SSU will display connection information on

the status bar of the Main Window. If the connection cannot be established with the remote server, the Client SSU will stop attempting to make a connection, display an error message, and return to the 'Main Window' to wait for user input.

If the Client SSU is launched without a telephone number, IP address, or DNS name specified on the command line, it will display the Main Window and wait for user input.

7.2 CSSU Functional Specification

The following sections briefly describe the available functionality for the Client System Setup Utility. For detailed operation, see the Installation and User Guide that accompanies the ISM software CD.

The following figure shows the user interface to the CSSU.

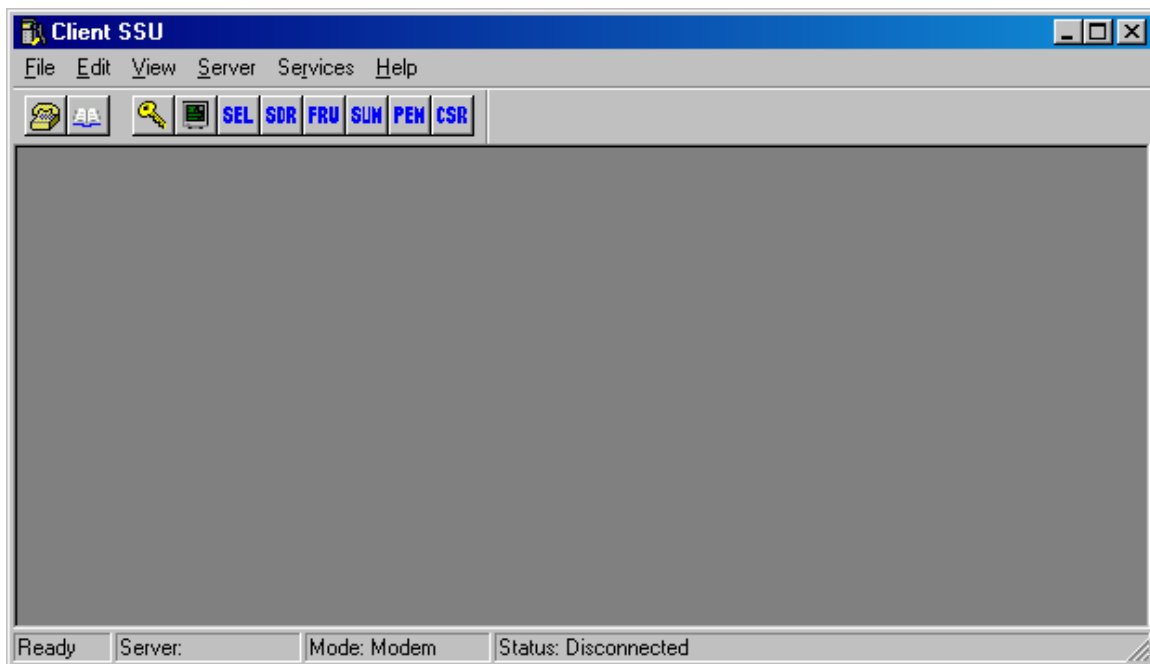


Figure 4. User Interface to CSSU












The Menu Bar is populated with manager options that can be accessed remotely by the CSSU. These include the Password Manager, Multiboot Manager, SEL Manager, SDR Manager, FRU Manager, SUM Manager, Platform Event Manager, and CSR Manager.

All manager options are displayed if the Client SSU is not connected to a SSU server. However, the Client SSU cannot identify the services supported by the SSU server until a connection is established. When the user selects an option from the menu, a connection dialog will be presented to the user to establish a connection with the server. After establishing the connection, if the specified SSU server supports the manager service, the manager service will be launched within the CSSU container. If the SSU server does not support the selected manager, an informational message will be displayed. The connection between the Client SSU and the SSU server will be maintained.

All manager options are displayed if the Client SSU is connected to the SSU server platform. Some options may be disabled if the connected SSU server does not support the manager feature.

The following is a list of Main Window toolbar buttons available from the Client SSU.

Figure 5. Main Window Toolbar Buttons

Bitmap	Description
	(Re)Connect: Launches the Connection dialog
	Disconnect: Disconnects from the connected server
	Phonebook: Launches the Phonebook dialog
	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 SUM Manager module
	PEM: Launches the PEM Manager module
	CSR: Launches the Configuration Save/Restore Manager module

7.2.1 Console Redirection Features

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 this reboot operation, the only information available to the user is the connection information on the status bar of the CSSU main window.

If a connection cannot be successfully established with the remote server, the Client SSU will display an error message and return to its main window waiting for 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 help users get more information during the server reboot, a console redirection window will appear within the CSSU main window to show the boot process on the server.

7.2.1.1 User Interface

When the Client SSU attempts a connection, either after being started from the command line or from the CSSU main window, it sends a command to the server that 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 mode output to the server's screen can be displayed in the Client SSU main window.

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

7.2.1.2 SSU Console Redirection Window

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

After the server is booted to the Service Partition and the Remote Service Agent (RSA) is started, a message is sent by the server to notify that it has switched to EMP mode. At this point, the console redirection window is closed.

7.3 CSSU Managers

The following sections describe the individual managers that are available for launching from within the CSSU application.

7.3.1 MBM Manager

The Multiboot Manager (MBM) provides an interface for selecting Initial Program Load (IPL) devices. Using the MBM, the user can identify all IPL devices in the system and prioritize their boot order. On power-up, the BIOS will sequentially attempt to boot from each device. Only a single instance of the MBM may be launched within the CSSU. Examples of the devices available for boot order selection include the floppy disk drive, system hard drive or PXE boot agent.

7.3.2 PWM Manager

The Password Manager provides security and password support options. Within the PWM, the user can either set or modify the current system passwords or update any of the various security options available. Only a single instance of the PWM may be launched within the CSSU. Examples of security options configured from the PWM include Administrator and User BIOS passwords, lock-out timer, video blanking, secure boot, floppy write protect and front panel lockout.

7.3.3 SEL Manager

The System Event Log Manager provides basic support for viewing and clearing the system event log on the server platform. A single instance of the SEL may be launched within the CSSU.

7.3.4 SDR Manager

The Sensor Data Record Manager provides basic support for viewing and clearing the system event log on the server platform. A single instance of the SEL may be launched within the CSSU.

7.3.5 FRU Manager

The Field Replaceable Unit Manager provides basic support for viewing the FRU Inventory areas on the server platform. A single instance of the FRU may be launched within the CSSU.

7.3.6 SUM Manager

The System Update Manager 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. A single instance of the SUM may be launched within the CSSU.

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.

The UIF is composed of four types of lines. The first is a platform line delimited by brackets. The second is the version number of the package being used, also in brackets. The rest are data lines in the format:

```
Hex<number of file>=<filename>
Update<number of file>=<Type of Update>.
```

The only type of update is OP, which represent the operational code. See Figure 6.

```
[L440GX+]
[05]
Hex0=LWBMC01.HEX
Update0=OP
Hex1=LWHSC12.HEX
Update1=OP
Hex2=LWFPC12.HEX
Update2=OP

Hex3=B-0015.BIO
Update3=BIO
```

Figure 6. Example .UIF File

It is possible to use each .HEX file individually by loading it through the File/Load dialog box. This is recommended only for experienced users who may want to perform updates in a different order than that specified in the .UIF file.

7.3.6.1 Recovery Agent

Working BMC firmware is necessary for correct operation of a server. With the capability of performing remote BMC firmware updates to a server comes the possibility that an error could occur during the update. To recover from BMC update errors, a recovery agent program exists on the Service Partition of the server.

When a remote BMC firmware update is being done, a checkpoint file is written on 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 since there are several points at which the recovery operation can begin. If an error occurs during the update, the recovery agent is invoked. The agent 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.

The recovery agent is an executable file named `recover.exe`, located in the Service Partition. If a remote BMC update is attempted and this file does not exist, an error will be reported to the SUM and the update will not take place.

7.3.6.2 BMC Firmware Update Process

The following steps are performed to do a remote update of BMC firmware on a server:

- The new firmware image file is transferred to the Service Partition on the server.
- Current firmware settings and SDRs are saved to files in the Service Partition.
- The firmware on the server is put in update mode so the firmware can be updated.
- The firmware is put in operational mode to run the new firmware.
- The saved firmware settings and SDRs are restored.
- The checkpoint file is removed.
- The server is reset to bring the firmware and BIOS into alignment.

Each of these steps is described in more detail below.

7.3.6.3 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 in the Service Partition to indicate the file is in the Service Partition.
- If the recovery agent software is running, it updates the number indicating how many recovery attempts have been made. This number is kept in a file in the Service Partition.

- The SUA calls the BIOS with a Set BIOS Flags command to set the flag to force a boot to the Service Partition. After this point, 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 cleared by the SUA or recovery agent.

7.3.6.4 Save Firmware Settings and Recovery Information

- The SUA/recovery agent saves current firmware settings that are necessary to restore after the update into a file in the Service Partition. Other data, such as SDRs, are also saved at this point.
- The operational mode watchdog timer in the BMC firmware is set running. The purpose of setting this timer is to ensure that if a system hang occurs before entering update mode, then when the timer expires, a reboot to the Service Partition will occur so that 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 gets a chance to run without a connection being established from a remote console. The EMP does not own the serial port. If a modem connection exists, it is between the CSSU and the SUA.
- The checkpoint file is written to indicate the update process got to the point of saving all configuration settings.

7.3.6.5 Put Firmware in Update Mode

- The SUA puts the firmware in 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 got to this point.
- The BMC firmware in the boot block enables the boot block watchdog timer before starting the update of the operational code. This timer watches firmware command activity (assumes that commands occur every so often 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 of setting or modifying the amount of time this timer runs before expiring.

7.3.6.6 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 got to 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.

7.3.6.7 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.
- The operational mode timer in the firmware is disabled.

7.3.6.8 Clear Checkpoint Information

- The SUA/recovery agent removes the checkpoint file and any 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.

7.3.6.9 Reset Server

After an update has occurred successfully, 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.

7.3.7 PEP Manager

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

7.3.8 CSR Manager

The Configuration Save/Restore Manager provides a way to save the non-volatile system settings on a server to a file, and allows those settings to be written back into non-volatile storage on a server. The CSR presents a main window to the user. This window contains buttons that 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.

A single instance of the CSR may be launched within the CSSU.

7.3.9 Save Configuration to File Button

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.

The BIOS version string and the firmware version information for the BIOS and firmware 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).

7.3.10 Restore Configuration from File Button

When the Restore Configuration From File button is clicked, the user is 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.

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 informed 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 installed BIOS or firmware versions do not match those in the backup file can cause the server to operate incorrectly.

7.3.11 Save 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 CMOS banks. During a restore operation, the first 16 bytes of bank 0 are not restored because these bytes contain information that cannot be altered.
- The entire 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 configuration data: One byte is used for settings such as whether an EMP password is set, whether EMP is set up for direct connect or modem access, and the EMP activation mode (e.g. always active). Other EMP configuration data includes three modem strings, 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.
- LAN configuration data: including, but not limited to, IP address configuration (Static or DHCP), subnet mask, access policy (always active, restricted, disable), alert destination and LAN alert policies.
- 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.

8. ISM Install / Uninstall

This section provides information on the Intel Server Management installation framework. It describes in details how to create configuration files and custom interfaces used to install an application. This section is intended as a reference for anyone who wishes to have applications installed by the ISM installation framework. It does not describe the internal implementation.

8.1 Extensibility, Customization

The Intel Server Management installation framework does not have specific knowledge of 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) must create configuration files describing the necessary steps to install that component on a system (files format is described later).

OEMs will be able to fully customize the ISM installation by modifying the configuration files provided and by inserting their own. The OEM can also customize the look and feel of the installation interface.

8.2 Remote Installation of Console/Server Components

The ISM installation framework can install Win32* components (consoles or server) on local or remote systems. In Win32 systems the Local Setup process will be started remotely from the installation console.

8.3 Supported Operating Systems

The installation console will support:

- Windows* XP Professional
- Windows 2000 Professional, Service Pack 3
- Windows 2000 Advanced Server, Service Pack 3
- Windows Server 2003, Enterprise Edition

Server systems can have:

- Windows 2000 Advanced Server, Service Pack 3
- Windows Server 2003, Enterprise Edition
- Novell* NetWare*² server 6.0 with Service Pack 1 or NetWare 5.1 with Service Pack 3
- Red Hat* Linux* server 8.0
- Red Hat Linux Advanced Server 2.1
- Caldera* OpenUnix*³ server 8.0

² The Novell NetWare Operating System is not supported on the SE7210TP1-E server platform.

³ The Caldera OpenUnix operating system is not supported on the SE7210TP1-E server platform.

8.4 Internationalization

The installation console will determine the local machine language and load the appropriate resource files. If there are no resources associated with the current language, US English resources will be loaded by default.

8.5 Installation User Interface

To start ISM setup from a console/server, execute setup.exe located at ISM\software directory on server systems resource CD image. Alternatively the installation may be launched from the server system CD menu that is automatically displayed when the CD is installed and “auto-runs”.

8.5.1 Starting ISM Setup

Once ISM setup is launched and during the initialization stage, ISM setup program reads all of the configuration files (INF files) and checks them for syntax and logic accuracy.

If any errors are found an error message will be displayed to the user and ISM setup will exit.

8.5.2 Installation Types

Once the configuration files have been read and initialized without any errors, the user will be asked to select from one the following three installation options:

- **Local install:** This option will install ISM on the local system where ISM setup is running on. The user will not be able to select individual ISM components or an additional system on which to install ISM.
- **Multiple system install:** This option will allow the user to select the target systems on which he/she would like to install ISM. Again the user will not be presented with the screen to select individual ISM components, however, the user will be able to choose the local machine as one of the selected target systems.
- **Custom install:** With this option the user will have the capability of selecting individual ISM components as well the target system where ISM will be installed.

8.5.3 License Agreement

The installation process will display the Intel Software License Agreement. The user will be able to continue with the installation only after accepting the terms of the agreement.

8.5.4 Feature Selection

This dialog box will be displayed only if the user has selected the Custom Installation option from the installation type screen. The user will be able to select which features to be installed on the target computers. However, even if a feature was selected for installation, it will be installed only if its condition is verified. A list of installed features will be kept in the ISM root directory on the target system in the Installation log file (logfile.log).

Features can be selected and deselected by clicking on the icon associated with a feature. The feature description will be displayed when a feature is highlighted.

A feature will be installed only if its parent has been selected. The control interface will automatically select the parent of a feature if the feature is selected. It also deselects all the siblings of a parent if the parent is deselected.

The features that are selected will be designated using two different icon images. If a feature and all its subsets (siblings) are selected, it will be designated with a full color checked box. Whereas, if some of siblings of a feature are not selected, the feature will be designated with a gray checked box. The features that are not selected will be designated with an empty unchecked box.

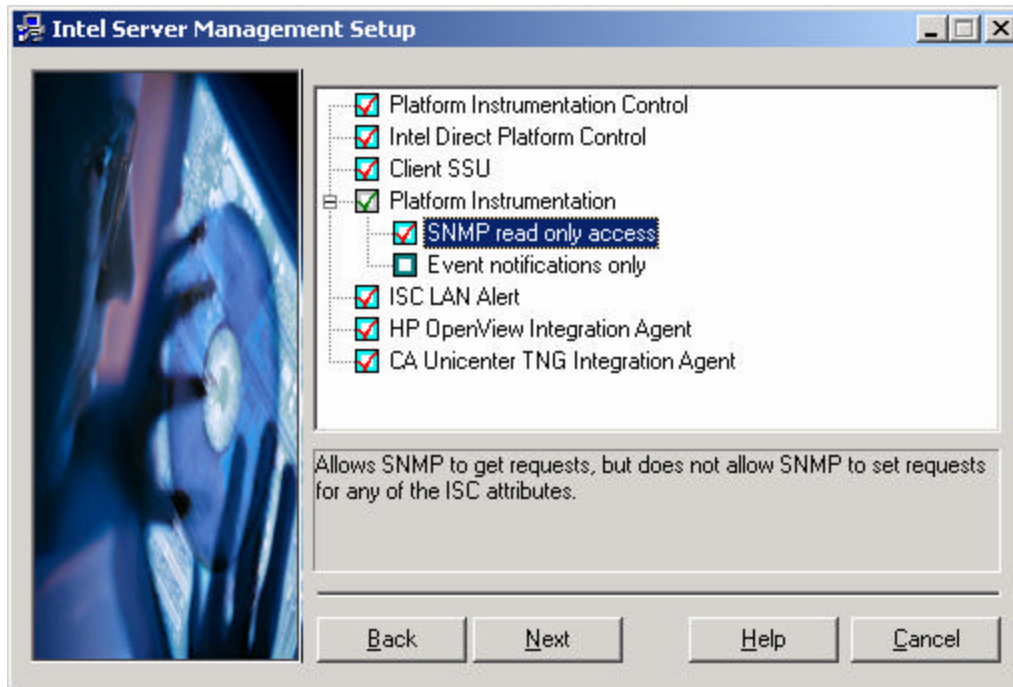


Figure 7. Installable Features

Intel Server Management 5.x will install the following client/server applications:

- **Platform Instrumentation Control (PIC):** supported on Windows 2000, Windows Server 2003, and Windows XP professional. If selected, this feature will also install Intel Server Management StandAlone Console.
- **Direct Platform Control (DPC):** supported on Windows 2000, Windows Server 2003, and Windows XP professional. If selected this feature will also install Intel Server Management StandAlone Console.
- **Client SSU Control:** Supported on Windows 2000, Windows Server 2003, and Windows XP professional.

- **DMI Browser:** supported on Windows 2000, Windows Server 2003 and Windows XP professional. This feature will be automatically installed as part of the Intel Server Management StandAlone Console.
- **Platform Instrumentation:** supported on Windows 2000, Windows Server 2003, NetWare 6.x and 5.x, OpenUnix server 8.0, Red Hat Linux server 8.0, and Red Hat Linux Advanced server 2.1. Installing this feature will also install the DMI Service Layer.
- **Event Notification Only:** This feature will allow only notification alerts for each server event, but does not allow operating system shutdown, hardware reset, or server power off action.
- **SNMP Read Only Access:** This feature will allow SNMP to get requests, but does not allow SNMP to set requests for any of the ISM attributes.
- **Hewlett-Packard OpenView integration agent:** only installed if the HP OpenView console is present on the selected systems. If this feature is installed, all ISM console tools (PIC, DPC, Client SSU or DMI Browser) will be integrated into the HP OV console.
- **Computer Associates Tng Unicenter integration agent:** only installed if the CA Tng Unicenter console is present on the selected systems. If this feature is installed, all ISM console tools (PIC, DPC, Client SSU or DMI Browser) will be integrated into the CA Tng Unicenter console.
- **LanAlert Viewer:** This feature will monitor the firmware generated SNMP traps from a server, i.e. any supported sensor status change. Supported on Windows 2000 and Windows XP. These SNMP traps are not traps generated by the remote operating system.
- **Command Line Interface:** This feature will install both the CLI proxy and the DPCCLI application on the target system. This installation only supports installing CLI on Windows based consoles. To install CLI on Linux, use the RPM contained on the ISM CD.

8.5.5 Remote Destination Selection

A dialog box will be displayed and will have the “Add/Remove” options only if the user has selected either the multiple install or the custom installation option from the installation type screen.

When the Add button is clicked a dialog with the network map appears. The user can either browse the network tree or manually enter a system name (following the UNC format) in the edit box in order to select a computer for installation. The destination list shows the selected systems.

After selecting a system, the user will be prompted for a user name and password having administrative rights on the targeted system.

Important: If the current windows settings uses encrypted passwords, the user cannot connect to a Caldera* UnixWare server running VisionFS*. To enable the system to accept plain text passwords, the user must add the following registry key to the system.

1. Open the systems registry by typing regedit using the Run option on the Start menu

2. Select HKEY_LOCAL_MACHINE
3. Select System\CurrentControlSet\Services\Rdr
4. Select the “Parameters” Key (or create a new one if it does not exist)
5. Add the following (DWORD) value: EnablePlainTextPassword
6. Modify the value and assign a data value of 1 (numeral one).
7. Exit the registry
8. Reboot the system prior to running ISM setup.

Upon exiting the network map dialog box, the user will be taken back to the “Add/Remove” dialog box. However now the dialog box will be showing the list of system selected along with their default destination paths. The default directory on the destination computers will be:

- Windows 2000, Windows server 2003, and Windows XP: “Program Files\Intel\Server Management”
- NetWare: “sys:system”
- OpenUnix: “/intel/server control”.

OEMs can set a default path other than the ones mentioned above for the ISM software destination on the target systems by adding a default path in the xxxISCsetup.inf file.

When the user clicks Install Now, a message box will be displayed to warn the user that Win32 target system will automatically be rebooted:

The user will be able to modify the destination directory by right-clicking the desired system and entering a new path. Only the systems with Windows can have their paths edited. Highlight a computer from the destination list and select Add or Remove to add or remove a system from the list. After selecting “Edit Path” the user can modify the installation path on the destination computer.

8.5.6 Local Destination Selection

When the user selects the Local Install only option of the ISM setup, it will presented with the following screen indicating that the local machine is the selected machine. The user will not have the choice of adding additional system. However, the user will be able to change the default destination path.

A status screen will show if any errors occurred while transferring files to the target machine. It will also show the location of the log file on the target system created during the installation process.

Upon completion of file transfer to the target system, the information screen will display whether the “Local install” program, which is the next phase of the install was successfully initiated on the local or remote machine.

If there are no errors during this stage the program will move automatically to the next screen. However, if there are errors, the program stays on this screen so the user can see the error message text and the “Next” button will be enabled for the user to go to the next stage of the setup.

The next screen is a progress screen if a local install is in progress. However, for a remote install only, the next screen will be an information screen that allows the user to exit the program.

Before starting the local install program, the installation can be halted. However, once the local installation is initiated, the installation will run its full course.

8.5.7 System Shutdown Screen

On the local machine installation, the user will be presented with the following dialog box for rebooting the system at the end of install process. The user will have the choice of forcing an immediate reboot by choosing “Reboot now”, or postponing the reboot until later by choosing “Reboot later”. Otherwise, the setup program will reboot the computer automatically after 60 seconds.

This dialog will not appear on remote installations, and the remote system will be rebooted automatically after 60 seconds. The Close button will stay gray. It is only activated for remote installs only.

8.5.8 Log File

The LocalSetup process will generate a log file called logfile.log on the local machine. The log file will contain the following information about the installation:

- List of features installed successfully
- List of installed components
- List of copied/replaced files
- Any error messages

8.6 Silent Installation

The Intel Server Management installation framework can be executed without user interface/interaction. In addition to the all the configuration files described, the user will have to supply a text file listing the systems on which to install ISM components and launch the setup application with the following command line parameters (not all are mandatory).

- **/silent**: path to the silent configuration file. Can either be a full path or just the file name if the file is located in the same directory as the setup program. This parameter is mandatory in order to install ISM in silent mode.
- **/username**: user name used to grant administrative rights on local/remote systems. This parameter is optional and/or can be overwritten in the silent configuration file.
- **/password**: user password. This parameter is optional and/or can be overwritten in the silent configuration file.
- **/log**: path to log file. Optional.

Examples:

```
Setup.exe /slient:silent.txt
Setup.exe /slient:c:\iscinstall\silent1.txt
Setup.exe /silent:silent.txt /username:eric /password:iscinstall
Setup.exe /silent:c:\isc\silent.txt /username:eric /password:iscinstall
        /log:c:\temp\install.log
```

Silent configuration file has to contain the following section.

```
[Destinations]
destination1, [Username], [Password]
destination2, [Username], [Password]
...
```

destination:

Remote/local system name. Must use the Universal Name Convention (UNC see example). When installing on the local system the system name can be replaced by the keyword Local.

```
[UserName]
```

Optional.

User name used to grant administrative rights to the setup application on the remote/local system. If this value is not defined, the setup program will use the value passed by command line parameter /username.

```
[Password]
```

Optional. Must be set if the username parameter was set.

Example:

```
[Version]
Signature="$Windows NT$"
Provider="Intel Corp, ESG"
  [Destinations]
  \\sayoung-desk, sueyoung, @password
  \\fred-nt, MyUser, password2
  Local, eric, password10
```

This above example will attempt to install ISM on the local system and on [\\sayoung-desk](#) and [\\fred-nt](#)

8.7 Uninstall ISM Features from Local Win32 System

There are three ways to uninstall ISM from a local Win32 system:

- **Using the control panel:** To uninstall ISM using the control panel, go to the Control Panel, Add/Remove Programs screen. Select Intel Server Management Version x.x in the list box. This selection will uninstall all ISM's features.
- **Using the start menu:** To uninstall ISM using the start menu, select Start / Programs / Intel Server Management and choose the uninstall option on the menu.
- **Using the CD:** The user can also remove ISM from the local machine by running the *uninstall.exe* program from the CD.

8.8 Uninstall ISM from Remote System (Win32, OpenUnix, NetWare)

To uninstall ISM from a remote console/server launch *uninstall.exe* located at \software directory on ISM's CD image. ISM can only be uninstalled from one system at a time so the user needs to select the desired system from which ISM is to be removed. The user can select a remote or a local system. The uninstall program is then initiated and launched automatically for Win32 systems.

Upon completion of the uninstall module, a shutdown screen will be displayed for the user. The user will have a choice of shutting the system immediately or later. If nothing selected the system will automatically shutdown after 60 seconds.

8.9 Recommended Files and Windows Registry Tree Structures

8.9.1 Source Files

Even though there are no restrictions on where applications installed by the Intel Server Management should install their binaries, it is recommended that all files will be copied into %ISCPATH%\bin (on Win32 platforms). That directory will be added to the system path.

8.9.2 Windows Registry

The Intel Server Management Windows Registry tree structure will have the following format:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Intel
      \Server Control
        \Console
        \Server
```

All ISM console and server applications should create their 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
          ...

```

8.10 Creating Configuration Files

In order for a component to be installed by ISM's installation framework, it must create or update all of the following sections.

8.10.1 Setup Control File: XXXISCSetup.inf

When the ISM setup is started, the setup will first determine the console language then it will try to open the corresponding ISCSetup.inf file (e.g. espSetup.inf) . That file contains the list of all the installation sections and their locations. If the corresponding language control file is not found, ISM will install the default US version (enuISCSetup.inf) components.

8.10.2 Default Install Path

OEMs can set a default path for the ISM software destination on the target systems by adding the following section:

```

[DefaultPath] // optional
DefaultDir=\program files\intel\Server Managment

```

If user does not include a drive letter, setup will use the drive that has the program files directory. If directory starts with a back slash it will assume a directory off of the root directory. If directory does not start with a back slash it will assume the user wants to start from Program files directory

9. Security

Intel Server Management 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, the password 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.

Note: The Server Board SE7210TP1-E uses an MD5 rather than MD2 hash.

9.1 Security Implementation

ISM v5.x provides the same security enhancements as previous releases of ISM. 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.

9.2 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 ISM v5.x release of the PI provides the following enhancements to improve the PI security:

- Replacing the legacy method for performing powerful control actions with a new version that requires 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.

9.2.1 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 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.

Note: SE77210TP1-E uses an MD5 hash.

9.2.2 LRA Notification-Only Control

ISM installation provides an option to configure services that use automated actions so that it will provide only notification actions (no power control actions). 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 lra.cfg file, LRA will have the ability to perform power control actions. The default is to have this option set to false.

9.2.3 SNMP Read-only Access Control

The ISM 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 System Setup Utility

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.

9.8 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 7. 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>				<R>				<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>		<i>		<y>
	<*>		<:>		<J>		<Z>		<j>		<z>
	<+>		<;>		<K>		<[>		<k>		<{>
	<, >		<<>		<L>		<\>		<l>		< >
	<- >		<=>		<M>		<]>		<m>		<}>
	<. >		<>>		<N>		<^>		<n>		<~>
	</>		<?>		<O>		<_>		<o>		

10. Service Partition

Some types of remote management require a special disk partition, called a Service Partition, on the target server. The Service Partition is established when the system is initially set up and it is populated with Datalight's ROM-DOS*, along with utilities, diagnostics, and any other software required for remote management.

Note: The Service partition is not supported on the Server Board SE7210TP1-E .

The Service Partition has a collection of software and hardware components that provide the support to allow remote execution of setup utilities, configuration utilities, diagnostics, etc., as well as remotely reset and power control the managed server.

The Service Partition is not marked as an active partition and the server will only boot from it when a special request is issued. The Service Partition is not normally visible to the average user because it has a special, non-standard partition type. Therefore, it does not appear as an accessible file system to the end user operating system. However some low-level disk utilities can see the partition entry, as in the case of Windows based Disk Administrator, and allow a drive letter to be assigned to the Service Partition.

10.1 External Dependencies

This section provides an overview of some of the elements of Service Partition that are covered in detail in other sections of this specification or platform-specific technical specifications. Some understanding of these elements is required to understand the complete function of the Service Partition environment.

10.2 BMC Firmware

The Baseboard Management Controller subsystem is the means by which a management console initially connects to the target server. The BMC subsystem supports connection via serial/modem or LAN interfaces. It provides commands that allow the management console to remotely perform the following actions in support of the offline service environment:

- Query operating system status
- Request operating system shutdown
- Request a service boot
- Reboot server
- Validate remote management passwords

The BMC subsystem is configured in the Platform Event Manager of the System Setup Utility on the target server. The Configure EMP menu is used to enable and configure remote serial management. The Configure LAN menu is used to enable and configure remote LAN management.

Some platforms also support the Server Configuration Wizard (SCW) . This includes the SE7500WV2 platform. The SCW is used to configure LAN and EMP remote management through a wizard-based interface.

10.3 BIOS Support for Service Boot

The BIOS on the target server includes support for booting from a Service Partition that is installed on a local hard disk. The BMC firmware and BIOS on the target server work together to support the request and execution of a service boot. The BIOS also supports a local service boot, which does not involve a remote management console.

Note: The Server Board SE7210TP1-E does not support a Service Partition.

10.4 BIOS Console Redirection

BIOS console redirection is initially enabled immediately prior to a service boot. Its purpose is to redirect the text mode screen and keyboard to the management console via the serial port or LAN. BIOS redirection is used to access BIOS setup and to view pre-boot messages on the server screen. Once the service operating system boots, BIOS console redirection is disabled, freeing the serial port or LAN controller for the use by the Remote Service Agent.

10.5 Intel Server Management Console

The Intel Server Management Console can be described as the GUI application that is used to remotely utilize the target server's offline service environment. It is capable of communicating with the target server via modem or LAN, and it is able to understand the various communication protocols and interfaces involved.

The Intel Server Management Console transitions through the following modes of communication as the offline service environment initializes:

- IPMI 1.5 protocol to initially connect and initiate a service boot
- Raw ASCII screen data from BIOS console redirection
- TCP/IP protocol over a PPP or Ethernet connection.
- Socket based communication with Remote Service Agent
- Protocol-based console redirection
- FTP protocol for file transfer

10.6 Service Partition Type

The partition type used by the Service Partition is 12H.

Note: There is no official registry of partition types and therefore, there is no way to ensure that type 12H will never conflict with other software.

10.7 Firmware / BIOS Service Boot Support

The firmware maintains three bits related to booting from the Service Partition:

- BOOT bit: Request BIOS to perform a Service Partition boot
- PRESENT bit: Service partition is present.
- SCAN bit: Request BIOS to detect presence of Service Partition.

The BIOS and firmware include support for a service boot failsafe 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 the handler for the timer restarts the system normally.

10.8 Remotely Initiating Service Partition Boot

When the management console connects to the target server, it is communicating with the server's BMC interface. An IPMI command is sent from the management console to set the BOOT bit. If the connection is via modem, BIOS uses the same serial port settings as EMP. This allows the remote user access to BIOS setup and the ability to see BIOS screen messages.

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 BIOS console redirection, even if it is not enabled in the normal BIOS setup.
2. It searches the partition table for a partition type 12H.
 - 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. If the BIOS does not find a Service Partition, it displays an error message on screen and logs an error to the System Event Log. The user at the management console sees the error message via BIOS console redirection.

Note: The BIOS clears the BOOT bit whether a Service Partition is found or not. This prevents repeated Service Partition boot attempts.

10.9 Local Boot from Service Partition

It is possible to boot the server locally from the Service Partition, while working at the server's console. This feature allows the user to run utilities from the Service Partition while physically present at the target server.

Depending on the platform's BIOS, there are two methods for activating a local boot to the Service Partition. On some platforms, during BIOS POST, the BIOS displays a message showing a function key such as "F4" that can be pressed to request a boot to the Service Partition. On other platforms, the user must enter BIOS setup and enable a setup option to request a boot to the Service Partition.

To activate a local boot from the Service Partition, the user must shutdown and restart the machine, then depending on the platform, either press a function key during BIOS POST or enter BIOS setup and enable a one-time boot from the Service Partition.

After the system boots from the Service Partition, the user can use a command-line interface to execute software that was installed on the Service Partition or load new software from the floppy diskette drive.

10.10 Service Partition Installation

The Service Partition must be in place before the target server can be managed remotely. The System Resource CD includes the files necessary for the installation. Installation is done in two steps, Section 8 contains details about the user interface:

1. The user boots the System Resource CD and runs Service Partition administration, a utility similar to FDISK, to create the Service Partition. The system is then rebooted from the System Resource CD.
2. The utility is used again to format the Service Partition and to install software. Following the format operation, the Service Partition administration utility automatically invokes a batch file that copies operating system files, Remote Service Agent files, remote diagnostic files, and other required files from the CD to the appropriate directories on the Service Partition.

The Service Partition administration utility drives the underlying ROM-DOS FDISK and FORMAT commands. Its purpose is to guide the user and ensure the correct installation of the Service Partition. At the same time, it hides the complexity and risks of the FDISK and FORMAT tools.

The Service Partition is at least 39 MB in size and formatted with a FAT16 file system. The actual size of the partition may be larger depending on the geometry of the hard drive. Following the successful installation of the Service Partition, the Service Partition administration utility sets the PRESENT bit. The partition table entry and disk space required for the Service Partition must be available before it is installed. Because of this, the Service Partition is normally installed before the end user operating system.

ROM-DOS can only access the first 8 GB on any hard drive. Hard drives that are larger than 8 GB must not have any existing partitions prior to installing the Service Partition. The Service Partition must be installed first in order to safely ensure that the Service Partition resides within the first 8 GB on the drive.

If the end user installs a new or replacement disk, the Service Partition should be installed prior to the end user operating system. Users wishing to install the operating system first must preserve sufficient space on the disk if they intend to install the Service Partition at a later time. Installing the Service Partition after the operating system is only allowed if the hard drive is smaller than 8 GB. The Service Partition install process does not have the ability to resize existing partitions.

10.11 Scan And Present Bits

Each time the BIOS boots, it checks the SCAN bit. If the SCAN bit is set, BIOS checks for the presence of a Service Partition and, depending on the outcome, it either sets or clears the PRESENT bit. The PRESENT bit will also be set during the Service Partition installation.

The PRESENT bit is used to discover whether the server has a Service Partition installed. The SCAN bit is useful 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. The SCAN bit should be set periodically by the management console, so that the PRESENT bit accurately reflects the presence of a Service Partition. After the scan, the BIOS clears the SCAN bit.

10.12 Service OS / System Resource CD Hidden Partition Support

A special version of ROM-DOS is used to provide support for the hidden partition. The partition type of the hidden partition (12H) is not a normal DOS-compatible type. Therefore, the version of ROM-DOS installed on both the System Resource CD and the hidden partition contains support to create and recognize the special hidden partition type.

10.13 Service OS Initialization

When the service operating system begins to run, software and drivers needed to initialize the remote environment are loaded by the config.sys and autoexec.bat files.

10.14 TCP/IP Stack for Remote Communication

When the management console first connects to the target server it is communicating with the server's BMC using an IPMI 1.5 session. Although the BMC supports power and reset control of the target server, it is insufficient to provide efficient communication with software running on the target server's processor.

For communication between the target server processor and the management console, a third party TCP/IP stack will be utilized. A TCP/IP stack is standards-based and ensures reliable, efficient communication. TCP/IP can also work over a LAN or serial port. As an added benefit, TCP/IP supports multiple endpoints, allowing multiple processes to share the same connection. For example, a socket-level text redirect session and a file transfer can be supported at the same time.

The Service Partition environment utilizes a TCP/IP network protocol stack called Fusion^{*}, from Pacific Softworks, Inc. The Fusion stack includes PPP, TCP/IP, UDP, and FTP protocols, along with a basic multi-tasking kernel. The Fusion software is designed for embedded applications and is independent of the operating system. The figure below shows the basic elements of the Fusion networking stack.

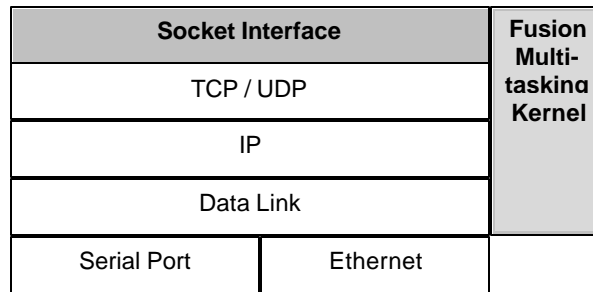


Figure 8. Fusion TCP/IP Network Stack

10.15 Network Initialization

Network Initialization is the same as RSA Initialization please refer to Section 10.20 for describes the steps taken to initialize the networking software.

10.16 PPP IP Address Configuration

For modem connections, the target server assumes the role of a PPP server. As a PPP server, it assigns private IP address for both sides of the PPP connection. By default, the target server side gets the address 192.168.0.10 and the client side gets the address 192.168.0.11. If these private IP addresses conflict with something on the client side, they can be overridden by editing Remote Service Agent invocation in the AUTOEXEC.BAT file on the Service Partition. For example,

```
rsapp /s 192.168.0.10 /c 192.168.0.11 /n 255.255.255.0
```

In this example, “/s” gives the target server side IP address, “/c” gives the management console side IP address and “/n” gives the value of the target server side netmask. To override the default addresses, all three parameters must be specified and both IP addresses must be on the same subnet.

10.17 PPP Serial Port Configuration

For modem connections, COM2 is the default serial port used by the PPP server because the EMP interface supports only COM2. The PPP server assumes that COM2 is configured to use IRQ 3 and port address 0x2f8. If the target server has a different configuration for COM2, the IRQ and port address can be overridden by editing Remote Service Agent invocation in the AUTOEXEC.BAT file on the Service Partition. For example,

```
rsapp /p 3e8 /i 4
```

In this example, “/p” gives the COM2 port address and “/i” gives the COM2 IRQ assignment. To override the default addresses, both parameters must be specified.

10.18 LAN Controller Configuration

To support LAN connections, the Fusion TCP/IP stack is configured with drivers for the LAN controller used on the platform. The Intel® 82550/82559 10/100 LAN controller and the Intel® 8254X 10/100/1000 controllers are supported.

There may be more than one instance or type LAN device on some systems. For example, one instance may be on the system board and another instance contained on a PCI add-in card. The correct instance to use in this environment is the on-board LAN device that is shared by the firmware subsystem.

The driver searches all PCI buses in the system for instances of supported LAN controllers. The driver identifies the correct LAN controller by comparing each LAN controller's MAC address with the one stored in the flash part of the Baseboard Management Controller (BMC). When a match is found, TCP/IP utilizes the matching LAN controller.

10.19 Remote Service Agent

The RSA runs on the target server after BIOS console redirection has been disabled and a PPP or LAN connection has been established with the management console. Once the RSA starts, it becomes the primary interface to the server from the outside world. Additionally, standalone applications running on the target server that are "network aware" interfaces to the RSA use the network services.

The RSA provides a number of remote services:

- Protocol-based text mode console redirection
- Management console control interface
- Interface to the network stack for standalone applications
- File transfer service
- Execution of DOS-based utilities

The figure below shows how the Remote Service Agent relates to the service operating system and the networking stack. The area within the dotted lines contains software that is bound directly to the networking stack. The area outside of the dotted line contains the service operating system and transiently loaded utilities.

Note: The Service partition and RSA are not supported on the Server Board SE7210TP1-E.

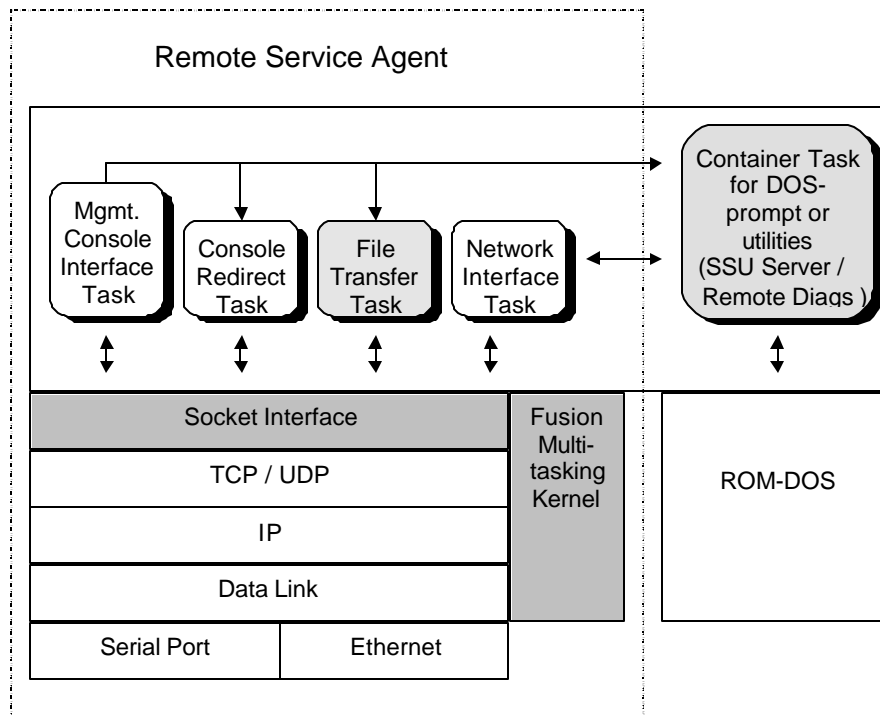


Figure 9. Remote Service Agent Overview

The multi-tasking capability shown in this section does not include applications that rely on DOS services. Even though multiple processes can use the network interface, there can be only one DOS-based utility or process running at a time. The shaded boxes in the figure indicate processes that use DOS services and cannot be executed concurrently.

10.20 RSA Initialization

The RSA and Fusion TCP/IP stack are bound into a single executable that loads from the AUTOEXEC.BAT file on the Service Partition. The RSA first determines from BIOS if the Service Partition boot was initiated remotely or locally. If it was a local service boot, the RSA exits to the DOS command prompt.

To support both modem and multiple LAN controllers with the smallest impact to conventional memory use, there are multiple RSA executables. RSAPPP.EXE contains RSA and the TCP/IP stack configured to support PPP. RSALANx.EXE (where x is a number) contain RSA and the TCP/IP stack configured to use a particular LAN controller. In other words, RSALAN1.EXE supports one type of LAN device, RSALAN2.EXE supports another, and so on.

The decision on which executable to use is made automatically during execution of the AUTOEXEC.BAT file on the Service Partition. One of the executables is invoked unconditionally with only the parameter "/findpath". This parameter tells RSA to determine from the on board firmware the path of the current firmware session. It determines if the session is over modem or LAN and what type of LAN device is in use. Based on the path, it will exit with a unique exit code that is then used by conditional statements in the AUTOEXEC.BAT file to invoke the correct executable.

10.21 Execution of DOS-based Utilities

The Remote Service Agent supports two methods of executing DOS-based utilities on the target server. The first method is via a command request from the management console for execution of a specific program. This method is used by the management console to run software for which it has prior knowledge, or software with a management console-based front end, such as Remote SSU.

The second method uses a combination of a DOS command shell and protocol-based console redirection. This method allows a user at the management console to remotely execute text-based DOS programs.

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

10.22 Modem-based Security

For modem connections, the target server's BMC subsystem is protected from unauthorized logins by a BIOS-based password. The password is established via BIOS setup. Once the remote client submits the EMP password and is allowed access to the server by the BMC subsystem, the transition to a TCP/IP based connection to RSA services occurs during the same modem connection.

10.23 LAN-based Security (IP Filtering)

When the management console first connects to the BMC subsystem via LAN, the session is authenticated via a CHAP-like mechanism. The authentication scheme uses the remote LAN password to authenticate the client without ever sending the remote LAN password over the network. The remote LAN session must be maintained while the server boots from its Service Partition.

When RSA starts, it asks the firmware for the IP address of the current authenticated client. Henceforth, all the services of RSA only accept connections from the authenticated IP address. Connection attempts originating from any other IP address are rejected. The IP filtering also applies to any network-aware applications running from the Service Partition. Those applications, such as SSU server, will only be presented with connection requests from a single authenticated IP address.

11. Enterprise System Management Console Integration

The suite of software applications known as Intel Server Management is designed primarily to allow a user to obtain detailed information pertaining to a single server. In large enterprise-wide network environments, a network administrator is more likely to use an application referred to as an Enterprise System Management Console (ESMC) to obtain information about the network. It is not uncommon to be able to integrate or “plug in” third party applications into these ESMCs so that a user can launch an integrated application from within the ESMC’s user interface. In addition, an ESMC will often display information provided to it by an integrated application such as the health of an individual server on the network.

This act of integrating ISM into ESMCs provides ease of use of ISM applications for network administrators, especially those who are dealing with very large networks. The typical user may have many server management applications, in addition to those of ISM, installed on the system that is being used to manage the network. Being able to select and launch an application on a per server basis within an ESMC framework allows significant ease of use.

This section will provide a high-level overview of the ISM software components that allow ESMC integration.

ESMC integration enables the following functionality:

- Discovery of ISM application services on a server.
- The capability to launch one or more ISM applications from within an ESMC framework.
- Registration for IA based server health events.
- The ability of an ESMC to display the health of an IA based server from within its user interface.

11.1 Supported Enterprise System Management Consoles

- Hewlett Packard OpenView Network Node Manager Version 6.2
- Computer Associates Unicenter, The Next Generation Version 3.0
- Intel Server Management, Standalone Console, Version 5.8

11.2 Supported Operating Systems

- Windows XP Professional
- Windows server 2003
- Windows 2000 (All versions)

11.3 Components

The components that make up ESMC integration are the ESMC agents, Console Tools Manager (CTM), and ISM application plugins. These components reside on the same system where the ESMC is running.

11.3.1 Console Tools Manager

The Console Tools Manager (CTM) is the primary component. CTM acts as a traffic controller coordinating communication between ESMC agents and ISM application plugins. Any communication that occurs between a plugin and agent must go through CTM. It is also used as a data repository keeping track of the associations between ESMC agents, ISM application plugins, and discovered IA based servers. CTM runs as its own process.

11.3.2 ESMC Agents

For each ESMC supported, there is an associated agent designed for that specific ESMC. This agent basically provides the connection between the ESMC and CTM. Information communicated to CTM from an agent would be information having to do with newly discovered servers by the ESMC and ISM application launch commands. Information supplied to the agent from CTM would have to do with server health and ISM application support on a server that the ESMC has discovered.

11.3.3 ISM Application Plugins

Each ISM application that can be launched from within an ESMC has a plugin associated with it. This plugin has been designed specifically for that ISM application. Similar to the ESMC agents, plugins provide a connection between an ISM application and CTM. Information communicated to the Console Tools Manager from a plugin has to do with a server's health and whether the application's service is running on a server. Information communicated to the plugin from CTM would be IP addresses of servers discovered by ESMCs and requests to launch an application on a particular server.

11.4 ESMC Functionality

Enterprise System Management Console integration provides the following functionality:

- Discovery of ISM application support on a server.
- The capability to launch one or more ISM applications from within an ESMC.
- Registration for overall server health events and enablement of the ESMC to display overall server health.

11.5 CTM/Agent Connection

When an ESMC is launched, a process for the ESMC's registered agent will also be launched. An agent process (hereafter referred to as an agent) facilitates communication between an ESMC and CTM and runs in its own process, just as does CTM.

The ESMC agent will start a CTM process and then connect itself to CTM so that CTM and the agent may communicate. Only one instance of CTM on a system can be running at one time. Any other ESMC agents that are subsequently launched will connect to the existing CTM instance.

In order to connect to CTM, an agent provides a reference to itself to CTM. CTM will take this agent reference and register it with itself. This enables CTM to keep track of all connected

agents and to communicate back to any one of them. When an ESMC is closed, CTM will unregister its agent.

11.6 CTM/Plugin Connection

An application plugin facilitates communication between an application's service running on an IA based server and CTM. Application plugins are implemented as DLLs that run in CTM's process space.

When CTM starts, it will check to find out which ISM applications are installed using the system registry. There is no point in going out over the network to look for ISM application services on a server if the application is not installed on the system. For all ISM applications found, that application's plugin DLL will be loaded and an instance of the application plugin instantiated. A reference to each plugin instance is then registered by CTM similar to ESMC agent references. If no ISM applications are installed and hence no ISM application plugins are installed, the agent attempting to connect to CTM will fail to connect and both the agent service and CTM will shutdown.

11.7 Server Discovery

When a new server is discovered by an ESMC, CTM will create an object representing the newly discovered server and register it within itself similar to what happens with agents and plugins. This server object will keep track of which agents have discovered the server and which plugins have discovered their required service on the server. Only one server object per IP address will ever exist at one time. When the object is created, the server IP address will be included as a data member. This will be done only once when the server is first discovered by an ESMC. The ESMC's registered agent will then be associated with the server object. Later, if a different ESMC subsequently discovers the same server, that ESMC's agent will also be associated with the server object. If there are multiple ESMCs resident on the system then it is possible for a server object to have associated with it multiple ESMC agents.

Next, CTM will send the IP address out to all application plugins that have been loaded, which will conduct a discovery of their required service on the newly discovered server. This will be done each time a server is discovered by an ESMC. If an application plugin successfully discovers its service on a server then the plugin will notify CTM to associate itself with the server object held by CTM.

When at least one of the plugins has notified CTM that it has discovered its service on the discovered server, CTM will notify the ESMC via its agent that an ISM application can be launched against the discovered server, with information identifying the particular application. Server health information will also be provided to the ESMC if that information is provided to CTM by the plugin. If other ESMCs have discovered the same server previously, those ESMCs will also be notified in case they need to update their user interface.

Upon receiving information that an ISM application can be launched against a discovered server, the ESMC will create an icon representing ISM within its user interface. This icon is usually associated with an icon representing the discovered server. If server health information is provided, the ISM icon will commonly be of a color representative of the health of the server. Some type of menu listing ISM applications is also created so that users may launch ISM applications against the discovered server.

11.8 Server Health

Each server object within CTM holds a member variable for server health state. This information is provided to CTM by each plugin whose service has been discovered on a server. Each plugin that discovers its service on a server will provide CTM with server health information, if it is able to. CTM will associate each plugin's server health information with the respective server object. Each time a plugin calls into CTM with new health information, CTM will examine each plugin's health contribution for the server object. The worst health contribution will be designated the overall health of the server. If a plugin's health update causes the overall server health to change, CTM will send a health update notification to all ESMC agents that are associated with the server object.

11.9 ISM Application Launch

Most ESMCs enable a user to launch an ISM application by right clicking on an icon that represents ISM and selecting an ISM application menu item from a popup menu. When a user does this, the ESMC will send the launch command to CTM via its agent. CTM will then send a launch command to the application's plugin with launch parameters, which would include the IP address to launch the ISM application against. Each plugin handles the launching of its application once the command to launch has been given.

11.10 Operation

Most of the functionality provided by ESMC integration takes place in the background and does not involve any user interaction. There is only one function provided by ESMC integration that requires user interaction and that would be to launch an ISM application.

11.10.1 Hewlett Packard OpenView Network Node Manager Server Health Display And Update

Within HP OpenView NNM, an icon representing ISM applications will automatically be displayed in a color that represents the health of the server. This icon is usually visible below the individual server level when navigating through the hierarchy of display levels. This will occur provided the server is running one or more of the ISM application services that are capable of supplying health information to HP OpenView NNM. If the health of the server changes, this information will automatically be supplied to HP OpenView NNM and the ISM icon color will change accordingly.

For HP OpenView NNM, the possible health states and associated colors are:

- OK Green
- Non-Critical Yellow
- Critical Orange
- UnKnown Blue

11.10.2 Computer Associates Unicenter TNG Server Health Display And Update

The manner in which CA Unicenter provides server health information for those servers running ISM application services is very similar to HP OpenView. Upon launching the 2D Map application, part of the CA Unicenter application suite, a window will appear with an ISM World View icon. This icon will be available if any Intel® servers running ISM application services have been

discovered. Double clicking on the icon will bring up window that contain icons representing each Intel server discovered that is running ISM application services. The color of each of these icons will represent the health of each individual server.

The color of the ISM World View icon represents the overall health of all Intel servers discovered that are running ISM application services. For CA Unicenter, the possible health states and associated colors are:

- OK Green
- Non-Critical Yellow
- Critical Red
- UnKnown Blue

11.11 Levels Of Discovery

There are two levels of information discovery that take place when an ESMC is launched and ESMC integration is in place. The first level is discovering all machines on a network. This is commonly accomplished by the ESMC. The second level is discovering what ISM application services reside on any of the machines that were discovered during the first level of discovery.

11.11.1 First Level Discovery

First level discovery is the process of discovering machines on a network. For ISM 5.0, the first level of discovery will be performed by the ESMCs themselves just as in previous versions of ISM. When an ESMC discovers a new IA based server, it will send an event over to CTM via its agent as explained previously. CTM will then take over from there, which actually involves second level discovery, explained next. Once tool support and health (second level discovery) for any given server is determined, CTM will cache this information in a server object and notify all agents that know of the particular server via their agents as described previously.

11.11.2 Second Level Discovery

After a server has been discovered through first level discovery it must then be determined which ISM tools are supported on the server and the server's overall state of health. The process of doing this is referred to as second level discovery. Most of the process of second level discovery has already been explained previously in this document.

12. LAN Alert Viewer

The LanAlert Viewer Intel® Server Management application is implemented using Java and provides a user interface to see detailed alert information sent from a configured server. On client systems running Windows 2000, Windows 2003, and Windows XP Professional, LanAlert Viewer supports monitoring of server firmware generated Simple Network Management Protocol (SNMP) packets. The LANAlert Viewer architecture consists of two modules:

- Alert Viewer: A Java console that provides a user interface to see alert information.
- Alert Manager: A COM server that runs as a service in Windows XP Professional and Windows 2000. This module is responsible for monitoring and decoding LANAlerts. It contains modules to receive firmware generated Simple Network Management Protocol traps using Microsoft Windows Simple Network Management Protocol trap service or raw sockets depending on the platform and service availability.

Lan Alerting is built on top of another the Platform event filtering 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.

12.1 Alert Viewer

The LanAlert Viewer can be launched from the Intel Server Management program group. It displays all of the alerts that the Alert Manager has received since the system initialized. It will add new alerts when they occur, depending on the alert notification selection. All the new or unacknowledged alerts will have a red icon associated with it in the first column. The LANAlert Viewer has seven buttons at the window bottom. Each action is explained in Table 8.

Table 8. LANAlert Viewer Buttons

Button Name	Description
Configure	This launches the LANAlert configuration dialog which allows the user to configure different notification and viewer options
Select All	Selects all alerts.
View Details	This will launch the detailed view of the selected alert(s), which will have all the information about the selected alerts.
Acknowledge	This sets the selected alerts' "status" to acknowledge. This means the user has seen and is aware of the alert. The red icon will be removed from the first field for acknowledged alerts.
Delete	Removes the selected alert from the list.
Close	This closes the viewer.
Help	Display the help dialog.

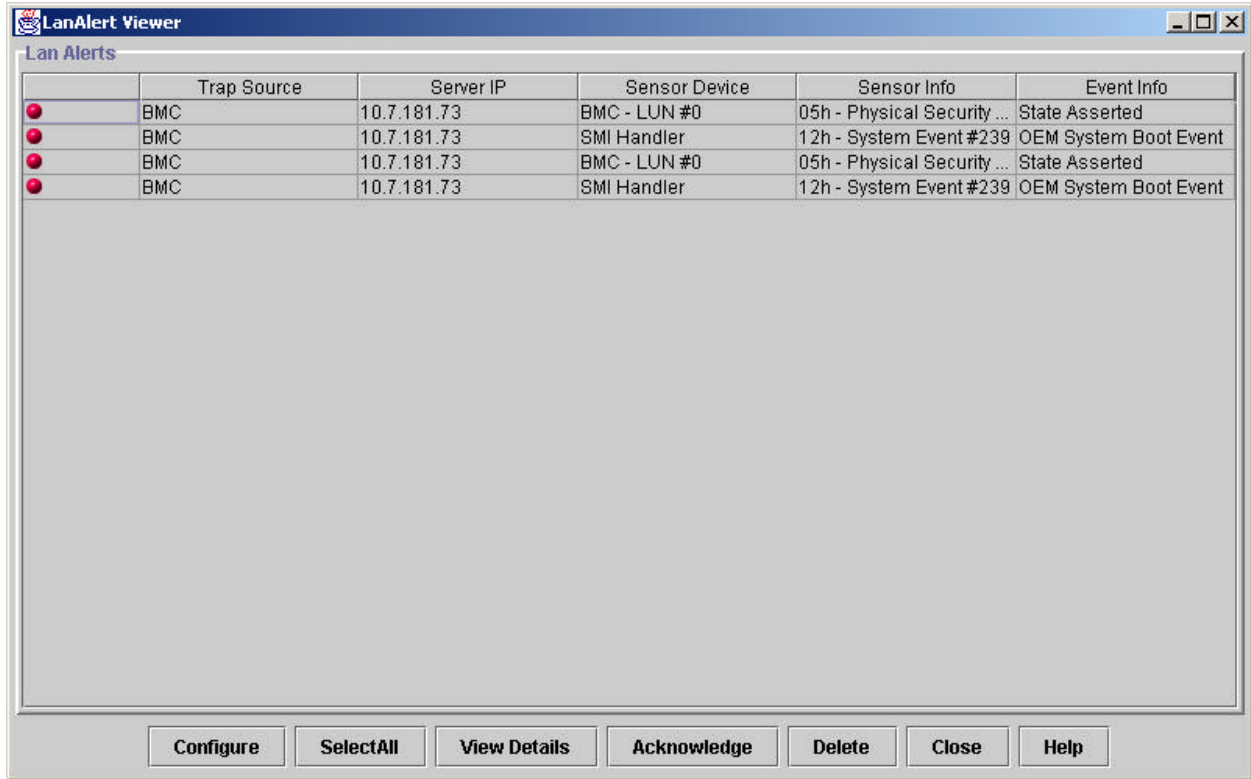
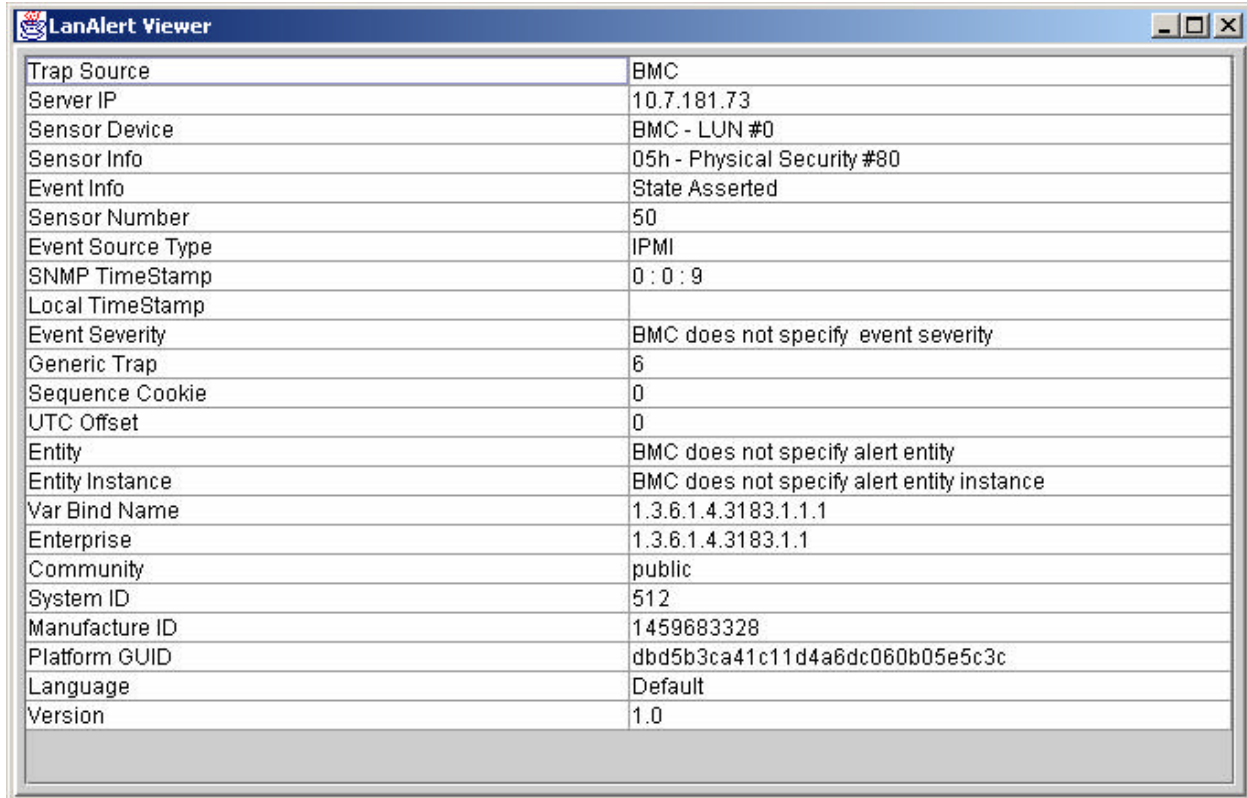


Figure 10. LanAlert Viewer

The LanAlert Viewer is available for launching from the program menu under Intel Server Management. Launching the application will start the viewer as well as the manager if the manager is not already running. The Alert Details dialog box displays information about the LANAlert.



Trap Source	BMC
Server IP	10.7.181.73
Sensor Device	BMC - LUN #0
Sensor Info	05h - Physical Security #80
Event Info	State Asserted
Sensor Number	50
Event Source Type	IPMI
SNMP TimeStamp	0 : 0 : 9
Local TimeStamp	
Event Severity	BMC does not specify event severity
Generic Trap	6
Sequence Cookie	0
UTC Offset	0
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	512
Manufacture ID	1459683328
Platform GUID	dbd5b3ca41c11d4a6dc060b05e5c3c
Language	Default
Version	1.0

Figure 11. LanAlert Details Dialog Box

12.2 Simple Network Management Protocol Trap and LANAlert

The description of various fields of the Platform Event Trap (PET) format that is typically a Simple Network Management Protocol-Trap format is listed below from the Baseboard Management Controller perspective. Refer to the Platform Event Trap specifications, located on the IPMI web site (<http://www.intel.com/design/servers/ipmi/index.htm>) for more details. The alert implementation in the Baseboard Management Controller encodes the trap fields and bundles them into Type-Length-Value format.

The specific trap and 'variable-bindings' field encodes the alert information for the alert-recipient.

12.3 Header

The trap header consists of the following two fields.

Version	SNMP rev-1
Community String	Configurable by the user. Default is 'public'.

12.4 Protocol Data Unit (PDU)

The trap protocol data init fields are described in Table 9.

Table 9. Protocol Data Unit Fields

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-bit Integer. The Baseboard Management Controller 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 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	<p>Time elapsed between last (re) initialization of the network entity and the generation of the trap. The unit is 1/100th of a second.</p> <p>The Baseboard Management Controller initializes this timer when it receives a request from the BIOS to log a system boot.</p>
Variable-bindings	See Section 12.5: Variable Bindings Field.

12.5 Variable Bindings Field

This field is a part of the trap Protocol Data Unit and it carries the bulk of the event trap information. The Baseboard Management Controller packs 46 bytes of information in this field.

The Object Identifier for this varbind is: 1.3.6.1.4.1.3183.1.1.1

Table 10 lists the different fields and their position in the string. Data is in the network byte order (ms-byte first).

Table 10. Variable Bindings Fields

Offset	Name	Size	Description
1:16	GUID	16 bytes	Globally unique ID (GUID) for the platform. All 0's = unspecified (use agent-addr to identify the platform that generated the trap).

Offset	Name	Size	Description
17:18	Sequence # / Cookie	Word 2 Bytes	0000h = unspecified. The Baseboard Management Controller maintains a sequence number for the Alert message it is sending. This might be useful for the console software running at the remote node (client) to identify the new instance of the Alert message and ignore the processing of the same message received through network due to recirculation. This number should not be used for tracking the lost message as the Baseboard Management Controller does not keep the history of the sent messages and does not expect any acknowledgement from the client on reception of the alert message.
19:22	Local Timestamp	Dword 4 Bytes	Differs from Simple Network Management Protocol trap timestamp in that this is platform local time based. Encoded as number of seconds from 0:00 1/1/98. 0000 0000 = unspecified.
23:24	UTC Offset	Word 2 Bytes	Universal Time Coordinated (UTC) Offset in minutes (two's complement, signed. -720 to +720, 0xFFFF=unspecified).
25	Trap Source Type	Byte	This describes the sender of the trap over network. 20h for the.
26	Event Source Type	Byte	Class of device or type of software that originated the event: This can be different from the device or type of software that sends the trap. The Baseboard Management Controller sends this as Intelligent Platform Management Interface (IPMI) – 20h
27	Event Severity	Byte	Severity (based on DMI Event Severity). 00h = unspecified 01h = Monitor 02h = Information 04h = OK (return to OK condition) 08h = Non-critical condition 10h = Critical condition 20h = Non-recoverable condition The Baseboard Management Controller leaves this field unspecified.
28	Sensor Device	Byte	Identifies the instance of the device that holds the sensor that generated the event. The Baseboard Management Controller maps it to Byte 1 (bits 7-1) of 'Generator Id' field of the Event Message. FFh = unspecified.
29	Sensor Number	Byte	The Sensor Number field is used to identify a given instance of a sensor relative to the Sensor Device. The Baseboard Management Controller maps this to Sensor Number field of the Event Message FFh = unspecified. 00h = unspecified.
30	Entity	Byte	Entity ID from Intelligent Platform Management Interface v1.0 specification. Indicates the platform entity the event is associated with (e.g., processor, system board, etc.) The Baseboard Management Controller 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 Baseboard Management Controller leaves this field unspecified. 00h = unspecified.

Offset	Name	Size	Description
32:39	Event Data	8 Bytes	Other event specific information. The Baseboard Management Controller maps this to 'Event Data 1', 'Event Data 2' and 'Event Data 3' of the event message. Rest 5 bytes are padded with FFh.
41:44	Manufacturer ID	Dword 4 Bytes	Manufacturer ID using Private Enterprise IDs per Internet Assigned Numbers Authority (IANA). The Baseboard Management Controller uses this from Field Replaceable Unite (FRU).
45:46	System ID	Word 2 Bytes	This number can be used to identify the particular system/product model or type. The Baseboard Management Controller returns same as the product-Id field in the application command GetDeviceId.

12.6 Alert Configuration

The Baseboard Management Controller maintains an event filter table that is used to select the events that will trigger a LAN Alert. 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 sends an alert when an event matches one of the filters.

LAN Alerts 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
- 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

12.7 Platform Event Manager

The Platform Event Manager module in the System Setup Utility lets the user configure the following:

- Platform Event Paging (PEP): pages the user to notify him/her of events on the server.
- BMC LAN Alert (LAN): sends a LAN alert to notify the user of events on the server.
- Emergency Management Port (EMP): analog modem configuration and numbers on the server.

Some platforms also support the Server Configuration Wizard (SCW). Currently this includes the SE7500WV2 platform. The SCW is also used to configure LAN Alerting options through a wizard-based interface.

13. Platform Event Paging

Platform Event Paging is built into the Intel Server Management 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.

Note: Platform Event Paging is not supported on the Server Board SE7210TP1-E.

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 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 in use by another application, the BMC will interrupt and take ownership of the modem to complete the page.

13.1 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.

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

13.2 Platform Event Manager

The Platform Event Manager module within the System Setup Utility allows the user to configure the following:

- Platform Event Paging: pages the user to notify him/her of events on the server.
- BMC LAN Alert: sends a LAN alert to notify the user of events on the server.
- Emergency Management Port: analog modem configuration and numbers on the server.

Some platforms also support the Server Configuration Wizard (SCW). Currently this includes the SE7500WV2 platform. The SCW is used to configure paging options through a wizard-based interface.

14. 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.

Note: ICMB is not supported on the Server Board SE7210TP1-E.

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 Management.

ICMB provides the ability to communicate the following information:

- Chassis management functions
- System Event Log
- Chassis power control
- Field Replaceable Unit part numbers and serial numbers

On IA-32 based systems the ICMB card is plugged into a standard expansion slot and into the IPMB cable system board connector.

14.1 ICMB Requirements

The user 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 the user must do the following:

- Set up an ICMB Connection
- Configure the point server for ICMB

14.1.1 Setting Up an ICMB Connection

In general, the user must meet the following connection requirements to manage or monitor servers through an ICMB connection:

- Establish a Management Point Server. This server is a managed server that has an ICMB interface and has the ISM software installed.
- A functional LAN connection must exist between the Management Point Server and the client workstation.

- All servers to be managed or monitored 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 details on connecting a specific server platform for ICMB management, refer to the server's product guide.

14.1.2 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:

14.1.2.1 Windows NT and Windows 2000 Systems

1. Go to the services control panel.
2. Start the Intel EIF Agent service⁴.

14.1.2.2 NetWare Systems

1. Open the ISC_ON.NCM file for editing.
2. Remove "rem" from the 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.

14.1.2.3 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
```

14.2 Setting Up ICMB

The Intelligent Chassis Management Bus (ICMB) feature allows the user to interconnect and share management information among multiple remote devices even when these devices do not have Intel's server management Platform Instrumentation installed. For example, the managed server could be configured to be an ICMB Management Point⁵ 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

⁴ In the control panel you can specify that the EIF service is automatically started each time you start the system.

⁵ 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.

devices. The amount of FRU information available depends on the type of ICMB device to be managed.

In order to use the ICMB feature, one server must be chosen to be a Management Point Server. The EIF service must be started on that system⁶. For information on how to set up for the ICMB feature, refer to the *Intel® Server Management User's Guide*.

14.2.1 Discovering Remote ICMB Systems

Before using the ICMB feature to view connected servers, the Management Point Server must be configured and it must discover 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.

⁶ 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.

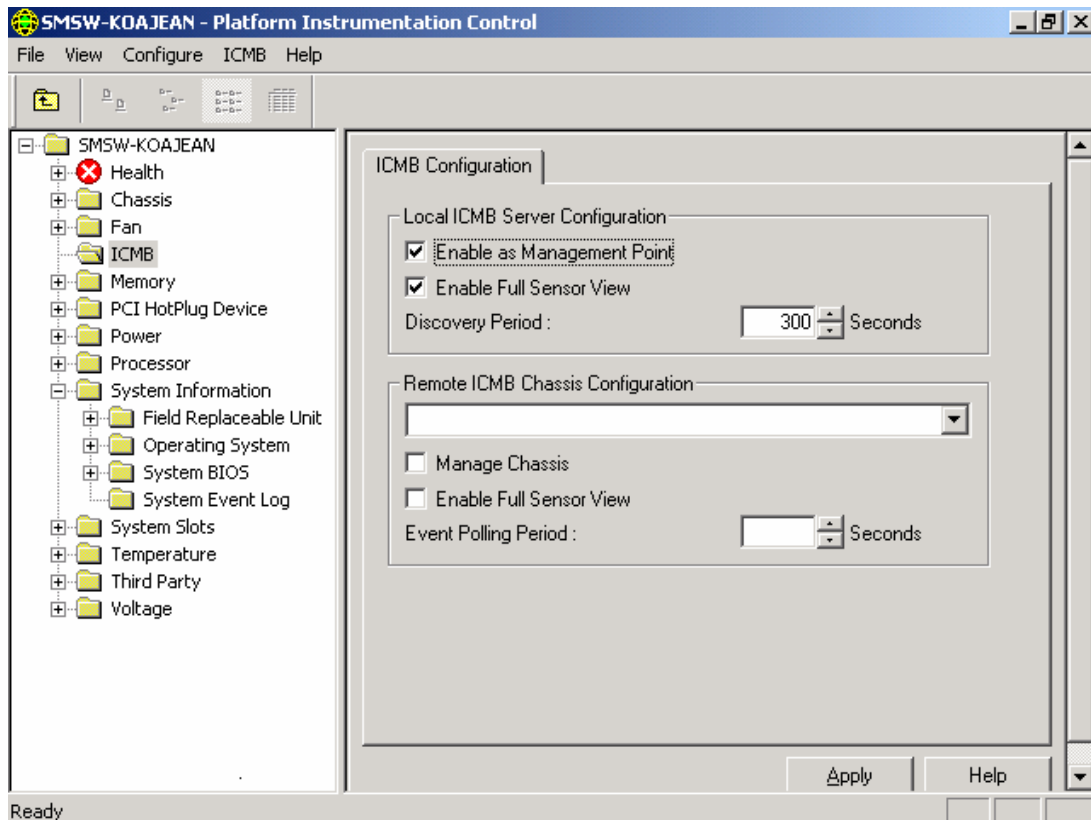


Figure 12. Enabling ICMB Features

14.2.2 Viewing and Managing Viewing Remote ICMB Systems

Once the discovery⁷ process is complete the ICMB folder can be expanded as shown in the navigation pane when connected to the Management Point Server. Every remote ICMB system appears beneath the folder.

The user 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 to be viewed.

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 and the System Event Log.

⁷ Each time you add or remove a remote ICMB chassis from your network, you must update the ICMB configuration by rediscovering existing ICMB systems.

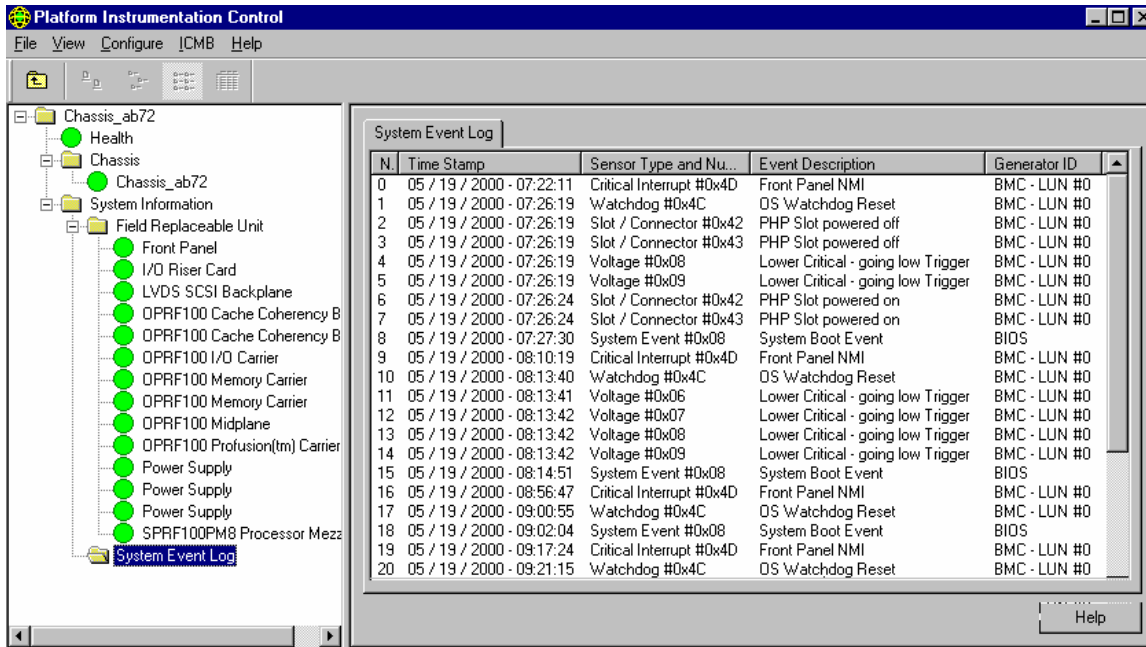


Figure 13. Displaying Remote Server Information

Viewing information about a remote ICMB system does not cause the client to lose connection to the Management Point Server. The user can change the view back to the Management Point Server or to any other ICMB-managed device at any time.

The user 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 used 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.

15. Command Line Interface / Serial Over Lan

15.1 Serial Over LAN

The Serial Over LAN (SOL) feature enables suitably designed servers to transparently redirect the serial character stream of a baseboard UART to/from a remote client via the LAN.

The BMC is responsible for controlling the serial hardware MUX, the transformation of serial data to and from network packets, and the transmission and reception of SOL network packets through the NIC TCO port.

A remote SOL client is responsible for initiating the SOL session with the BMC and transformation of console input and output to and from network packets.

Note: SOL is not supported on the Server Board SE7210TP1-E.

15.2 Command Line Interface

A Command Line Interface (CLI) is an integral part of the architecture. The CLI provides the interface to the SOL service as well as an interface for platform control. The user gains access to the CLI from an operating system command line shell, such as Window's CMD or a Unix shell such as csh or ksh, or from a Telnet style programs that can connect to a socket of type SOCK_STREAM.

The CLI platform control interface provides functionality similar to the DPC console. Platform control commands are accomplished by interpreting command strings within the network proxy, translating them to standard IPMI-Over-LAN frames, and sending them to the BMC in the same fashion as the DPC console.

In addition to platform control, the CLI proxy provides the interface to the SOL character stream. The SOL and IPMI platform control interfaces use different IPMI sessions. For this reason, the CLI interface is modal and under the control of the user. When in platform control mode, the CLI will display a unique prompt allowing the user to know it is in platform control mode. When in the SOL mode, the CLI does not display a prompt and all information displayed comes directly from the SOL character stream.

15.3 SOL/CLI Client Architecture

To allow access from telnet style programs, primary SOL/CLI services are implemented as a background network task. Throughout this document, this task will be referred to as the *network proxy*. The network proxy can run on individual management workstations or may be a centralized service that can be used by any management workstation.

A thin veneer program provides the command shell interface to the proxy. This program connects the network proxy to console stdin and stdout for scripting purpose. Throughout this document, this program will be referred to a *dpccli*. The dpccli program must be run from the command shell of the management workstation.

The diagram below shows all major architectural client-side components and their relationship to each other. The two boxes at the top indicate components of the architecture that are supplied by the host operating system. The gray boxes comprise the components developed to complete the architecture and are the subject of this document.

There are two basic ways to issue CLI commands through the network proxy to a remote server: by using CLI's console interface, called dpccli; or by using telnet. Windows Hyperterminal is not supported.

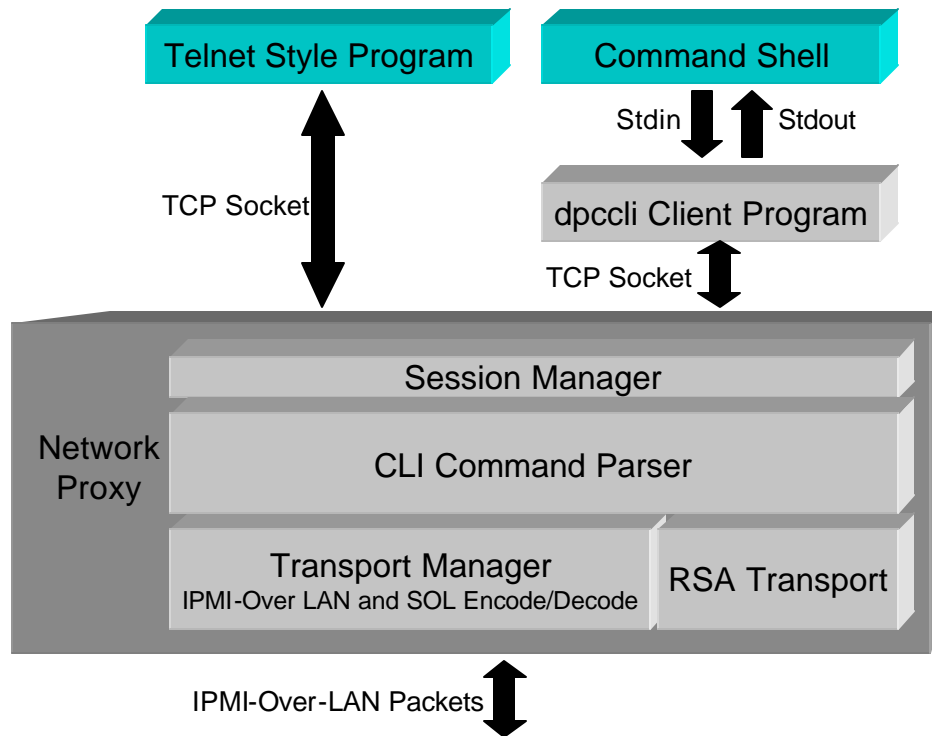


Figure 14. CLI Interface Flowchart

15.3.1 Dpccli Client Program

The dpccli client program provides an interface between the network proxy and a management workstation's console stdin and stdout. This interface is suitable for running dpccli from a command line shell or in conjunction with scripting languages.

To facilitate non-interactive operation, dpccli can take several command line arguments. These include IPMI session establishment parameters and sources for input character streams. Section 15.4 describes in detail the syntax of the dpccli program.

15.3.2 Network Proxy

The Network Proxy is a background service that implements most aspects of the architecture. Because all of its interfaces are socket based, it may be run anywhere in the enterprise and may be used by multiple management workstations. Security is provided through IPMI session authentication with the BMC.

The network proxy stack consists of a Session Manager, a CLI Command Parser, a Transport Manager, and a Remote Service Agent (RSA) Transport. The following sections provide a description of network proxy stack.

15.3.2.1 Session Manager

The Session Manager is responsible for accepting connection requests from network proxy users (Telnet, HyperTerminal, dpccli, etc.). Upon receiving a connection request, the Session Manager will spawn a thread of execution that will manage this network proxy/client association for the lifetime of the session. This mechanism allows the network proxy to support multiple simultaneous sessions and to be deployed as a centralized service.

To provide maximum portability, the session manager uses standard Berkley* socket interfaces. It listens and accepts SOCK_STREAM connections to port 623. If the administrator chooses not to deploy the network proxy as a centralized gateway service, it can be configured to accept connections only from the local host (127.0.0.1).

Since this is not a parameterized interface, the Session Manager will prompt the user for all IPMI session establishment parameters. With the exception of the password, all parameter and command input will be echoed back through the socket. An asterisk will be echoed back for all password characters entered. If the target server rejects the authentication information, the user will be re-prompted all three pieces of information again. On the third failed attempt, the session will be dropped and the connection to the network proxy client will be closed.

An individual session will terminate when the user closes the client-side socket or using the CLI commands *quit* or *exit*.

15.3.2.2 CLI Command Parser

All user input flows through the CLI Command Parser. The CLI supports two modes of operation that are selectable by the user. The first (and default) mode is platform control. The second is the SOL mode. While in the platform control mode, an input prompt will be displayed to indicate as much. In SOL mode, the CLI Command Parser does not display a prompt.

The platform control mode is responsible for interpreting platform control commands read from the client, transforming them to the appropriate IPMI command, and sending them through the Transport Manager component.

By issuing a CLI command, the user can direct the parser to switch to the SOL mode. In this mode, it will send and receive data as a SOL character stream. At this point, the parser does not echo back typed characters and does not interpret input characters as commands except for the escape sequence that indicates that the user wants to return control back to the CLI command parser.

Since the SOL session is initiated and maintained throughout the CLI session, the parser can buffer SOL output while in command parsing mode. This buffered output will be displayed when the parser switches from command mode to the SOL console mode.

Refer to Section 15.6 for a description of the CLI command vocabulary.

15.3.2.3 Transport Manager

The Transport Manager is responsible for establishing all IPMI sessions with the BMC and for best attempt delivery of IPMI commands and SOL data. It uses the same service interface as the Windows DPC Transport Manager and supports servers running IPMI version 1.0 or 1.5.

15.4 Dpccli Command Line Syntax

The console interface for dpccli is particularly useful in a scripting environment that uses standard console input and output. It is also useful as a simple interactive interface when formatted output (i.e. VT100, VT-UTF8, etc.) is not required.

To support non-interactive use, dpccli accepts command line options to control its behavior. Options can be specified in any order. The first text encountered not associated with a command line option is interpreted as text to be sent to the network proxy and therefore must be placed last on the command line. White space between the option flag and its associated argument is optional. The dpccli command line syntax is as follows:

```
dpccli [-?|-h][-s Server] [-u user] [-p password] [-i inputFile] [-o outputFile] [-c]
[-I] [-v] [-P networkProxy] [-a alternatePort][-r rcFile][text]...
```

where:

- ? |h These are the help options. They will display a usage message and exit. If either of these options are specified, all other options and input text are ignored.
- s This option takes the IP or DNS hostname associated with the NIC used by the BMC. If not specified on the command line, the user will be prompted for the information.
- u This option takes the IPMI username to be associated with this session. If not specified on the command line, the user will be prompted for the information.
- p This option takes the IPMI password associated with the username of the session. If not specified on the command line, the user will be prompted for the information.
- P This options takes the IP or DNS hostname of the system running the network proxy this client should contact for service. The default IP address is the local host (127.0.0.1).
- i This optional flag takes a file name to be read as standard input. When the end of file is reached, the session will be terminated unless the continue flag (-I) has been specified. If this option is not specified, input will be read from the command line and/or console stdin.
- o This optional flag takes a file name to be written to as standard output. If this option is not specified, all output will be written to console stdout.
- c This optional flag will force the BMC session into console/SOL Mode. If not specified, platform control mode is assumed. This is not supported when managing the Server Board SE7210TP1-E.

- I This optional flag indicates that the session will continue in the interactive mode after processing all characters read from an input file and/or from the command line. This is the default mode if an input file and/or text was not specified on the command line.
 - v This optional flag will place the session in verbose mode. In this mode, session progress messages will be sent to standard error. In addition, any non-zero exit condition will print an associated error message. This is also the default when the session is in an interactive mode.
 - a This option allows the users to specify an alternate network proxy port number. The default port number is 623.
 - r This option specifies an alternate dpccli RC file. By default, dpccli will first look for a file named *.dpcclirc* in the directory specified by the environment variable HOME and then in the current working directory. This option specifies the path including filename which can be different than *.dpcclirc*.
- text If any text is specified after command line options, it will be treated as input data for the CLI session. Once all text has been processed, the session will be terminated unless the interactive flag (-I) has been specified. White space separated arguments are treated as a single line of input. If white space characters are to be included in the input, they must be enclosed in double quotes. If no text is specified on the command line, the session will default to an interactive mode.

When dpccli exits, it returns a status code to the environment. Non-zero values indicate an error condition was encountered. Each scripting language has its own method for obtaining executable return values. For Windows and Unix batch scripts, this is %errorlevel% and \$? respectively.

15.5 .dpcclirc File Format

In some situations common command line options will be frequently used. An example might be the network address of a centralized network proxy (-P). So the user does not need to enter this information on each invocation of dpccli, the program can utilize a configuration file that is read at each time dpccli is started. By default, dpccli will look for a file with the name *.dpcclirc* first in the directory specified in the HOME environment variable and then in the current working directory. The file and its path can be explicitly specified on the command line using the -r option.

Options specified on the command line always take precedence over options specified in the configuration file. Not all options are supported from *.dpcclirc*. The supported options are a, c, I, v, i, o, p, P, s, and u.

Only the options listed above are interpreted. Command text will not be processed through this file. Any option not understood or supported is silently ignored. This allows blank lines or comments that start with a non-option letter (i.e. #) to be placed in the file. The syntax of the file is one option per line. The line must start with the option letter (optionally preceded by a hyphen), and the option argument if it applies. The following example sets the name of the network proxy and its alternate port address:

```
-P kalama1  
-a 3033
```

15.6 CLI Command Vocabulary

When a network proxy user first connects, s/he is prompted for the target server name or IP address and IPMI session authentication information. After establishing the IPMI session with the target BMC, the CLI command line parser will be in an interactive platform control mode. In this mode, the parser reads a line of user input and interprets it as a command from its platform control vocabulary. This section outlines the CLI command vocabulary.

The command line parser will recognize any portion of the command string that is unique. In other words, `diag` may be used in place of the full command name `diagint`.

15.7 Alarm -s

This command is available only on servers configured specifically with hardware for telephone company (telco) alarm capabilities.

Note: This command is not supported when managing the Server Board SE7210TP1-E. Issuing this command causes the following message to be returned: “error COMMAND IS INVALID”.

15.8 console [-f]

The `console` command will transition the CLI parser from command mode to SOL mode. In this mode, the character stream is passed unaltered through the SOL protocol allowing the user to interact directly with the console serial port of the server. Any SOL output data that was received and buffered when CLI was in the command mode will be displayed at this time. The `-f` option will cause any buffered data to be flushed before switching to SOL mode.

The user may switch from console mode to CLI command mode by typing the escape sequence tilde followed by a period (~.) To escape the tilde and have it sent to the console, a second tilde should be typed.

Note: This command is not supported when managing the Server Board SE7210TP1-E.

15.9 exit and quit

The user can terminate the CLI session using the `exit` or `quit` command. This command will close all IPMI sessions associated with a network proxy user as well as closing the network proxy socket.

15.10 id

The `id` command displays the 16-byte system GUID of the managed server in the conventional GUID format. For example:

```
422e7704-23f5-4706-a943-a7859c073aed
```

15.11 network [mac | ip | subnet | gateway]

The *network* command displays the network configuration of the BMC. This includes the MAC address, IP address and source (static, DHCP, BIOS, other), subnet mask, and gateway IP address. Without arguments, all network information is displayed. Optionally, the user can specify which network configuration information is of interest.

15.12 Power -s

Displays the current power state of the managed server.

15.13 power on [-c]

The *power on* command will initiate a power up sequence on the managed server. The `-c` option will cause the session to switch to console/SOL mode after successfully executing the IPMI power-on command.

Note: The `-c` option is not supported when managing Server Board SE7210TP1-E platforms.

15.14 power off [-f]

The *power off* command will initiate a power down sequence on the managed server. By default, a power off command will attempt a graceful shutdown the operating system before executing the IPMI power-off command. The `-f` option will force a power off without performing a graceful shutdown. A graceful shutdown requires Intel Platform Instrumentation to be installed on the server.

Note: The Server Board SE7210TP1-E does not support a graceful shutdown of the operating system.

15.15 reset [-f] [-c]

The *reset* command will perform a platform reset. By default, a reset command will attempt a gracefully shutdown the operating system before executing the IPMI reset command. The `-f` option will force a reset without performing a graceful shutdown. The `-c` option will cause the session to switch to console/SOL mode after successfully executing the IPMI reset command. A graceful shutdown requires Intel Platform Instrumentation to be installed on the server.

Note: The `-c` option is not supported when managing Server Board SE7210TP1-E platforms.

15.16 sel [-c] [-num]

The *sel* command displays System Event Log records. Each record is displayed on a single line. The `-c` option will display the record in a Comma Separated Value (CSV) format where a single comma will separate each field. The `-num` option displays the most recent *num* number of events. If `-num` is not specified, all SEL records will be displayed

The general format is as follows:

Record # | Date Time | Sensor | Event description

The following are examples of both format types:

```
23 | 08/23/01 | 13:22:01 | Fan #01 | Lower Critical - going low
24 | 08/25/01 | 06:13:41 | System Event | System Boot Event
```

```
23,08/23/01,13:22:01,Fan #01,Lower Critical - going low
24,08/25/01,06:13:41,System Event,System Boot Event
```

Time and date formats are appropriate for the local where the network proxy is run.

15.17 sensors [-v] [-c] [-f ok|nc|cr|nr|us] [volt|temp|power|fan]

The *sensors* command displays the current status of platform sensors. The `-v` option will display sensor values if they are available. The display can be limited to specific sensor groups by listing them as arguments to the command. The `-c` option will display the record in a Comma Separated Value (CSV) format where a single comma will separate each field.

The general display format is as follows:

Date | Time | Sensor Type | Sensor # | Status [| Value | Units]

The following are examples of both format types using the `-v` option:

```
09/13/01 | 10:08:55 | Voltage | #02 | ok | 5.2 | Volts
09/13/01 | 10:08:55 | Temperature | #12 | critical | 102 | Degrees Celsius
```

```
09/13/01,10:08:55,Voltage,#02,ok,5.2,Volts
09/13/01,10:08:55,Temperature,#12,critical,102,Degrees Celsius
```

The `-f` option allows for filtering the display of events based on status where:

- ok = Operating in normal ranges.
- nc = Non-critical – Warning condition where sensor is outside of normal ranges
- cr = Critical – Potentially fatal condition where sensor is exceeding specified ratings
- nr = Non-recoverable – Potential damage
- us = Unspecified status – Fault detected but severity unspecified

The filter condition is treated as a threshold. That is, if the filter was set for `cr`, all sensors that have a status of `cr`, `nr`, or `us` will be displayed.

15.18 diagint [-c]

The *diagint* command will cause BMC to generate an IPMI diagnostic interrupt. The `-c` option will cause the session to switch to console/SOL mode after successfully executing the IPMI diagnostic interrupt command. The `-c` option can only be used over a telnet session.

Note: The `-c` option is not supported when managing Server Board SE7210TP1-E platforms.

15.19 boot [-f] [-c] (normal | service)

The *boot* command sets the IPMI boot options and resets the system. By default, a boot command will attempt a graceful shutdown the operating system before executing the IPMI reset command. The *-f* option will force a boot without a graceful shutdown.

Note: The Server Board SE7210TP1-E does not support a graceful shutdown of the operating system.

The *-c* option will cause the session to switch to console/SOL mode after successfully executing the IPMI reset command. If the *service* boot mode is used with *-c*, the command parser will attempt to open a connection with the Remote Service Agent (RSA) running on the Service Partition instead of establishing a SOL session.

Notes:

- The *-c* option can only be used over a telnet session to the remote server.
- The *-c* option is not supported when managing Server Board SE7210TP1-E platforms.

15.20 service (console | exit | ftp (start | stop))

This command is not supported on the Server Board SE7210TP1-E. The *service* command allows the user to interact with the Remote Service Agent (RSA) running from the Service Partition. When *console* is specified, the RSA is instructed to start and redirect a DOS command window through the CLI parser. The character stream is passed unaltered to and from the RSA. The user may switch from RSA console mode to CLI command mode by typing the escape sequence tilde followed by a period (~.) To escape the tilde and have it sent to the console, a second tilde should be typed. This does not break the RSA DOS console connection, which can be reestablished by issuing the *service console* command again.

Notes:

- This command can only be used over a telnet session to the remote server.
- This command is not supported when managing Server Board SE7210TP1-E platforms.

When *exit* is specified, the CLI Parser will close the RSA connection and return to the platform control mode.

The *ftp start/stop* command instructs the RSA to start or stop the FTP server. Once the FTP server has been started by the RSA, standard operating system FTP clients can be used to directly transfer files to and from the Service Partition. An FTP client is not built into the CLI command parser. The FTP server cannot be started while an RSA console session is active. Attempting to do so will generate an error message from the CLI parser.

15.21 set (prompt=*text* | prefix=*text*)

The *set* command allows the user to define the CLI command mode *prompt* and the *prefix* to be applied to CLI command responses. The default prompt is `dpccli>` while the default prefix is an empty string. The prompt and prefix strings can be comprised of any literal text and three system variables. The system variables are `$system`, `$time`, `$date`. The *system* variable is set

to the hostname or IP address of the managed server. The *time* and *date* variables will reflect the current time and date for the system hosting the network proxy in a format appropriate for the local of the hosting system.

15.22 Identify [-on [# of seconds]] [-off]

The *identify* command causes the server to signal its location (e.g. with a blinking led, or beep). This is intended to locate the server amongst a rack of servers. If no parameters are specified, or just '-on' is specified, the server will identify itself for 15 seconds. When '-off' is specified, the server will stop identifying itself (this has no effect if the server is not identifying itself). Example: `identify -on 50`.

Note: This command is not supported when managing Server Board SE7210TP1-E platforms.

15.23 version

The *version* command will display the version of the active dpcproxy.

15.24 help [CLI command]

The *help* command will display usage messages for the *CLI command* specified. If a CLI command is not specified, this command will list all possible CLI commands.

15.25 Network Proxy Command Line Syntax

The network proxy can be started with several command line options to control its runtime behavior. Options can be specified in any order. White space between the option flag and its associated argument is optional. The network proxy can be started with the following command line arguments:

```
dpcproxy [install*] [uninstall*] [-?|h] [-f] [-p Port] [-L] [-l Language] [-d
LogFileDirectory] -u
```

where:

- ? | h These are the help options. They will display a usage message and exit. If either of these options are specified, all other options and input text are ignored.
- install This option will install the proxy as a Windows service, and is thus only needed on windows. Specify the parameters to use each time the dpcproxy is started as additional parameters following "-install". The service must be started after it is installed. Once it is installed the service will be started up automatically every time the system starts up.
- uninstall Removes dpcproxy from the Windows service control manager database, so that dpcproxy is no longer an installed service. The service must be stopped for this command to execute properly.
- f This option will cause the network proxy to run in the foreground. In a Linux environment the proxy will run as a background daemon by default. Under the Windows operating

system the proxy cannot be started from the command line without this switch, the -install and -uninstall switches must be used for background operation.

- p This option takes a port number and sets an alternate port for the network proxy to listen to for incoming client connections. By default, the network proxy listens on port 623, which is a privileged port in most operating systems.
- L This options cause the network proxy to accept connections only from the local host address 127.0.0.1. This option will prevent this instance of the network proxy from proving services to systems other than the local system.
- l This options takes a language specification to use for localization of messages and dates sent to a network proxy client. If this option is not specified, the network proxy will use the language specified in the LANG environment variable. If a language is not specified on the command line or through the LANG environment variable, the network proxy will default to the locale en_US.
- d This options takes a directory path that will be prepended to all debug log files generated by the network proxy. If this option is not set, debug log information will not be kept.
- u This option turns off Serial-Over-LAN (SOL) data encrypted. All SOL data is sent unencrypted.

Note: The SOL feature is not supported when managing a Server Board SE7210TP1-E platform.

In a Linux environment, these options are specified on the command line that starts the network proxy. In a Microsoft operating system environment, these options can be specified on the command line only when running in foreground mode (i.e. -f). When the network proxy is running as a Windows service, these command line options can be passed as additional parameters following the install parameter.

Under the Windows operating system background operation is provided solely through the -install switch. Invoking dpcproxy with this switch will install the dpcproxy service within the service control manager. The dpcproxy service can subsequently be started and stopped using 'net start' and 'net stop' or the service control panel and finally uninstalled using 'dpcproxy -uninstall'. When executing dpcproxy from a Windows command prompt one of -f, -install, or -uninstall must be specified for supported operation.

* install and uninstall are only needed for the Windows proxy.

15.26 Operation Environment

The network proxy and dpccli will support the following operating system environments:

- Windows 2000 and Windows server 2003 for all workstation and server configurations
- RedHat Linux 7.2 and 7.3 for all workstation and server configurations

Both the network proxy and dpccli will run in the minimum memory and disk configuration defined by the operating system supplier.

15.27 Installation

Manual installation can be performed as indicated in the following sections.

15.27.1 **dpccli**

The *dpccli* program is installed as a single executable and may be run from any directory. No special privileges are required.

15.27.2 **dpcproxy**

The network proxy, *dpcproxy*, is installed as a single executable and may be run from any directory. The default client port of 623 is a privileged port. Unless it is changed through the command line `-p` option, it will require root/administrative privileges to start.

16. Native Command Line

16.1 Native Command Line Overview

Native command line is a feature that allows the user to directly send text-based commands to the server's Baseboard Management Controller (BMC) using a serial port connection. The connection requires the use of a "Null Modem" cable connected to Serial B (Emergency Management Port). Terminal mode supports standard binary IPMI 1.5 hex-ASCII commands and specific text commands. In terminal mode the user can:

- Power the server on or off
- Reset the server
- Retrieve the server's health status
- View and configure the server boot options
- View and configure the BMC's terminal mode configuration
- Execute any platform-supported binary command specified in the Intelligent Platform Management Interface (IPMI) v1.5 specification using the hex-ASCII format

See the ISM Installation and User Guide on the ISM CD for a full description of commands.

Note: The Native Command Line feature is not supported when managing the Server Board SE7210TP1-E platform.

17. Standalone SNMP Subagent Introduction

17.1 SNMP Subagent Description

Intel® Server Baseboard Simple Network Management Protocol (SNMP) subagent is an SNMP extension agent. It provides the interface and a database for retrieving server information and monitoring server health status on the network.

Note: The SNMP Stand Alone Subagent is only supported on the Server Board SE7210TP1-E.

The Management Information Base (MIB) file that accompanies the SNMP subagent contains the definitions of the management information the SNMP subagent can access. Each one is distinguished by a unique object identifier (OID). The SNMP subagent supports SNMP based access (GETs, SETs and TRAPs) to the instrumented components on the managed server, collecting and returning information as requested by a management system. It plugs into the SNMP master agent infrastructure supported by the operating system and responds to queries and sets filtered to it by the master agent based on the OID specifying the data defined in the MIB to be retrieved or set.

There are two sources of information for the SNMP subagent on the server. The SNMP subagent communicates with the mini Baseboard Management Controller (mBMC) using an Intelligent Platform Management Interface (IPMI) driver. Through the IPMI driver the SNMP subagent has access to information such as power supplies, voltages, temperature sensors, cooling devices, chassis intrusion sensors, and the System Event Log (SEL). The SNMP subagent also has access to information on processors and memory that are stored in the System Management BIOS (SMBIOS) tables.

For Microsoft Windows based systems, the SNMP subagent is implemented as a Dynamic Linking Library (DLL) and is configured in the Registration Database. When the SNMP master agent (Snmp.dll) is started, it queries the registry. Then it loads and initializes the DLL for the registered SNMP subagent. The SNMP master agent invokes DLL entry points to request MIB queries and sets, and obtains events generated by the subagent. The implementation of the SNMP subagent for Microsoft Windows uses an SMBIOS Access Layer to access the SMBIOS tables.

For Linux systems, the SNMP subagent is implemented as an rpm package. It is installed, configured and started as a service. The SNMP master agent (NET-SNMP) communicates with the subagent through AgentX* protocol. The implementation of the SNMP subagent for Linux uses an SMBIOS Access Layer to access the SMBIOS tables.

17.2 General Architecture

The SNMP master agent must be installed and configured before installing the SNMP subagent. Figure 1 describes how the SNMP subagent interfaces with the SNMP master agent and the mBMC on the platform.

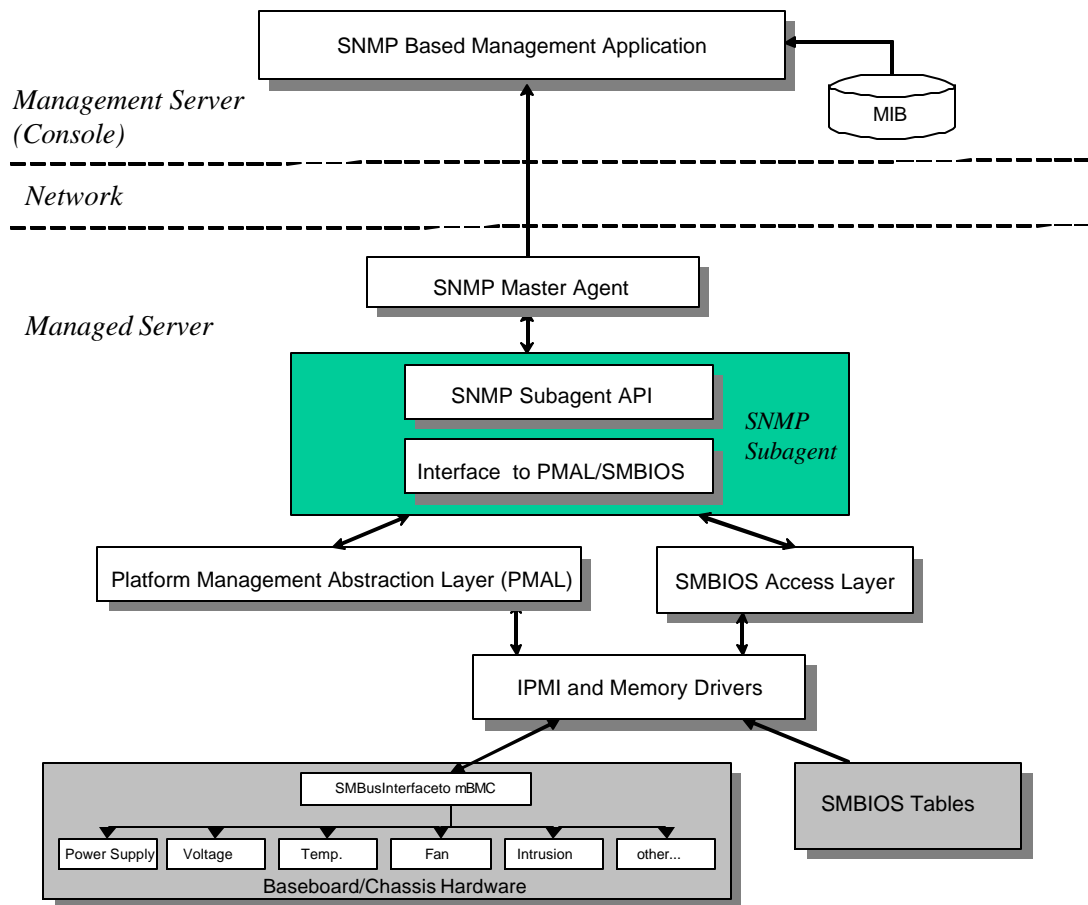


Figure 15. SNMP Agent Architecture

All SNMP traffic coming over the network to the managed server is received by the SNMP master agent. When the SNMP subagent initializes, it notifies the master agent of the OID values that the subagent's responsibilities. These OID values correspond to the data provided in the MIB. The SNMP-based Management Console uses the MIB to determine the OID values for particular attributes, and whether or not the attribute may be modified through an SNMP SET. Both requests to retrieve data (SNMP GET) and requests to modify data (SNMP SET) identify the attribute of interest by OID.

The master agent routes SNMP requests to the appropriate subagent, based on the supported OIDs. The SNMP request contains information about the originator of the request. The subagent processes the request, and sends the information back to the SNMP master agent. The master agent then sends the information to the SNMP-based Management Console.

In addition to responding to SNMP GET and SNMP SET requests, the SNMP subagent generates TRAPs. While one component of the SNMP subagent is waiting for SNMP requests from the SNMP master agent, another component of the subagent monitors the System Event

Log (SEL). When a new SEL entry is detected, the SNMP subagent analyzes the SEL entry and sends an SNMP TRAP to the SNMP master agent.

The SNMP master agent duplicates and transmits the SNMP TRAP to all nodes that are configured to receive traps from the managed server. The trap recipients are configured during the installation and configuration of the SNMP master agent.

The SNMP subagent uses a Platform Management Abstraction Layer (PMAL) and the IPMI driver to access the information from the mBMC. The following information may be accessed: power supplies, voltages, temperature sensors, cooling devices, chassis intrusion sensors and the SEL. The information regarding processors and memory is stored in the SMBIOS tables, and is accessed through direct memory mapping.

18. Install/Uninstall

The SNMP master agent must be installed and configured on the managed server according to the operating system directions before installing the SNMP subagent. It is important that the community name string and trap destinations are configured correctly. Once the SNMP subagent is installed, the MIB file must be copied to any SNMP Management Applications requiring the supported OID and attribute information. Operating-specific installation and configuration information follows.

18.1 Preparing for Installation

18.1.1 Linux Systems

18.1.1.1 Master Agent

The SNMP subagent works with NET-SNMP Version 5.

18.1.1.2 Master Agent Configuration File

Since the SNMP subagent is designed to use the AgentX protocol to communicate with NET-SNMP master agent on Linux, the configuration file `/etc/snmp/snmpd.conf` for `snmpd` needs to have the following lines in it (the first line is a comment line). The master agent must be restarted in order for any configuration file changes to take effect.

```
# This line allows SNMP remote access to the subagent
rmcommunity <communityname>

# This line turns on agentx master agent support
master agentx

# This line enables V2 trap sending
trap2sink localhost <communityname>
```

18.1.1.3 MIB File Location

The MIB file (`basebrd5.mib`) is located in `/usr/share/snmp/mibs`.

18.1.2 Windows Systems

18.1.2.1 Master Agent

For Microsoft Windows-based systems, the SNMP service is available on the operating system installation CD and must be installed. It is not included in the operating system installation by default, but can be added after the initial operating system installation completes.

18.1.2.2 MIB File Location

The MIB file (basebrd5.mib) is located in the same location the SNMP subagent is installed. The default installation directory is C:\Program Files\intel\ServerManagementSNMP. The MIB file is not required by the SNMP subagent or execution, but is required for management applications that issue SNMP GET and SET commands based on the MIB.

18.2 Install Framework

The SNMP subagent and MIB file are installed using the Intel Server Management (ISM) installation framework. The SNMP subagent is presented as a feature set under the custom install option. The SNMP subagent does not require other ISM components to be installed on the managed server. However, it coexists with the ISM software stack if the stack is installed on the managed server. The ISM installation framework supports a local installation of software, and installs software to one or more remote systems.

When the install programs runs, the installation screen provides the user with three installation options. This install option screen advises the user that the Custom Install options must be used to install the SNMP subagent on the managed server. The user will be presented with the three installation options:

- **Local install:** This option installs ISM on the local system. The user cannot select individual ISM components or additional systems. The SNMP subagent will be not installed when this option is selected.
- **Multiple system install:** This option allows the user to install ISM to selected target systems. The user will not be presented with a screen to select individual ISM components, but the user can choose the local machine as one of the selected systems to receive the software. The SNMP subagent will not be installed when this option is selected.
- **Custom install:** With this option, the user can select a feature set and the target system where ISM will be installed. The feature set is:
 - **Platform Instrumentation Control (PIC):** supported on Windows 2000 and Windows XP professional. If selected, this feature will also install *Intel Server Management StandAlone Console*.
 - **Direct Platform Control (DPC):** supported on Windows 2000 and Windows XP professional. If selected this feature will also install *Intel Server Management StandAlone Console*.
 - **One-Boot Flash Update Utility(OFU):** supported on Windows 2000 and Windows XP professional.
 - **Client SSU Control:** Supported on Windows 2000 and Windows XP professional.
 - **DMI Browser:** supported on Windows 2000 and Windows XP professional. If selected this feature will also install *Intel Server Management StandAlone Console*.
 - **Platform Instrumentation:** supported on Windows 2000, Windows.Net, NetWare 6.x, UnixWare 7.x. Installing this feature will also install the DMI Service Layer.

- **HP OV integration agent:** only installed if the *HP OV* console is present on the selected systems. If this feature is installed, all ISM console tools (PIC, DPC, Client SSU or DMI Browser) will be integrated into the *HP OV* console.
- **CA Tng Unicenter integration agent:** only installed if the *CA Tng Unicenter* console is present on the selected systems. If this feature is installed, all ISM console tools (PIC, DPC, Client SSU or DMI Browser) will be integrated into the *CA Tng Unicenter* console.
- **LanAlert Viewer:** This feature will monitor the SNMP traps from a server, i.e. any supported sensor status change. Supported on Windows 2000 and Windows XP.
- **Command Line Interface (CLI):** this feature provides the interface to the Serial Over LAN service as well as an interface for platform control. This feature is only available in ISM 5.1 for SE7500WV2 platforms. Serial Over LAN service is not supported by mBMC based servers.
- **SNMP Subagent Set:** supported on Windows 2000.

The process to install the SNMP subagent is independent of the process of installing ISM components. When the SNMP agent is selected, all components required for the SNMP subagent to run are installed. This includes the IPMI driver and PMAL library, regardless of whether the ISM software stack is installed. For detailed information on ISM installation framework, refer to the installation guide for ISM 5.x.

18.2.1 Window-based Install

The SNMP subagent implemented for Windows shares the same IPMI driver as the ISM software stack. Therefore, the install program loads the IPMI driver if ISM software stack has not been installed. The install program ensures only one copy of the IPMI driver is installed, even if the ISM software stack and the SNMP subagent are both installed on the system. The install program is responsible for registering the SNMP subagent to the SNMP master agent.

18.2.2 Install for Linux System

The SNMP subagent implemented for Linux shares the same IPMI driver as the ISM DMI software stack. The install program installs the IPMI driver even if the ISM software stack has not been installed. The install program ensures only one copy of the IPMI driver is installed, even if the ISM software stack and the SNMP subagent are both installed on the system. The install program loads the SNMP subagent rpm, runs the configuration scripts, and starts the SNMP subagent as a service.

18.3 Uninstall

For Windows systems, uninstall does not allow a selective uninstall of a feature within a component. Launching the uninstall process removes all the installed ISM components as well as the SNMP subagent. It stops the service, performs un-register for the DLL and service, and removes the files and folders.

For Linux systems, the `rpm -e` command must be executed to uninstall ISM or the subagent.

- `rpm -e ism` uninstalls ISM

- `rpm -e ipmidrvr` uninstalls the driver
- `rpm -e snmpsa` uninstalls the SNMP Subagent.

19. Functionalities

Through basic SNMP GETs, SETs and TRAPs, the SNMP subagent provides the following functionalities for managing servers:

- Access sensor data
- View and modifying threshold settings
- Read the SMBIOS tables
- Provide overall system health status based on the sensors' readings from monitored hardware components.

19.1 Access Sensor Data

The SNMP subagent provides access to the management information accessible through IPMI commands that the mBMC responds to on the managed server. The SNMP subagent's Management Information Base (MIB) supports the following list of components that the mBMC and BIOS are capable of supporting:

- Voltage
- Temperature
- System Fan
- Memory
- Processor

19.2 View and Modifying Threshold Settings

Some sensors monitored by the mBMC have thresholds, defining normal, non-critical, and critical operating parameters. Many of the sensor thresholds can be modified as desired for the particular environment a server is running in. The SNMP agent's MIB is designed to display all possible thresholds and sensor readings, and makes all modifiable thresholds capable of being changed via the SNMP SET command. The SNMP SET feature for the SNMP agent can be globally turned off. The SNMP sub-agent supports threshold changes to the following sensors:

- Voltage
- Temperature
- System Fan

19.3 System Health Status

The SNMP subagent provides system health status as being “Ok”, “Non-Critical”, or “Critical” based on the health status of the following hardware subsystems:

Sensor	Sensor Health Status	System Health Status
Voltage	Ok	Ok
Temperature	Non-Critical	Non-Critical
Fan	Critical	Critical
Processor	Ok	Ok
	All Errors	Critical
Memory Array	Ok	Ok
Memory Device	Single-bit Error	Non-Critical
	Multiple-bit Error	Critical
Chassis	Chassis Ok	Ok
	General Chassis Intrusion	Critical

Changes to the overall health will be triggered by SEL events, which alert the SNMP subagent that an event has occurred which may impact the current overall health status of the server.

20. MIB Structure

20.1 Version Compatibility

The SNMP subagent works with the SNMPv3 master agent implementations, but it does not support all the new features of SNMPv3. To provide additional security and address CERT* advisories affecting SNMPv1 and some SNMPv2 implementations, the SNMP subagent does not support traps that adhere to the SNMPv3 format. It only supports SNMPv2 traps. The SNMP MIB is SNMPv2C and SNMPv3 compliant, meaning that the MIB compiles and loads in a SNMPv2 or SNMPv3 compliant MIB browser. The SNMP subagent has the capability to be backward compatible with SNMPv1 implementations.

Note: The backward compatibility of the subagent has not been verified.

20.2 Compliancy

The MIB can be loaded into HP OpenView. A known third-party vendor restriction is that HP OpenView restricts the number of characters in the SUMMARY directive entry to no longer than 246 characters.

20.3 MIB Extensions and Changes

The Intel® Baseboard MIB can be extended with new variables once the SNMP agent has been released, but existing variables cannot be removed from the MIB, they should be marked as obsolete or deprecated.

20.4 MIB Definitions

20.4.1 Base OID

The base OID for the MIB must conform to the master MIB maintained within Intel. For this agent, the base OID will be iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) intel(343) products(2) server-management(10) software(3) baseboardGroup5(5).

20.4.2 Event Configuration Settings

The events defined in the MIB have configuration settings embedded as comments. Some enterprise system management consoles, such as HP OpenView, use these settings to configure the events when the MIB is loaded. The use of these embedded configuration settings eliminates the task of configuring the events after loading the MIB.

The format of the configuration settings starts with "--" to indicate it is a comment within the MIB, followed by one of the following special tokens #TYPE, #SEVERITY, #SUMMARY, #ARGUMENTS, #CATEGORY, #STATE, or #STATUS. The following table describes the usage.

Table 11. MIB Event Configuration Usage

Configuration Token	Associated Information	Purpose
#TYPE	Quoted string	Text describing the event
#SEVERITY	One of the following: INFORMATIONAL, MINOR, MAJOR or CRITICAL	Describes the severity level for the trap
#SUMMARY	Quoted string of text and/or variables	Text and/or variables that describe the event.
#ARGUMENTS	Comma delimited integers enclosed in braces. Example: {3, 4}	Lists which arguments in the trap varbind list are to be inserted into the SUMMARY for display by the trap processing program. Counting starts at 0.
#CATEGORY	One of the following: "IGNORE", "LOGONLY", "Error Alarms", "Threshold Alarms", "Status Alarms", "Configuration Alarms" or "Application Alert Alarms"	Enables HPOpenView to automatically set category selection for the traps
#STATE	One for the following: FAILED, DEGRADED, OPERATIONAL	Describes the state of the component the trap is for.
#STATUS	One of the following: MANDATORY, DEPRECATED, OBSOLETE, OPTIONAL	Describes the subagent support for this trap. MANDATORY indicates it is valid. DEPRECATED indicates it is in the transition to OBSOLETE. OBSOLETE indicates the trap is no longer supported. OPTIONAL indicates the trap may or may not be supported.

20.4.3 IPMI Information

Beneath baseboardGroup5, the sensors and other information are organized into groups and tables based on the type of information. The following shows a breakout and grouping of managed system information below baseboardGroup5.

Table 12. Managed System Information Below Baseboard Group 5

Group / Table Name	OID
MODULE-IDENTITY	baseboardGroup5 1
systemManagementSoftwareGroup	baseboardGroup5 100
chassisInformationGroup	baseboardGroup5 200
processorGroup	baseboardGroup5 300
powerGroup	baseboardGroup5 400
powerUnitTable	powerGroup 10
powerSupplyTable	powerGroup 20
voltageProbeTable	powerGroup 30
discreteVoltageProbeTable	powerGroup 40
memoryGroup	baseboardGroup5 500
physicalMemoryArrayTable	memoryGroup 10

physicalMemoryDeviceTable	memoryGroup 20
thermalGroup	baseboardGroup5 600
coolingUnitTable	thermalGroup 10
coolingDeviceTable	thermalGroup 20
discreteCoolingDeviceTable	thermalGroup 30
temperatureProbeTable	thermalGroup 40
baseboard5EventGroup	baseboardGroup5 1000
eventVariables	Baseboard5EventGroup 10
systemManagementSWEvents	Baseboard5EventGroup 20
chassisEvents	Baseboard5EventGroup 30
processorEvents	Baseboard5EventGroup 40
powerEvents (powerUnitRedundancyEvents, powerSupplyEvents, voltageEvents, and discreteVoltageEvents)	Baseboard5EventGroup 50
memoryEvents	Baseboard5EventGroup 60
thermalEvents (coolingUnitEvents, coolingDeviceEvents, discreteCoolingDeviceEvents, and temperatureEvents)	Baseboard5EventGroup 70
slotEvents	Baseboard5EventGroup 80
systemEvents	Baseboard5EventGroup 90

The SNMP agent uses the following predefined attribute types in the MIB.

Table 13. Predefined Attribute Types in the MIB

Predefined Attribute Type	Actual Type	Possible Values
IntelStatus	INTEGER	other(1), unknown (2), ok (3), nonCritical(4), critical(5), nonRecoverable(6)
OneBasedIndex	Integer32	1...2147483647
IntelFeatureStatus	INTEGER	Other(1), unknown(2), disabled(3), enabled(4), notImplemented(5)
IntelRedundancyStatus	INTEGER	Other(1), unknown(2), full(3), degraded(4), lost(5), notRedundant(6), redundancyOffline(7)

21. SNMP Events

21.1 Event Design Methodology

Events are generated by the SNMP agent based on SEL events and provide as much information as possible concerning the event to the event reader. The events use the NOTIFICATION-TYPE construct specified in SNMPv2C.

The SNMP agent is designed to accommodate the full range of possible events, although specific server platforms may not support all of the events. Some server platforms do not support certain features in firmware. For example, some platforms do not support fan redundancy, so there are no events related to the cooling device redundancy being lost, regained or degraded.

Some server platforms do not physically have the sensor or the right sensor types to support a feature. For example, the Server Board SE7210TP1 does not have a Power Redundancy sensor and therefore cannot generate power redundancy events. Additionally not all sensors support full possible range thresholds. Refer to the server platform EPS for details on the features supported by hardware and firmware.

Table 14. SNMP Events

Chassis Events
chassis intrusion detected
chassis intrusion cleared
Voltage Sensor Events (using thresholds)
reading changed to OK
reading changed to lower critical
reading changed to upper critical
reading changed to lower non-critical
reading changed to upper non-critical
reading changed to lower non-recoverable
reading changed to upper non-recoverable
Cooling Device Events (using thresholds)
reading changed to OK
reading changed to lower critical
reading changed to upper critical
reading changed to lower non-critical
reading changed to upper non-critical
reading changed to lower non-recoverable
reading changed to upper non-recoverable
Temperature Sensor Events
reading changed to OK
reading changed to lower critical
reading changed to upper critical
reading changed to lower non-critical

reading changed to upper non-critical
reading changed to lower non-nonrecoverable
reading changed to upper non-nonrecoverable

21.2 Event OID Information

Events OID values are organized in a similar fashion as the IPMI information. The events are divided into the following categories under baseboardGroup 5.

Table 15. OID Event Categories

baseboard5EventGroup	baseboardGroup5 1000
eventVariables	Baseboard5EventGroup 10
systemManagementSWEvents	Baseboard5EventGroup 20
chassisEvents	Baseboard5EventGroup 30
processorEvents	Baseboard5EventGroup 40
powerEvents (powerUnitRedundancyEvents, powerSupplyEvents, voltageEvents and discreteVoltageEvents)	Baseboard5EventGroup 50
memoryEvents	Baseboard5EventGroup 60
thermalEvents (coolingUnitEvents, coolingDeviceEvents, discreteCoolingDeviceEvents, and temperatureEvents)	Baseboard5EventGroup 70
slotEvents	Baseboard5EventGroup 80
systemEvents	Baseboard5EventGroup 90

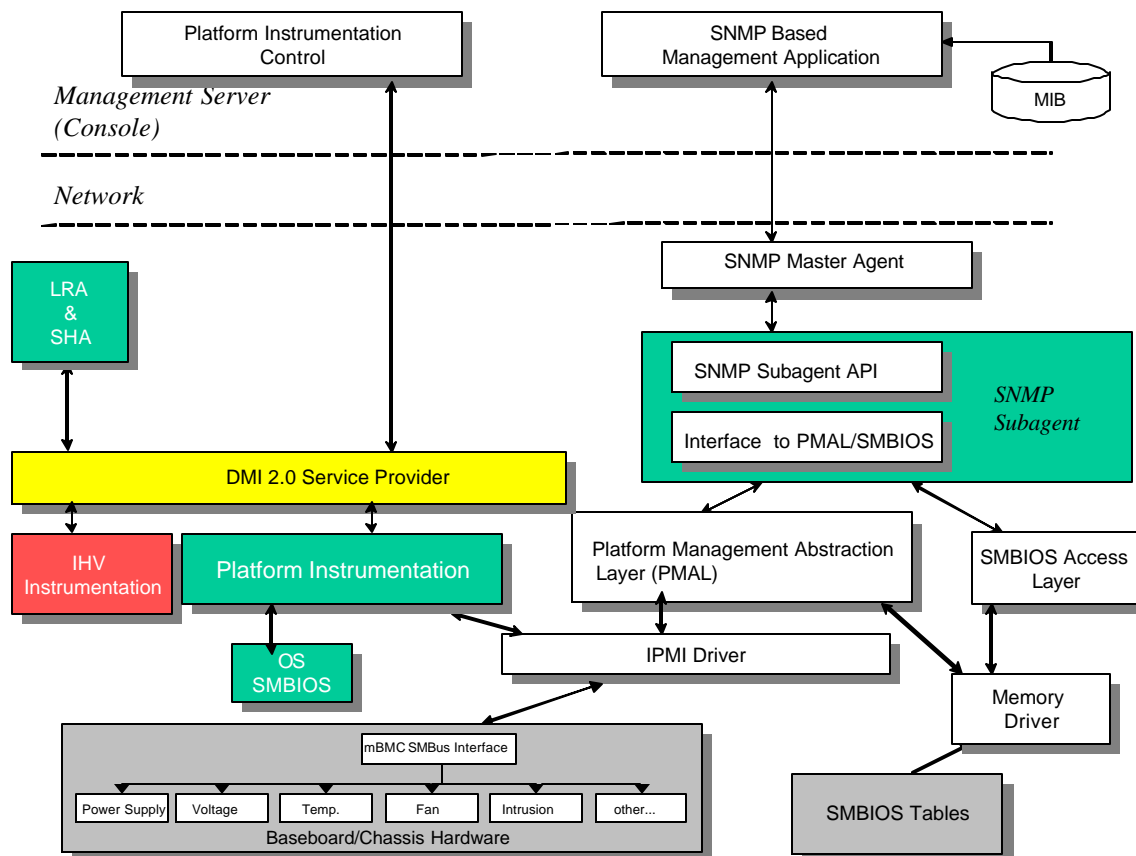
22. Coexistence with ISM DMI Based SMA

Both the SNMP subagent and the DMI based ISM software stack, may be installed and run on the same managed server. A discussion of the installation procedure is included in section 3 of this document.

Whether the SNMP subagent and the DMI based ISM SMA are installed at the same time or separately, the install program will ensure that only one version of any shared files is installed on the server.

For both the Windows and Linux implementations of the SNMP subagent, the same IPMI driver is used for mBMC access. Although the same IPMI driver is used, the data is not guaranteed to be synchronized. If changes are made to threshold settings using the SNMP subagent, the ISM System Management GUI may require a user initiated data refresh in order to display the new threshold values.

It is not guaranteed that the same overall server health will be reported by both the SNMP subagent and the ISM DMIbased SMA.



23. Configurable Settings

Fields for user-defined values are provided to enhance the flexibility for accessing the SNMP data. The SNMP subagent is designed to read the following configurable objects through a configuration file located at `/usr/local/snmpsa/conf/snmpsa.conf` for Linux and at `C:\Program Files\intel\ServerManagementSNMP\snmpsa.conf` for Windows.

The configuration file supports the definition of following fields:

```
PlatformDescription - Text description to specify the type of
system, such as an OEM name. This field is defined in the MIB
file, and can be accessed by OID.
PlatformId - Integer value for identify the platform.
TrapsEnabled - Boolean 0 or 1 to specify whether trap is
enabled.
SetsEnabled - Boolean 0 or 1 to specify whether set is enabled.
Manufacturer - Text description of the manufacturer.
ProductName - Text description of the SNMP subagent product
name.
ProductVersion - Text description of the version of the product.
ProductBuildNumber - Text description of the build number of the
product.
ProductDescription - Text description of the product.
```

Each line in `snmpsa.conf` defines one attribute and has the following syntax:

```
<Attribute Key> = <value>
```

Where the “Attribute Key” can be one of the following words. These are not case-sensitive:

```
PlatformDescription
PlatformId
TrapsEnabled
SetsEnabled
Manufacturer
ProductName
ProductVersion
ProductBuildNumber
ProductDescription
```

The Boolean value can be either 0 for false and 1 for true. A text string value needs to have double quotes (“) on both sides of the string. The maximum string length is 64 characters.

A line lead by a ‘#’ sign is a comment line. A sample file of `snmpsa.conf` is distributed in the release and will be installed at the final location.

Appendix 1: Server Board SHG2 Sensors

Sensor Name	Sensor#	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost	As	–
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy Regain Redundancy Lost	As	–
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As	–
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost
POST Error	06h	System Firmware Progress 0Fh	Sensor Specific 6Fh	POST error	As	–
FP Diag Interrupt (NMI for IA-32, INIT for IA-64)	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI	As	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Correctable ECC Uncorrectable ECC	As	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–
BB +1.5V	0Ah	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +2.5V	0Bh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +3.3V	0Ch	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog

Sensor Name	Sensor#	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
BB +3.3V Standby	0Dh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +5V	0Eh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +12V	0Fh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB -12V	10h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB VBAT	11h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc VRM1	12h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc VRM2	13h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 1	14h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 2	15h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 3	16h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 1	17h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 2	18h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 3	19h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 Performance	1Dh	Voltage 02h	Digital Discrete 06h	Performance Lags	As & De	–
LVDS SCSI channel 2 Performance	1Eh	Voltage 02h	Digital Discrete 06h	Performance Lags	As & De	–
Baseboard Temp	30h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Front Panel Temp	31h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
PDB Temp	32h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc 1 Temp	33h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog

Sensor Name	Sensor#	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Proc 2 Temp	34h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost Baseboard Temp	3Bh	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost Front Panel Temp	3Ch	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost PDB Temp	3Dh	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost Proc 1 Core Temp	3Eh	OEM C7h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost Proc 2 Core Temp	3Fh	OEM C7h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 1	48h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 2	49h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 3	4Ah	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 4	4Bh	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 5	4Ch	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 6	4Dh	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
PDB Fan 1	58h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
PDB Fan 2	59h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Power Supply 1	5Ah	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As	–
Power Supply 2	5Bh	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As	–
Power Supply 3	5Ch	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As	–

Sensor Name	Sensor#	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Missing CPU Module	5Eh	Module/Board 15h	Digital Discrete 03h	State Asserted	As	–
Proc 1 Status	5Fh	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3	As	–
				Disabled	As & De	–
Proc 2 Status	60h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3	As	–
				Disabled	As & De	–
DIMM 1	68h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 2	69h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 3	6Ah	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 4	6Bh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 5	6Ch	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 6	6Dh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
System ACPI Power State	78h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–
Button	79h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–

Sensor Name	Sensor#	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
System Event	7Ah	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset)	As	–
SMI Timeout	7Bh	SMI Timeout F3h	Digital 03h	State Asserted	As	–
Sensor Failure	7Ch	Sensor Failure F6h	OEM Sensor Specific 73h	I ² C device not found I ² C device error detected I ² C Bus Timeout	As	–
NMI Signal State	7Dh	OEM C0h	Digital Discrete 03h	–	–	–
SMI Signal State	7Eh	OEM C0h	Digital Discrete 03h	–	–	–

Appendix 2: Server System SSH4 Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost A/C Restored	As	–
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy Regain Redundancy Lost Redundancy Degrade	As	–
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost
POST Error	06h	System Firmware Progress 0Fh	Sensor Specific 6Fh	POST error	As	–
FP Diag Interrupt (NMI for IA-32, INIT for IA-64)	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI	As & De	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Correctable ECC Uncorrectable ECC	As	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–
BB +1.25V	0Ah	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +2.5V	0Bh	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +3.3V	0Ch	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
BB +3.3V Standby	0Dh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +5V	0Eh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +12V	0Fh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB -12V	10h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB VBAT	11h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc VRM	12h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 1	14h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 2	15h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator 3	16h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 1	17h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 2	18h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator 3	19h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 Performance	1Dh	Voltage 02h	Digital Discrete 06h	Performance Met or Lags	As & De	–
LVDS SCSI channel 2 Performance	1Eh	Voltage 02h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Proc 1 Hot	28h	Temp 01h	Digital Discrete 03h	State Asserted	As	–
Proc 2 Hot	29h	Temp 01h	Digital Discrete 03h	State Asserted	As	–
Proc 3 Hot	2Ah	Temp 01h	Digital Discrete 03h	State Asserted	As	–
Proc 4 Hot	2Bh	Temp 01h	Digital Discrete 03h	State Asserted	As	–
Baseboard Temp	30h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Front Panel Temp	31h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
PDB Temp	32h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc 1 Temp	33h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc 2 Temp	34h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc 3 Temp	35h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc 4 Temp	36h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Baseboard Temp	3Bh	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost Front Panel Temp	3Ch	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost PDB Temp	3Dh	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost Proc 1 Core Temp	3Eh	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Proc 2 Core Temp	3Fh	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Proc 3 Core Temp	40h	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Proc 4 Core Temp	41h	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 1	48h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 2	49h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 3	4Ah	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 4	4Bh	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 5	4Ch	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 6	4Dh	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Power Supply 1	5Ah	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Power Supply 2	5Bh	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Power Supply 3	5Ch	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Missing Module	5Eh	Module/Board 15h	Digital Discrete 03h	State Asserted	As	–
Proc 1 Status	5Fh	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled	As & De	–
Proc 2 Status	60h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled	As & De	–
Proc 3 Status	61h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled	As & De	–
Proc 4 Status	62h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled	As & De	–
Missing Memory Board	67h	Module / Board 15h	Digital Discrete 03h	State Asserted	As	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
DIMM 1	68h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 2	69h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 3	6Ah	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 4	6Bh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 5	6Ch	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 6	6Dh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 7	6Eh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 8	6Fh	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 9	70h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 10	71h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 11	72h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 12	73h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
System ACPI Power State	78h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Button	79h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–
System Event	7Ah	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset)	As	–
SMI Timeout	7Bh	SMI Timeout F3h	Digital Discrete 03h	State Asserted	As	–
Sensor Failure	7Ch	Sensor Failure F6h	OEM Sensor Specific 73h	I ² C device not found I ² C device error detected I ² C Bus Timeout	As	–
NMI Signal State	7Dh	OEM C0h	Digital Discrete 03h	–	–	–
SMI Signal State	7Eh	OEM C0h	Digital Discrete 03h	–	–	–
PCI Hot Plug Slot 5	84h	Slot Connector 21h	Sensor Specific 6Fh	Fault Ready for Installation Ready for Removal Power Off	As & De	–
PCI Hot Plug Slot 6	85h	Slot Connector 21h	Sensor Specific 6Fh	Fault Ready for Installation Ready for Removal Power Off	As & De	–
PCI Hot Plug Slot 7	86h	Slot Connector 21h	Sensor Specific 6Fh	Fault Ready for Installation Ready for Removal Power Off	As & De	–
PCI Hot Plug Slot 8	87h	Slot Connector 21h	Sensor Specific 6Fh	Fault Ready for Installation Ready for Removal Power Off	As & De	–

Appendix 3: Server Board SE7500WV2 Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost A/C Restored	As	–
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy Lost	As	–
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost
POST Error	06h	POST error 0Fh	Sensor Specific 6Fh	POST error	As	–
Critical Interrupt Sensor	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI, Bus Error	As & De	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Correctable ECC Uncorrectable ECC	As	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–
BB +1.2V	10h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +1.25V	11h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +1.8V	12h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +1.8V Standby	13h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +2.5V	14h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
BB +3.3V	15h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +3.3V Auxillary	16h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +5V	17h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +5V Standby	18h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +12V	19h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB +12V VRM	1Ah	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB -12V	1Bh	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB VBAT	1Ch	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
BB Temp	30h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Front Panel Temp	32h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost BB Temp	33h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost ATA Temp	34h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
ATA Temp	35h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost Front Panel Temp	36h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Tach Fan 1	40h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 2	41h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 3	42h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 4	43h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 5	44h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Tach Fan 6	45h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
LVDS SCSI channel 1 terminator Performance	68h	Voltage 02h	Digital Discrete 06h	Performance Met or Lags	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
LVDS SCSI channel 2 terminator Performance	69h	Voltage 02h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Power Supply Status 1 (SR2300)	70h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Power Supply Status 2 (SR2300)	71h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
PDB Fan	73h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
PDB Temp	76h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost PDB Temp	77h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Processor Missing	80h	Module / Board 15h	Digital Discrete 03h	State Asserted, State Deasserted	As	–
System ACPI Power State	82h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–
System Event	83h	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset)	As	–
Button	84h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–
SMI Timeout	85h	SMI Timeout F3h	Sensor Specific 6Fh	State Asserted	As	–
Sensor Failure	86h	Sensor Failure F6h	OEM Sensor Specific 73h	I ² C device not found I ² C device error detected I ² C Bus Timeout	As	–
NMI Signal State	87h	OEM C0h	Digital Discrete 06h	–	–	–
SMI Signal State	88h	OEM C0h	Digital Discrete 06h	–	–	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
Front Side Bus Select	89h	BSEL Mismatch F7h	Sensor Specific 6Fh	State Asserted	As	–
Proc 1 Status	90h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled Terminator Presence	As & De	–
Proc 2 Status	91h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR FRB1 FRB2 FRB3 Disabled Terminator Presence	As & De	–
Proc 1 Core Temp	98h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc 2 Core Temp	99h	Temp 01h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost Proc 1 Core Temp	A0h	OEM C7h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Fan Boost Proc 2 Core Temp	A1h	OEM C7h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Processor 1 Fan	A8h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Processor 2 Fan	A9h	Fan 04h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Proc VRM	B8h	Voltage 02h	Threshold 01h	[u,l][nr,c,nc]	As & De	Analog
Processor 1 HOT	C0h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–
Processor 1 HOT	C1h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–
DIMM 1	E0h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / De-assert	Readable Value / Offsets
DIMM 2	E1h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 3	E2h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 4	E3h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 5	E4h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 6	E5h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–

Appendix 4: Server Board SE7501WV2 Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost Soft Power Control Fault Power Unit Failure	As	–
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Fully Redundant Redundancy Lost Redundancy Degraded Non-redund: sufficient resources (loss of resources) Non-redund: sufficient resources (gain of resources) Non-redund: insufficient resources Redundancy Degraded from Fully Redundant (loss of resources) Redundancy Degraded from Non-redundant (gain of resources)	As	–
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost
POST Error	06h	POST error 0Fh	Sensor Specific 6Fh	POST error	As	–
Critical Interrupt Sensor	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI Uncorrectable Bus Error	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Uncorrectable ECC	As	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–
Session Audit	0Ah	Session Audit 2Ah	Sensor Specific 6Fh	Session Activation Session Deactivation	As	–
BB +1.2V	10h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +1.25V	11h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +1.8V	12h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +1.8V Standby	13h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +2.5V	14h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +3.3V	15h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +3.3V Auxillary	16h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +5V	17h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +5V Standby	18h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +12V	19h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB +12V VRM	1Ah	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB -12V	1Bh	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB VBAT	1Ch	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
BB Temp	30h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Front Panel Temp	32h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost BB Temp	33h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost ATA Temp	34h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
ATA Temp	35h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Fan Boost Front Panel Temp	36h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Tach Fan 1	40h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 2	41h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 3	42h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 4	43h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 5	44h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 6	45h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Tach Fan 7	46h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Digital Fan 1	50h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 2	51h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 3	52h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 4	53h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 5	54h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 6	55h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 7	56h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
LVDS SCSI channel 1 terminator power	60h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
LVDS SCSI channel 2 terminator power	61h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Power Supply Status 1 (SR2300)	70h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Power Supply Status 2 (SR2300)	71h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
PDB Fan	73h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
PDB Temp	76h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost PDB Temp	77h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Processor Missing	80h	Module / Board 15h	Digital Discrete 03h	State Asserted State Deasserted	As	–
System ACPI Power State	82h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–
System Event	83h	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset) PEF Action	As	–
Button	84h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–
SMI Timeout	85h	SMI Timeout F3h	Digital Discrete 03h	State Asserted State Deasserted	As	–
Sensor Failure	86h	Sensor Failure F6h	OEM Sensor Specific 73h	I ² C device not found I ² C device error detected I ² C Bus Timeout	As	–
NMI Signal State	87h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–
SMI Signal State	88h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–
Front Side Bus Speed Mismatch	89h	BSEL Mismatch F7h	Digital Discrete 03h	State Asserted	As	–
Proc 1 Status	90h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1. FRB2. FRB3 Disabled Terminator Presence	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Proc 2 Status	91h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1, FRB2, FRB3, Disabled Terminator Presence	As & De	–
Proc 1 Core Temp	98h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc 2 Core Temp	99h	Temp 01h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Proc 1 Core Temp	A0h	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Fan Boost Proc 2 Core Temp	A1h	OEM C7h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Processor 1 Fan	A8h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Processor 2 Fan	A9h	Fan 04h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Proc VRM	B8h	Voltage 02h	Threshold 01h	[u,][nr,c,nc]	As & De	Analog
Processor HOT	C0h	Temp 01h	Digital Discrete 07h	Transitioned to Non-Critical from OK	As & De	–
DIMM 1	E0h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 2	E1h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 3	E2h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 4	E3h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 5	E4h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 6	E5h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–

Appendix 5: Server Board SE7501BR2 Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost Soft Power Control Fault Power Unit Failure	As	–
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy lost	As	–
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost
POST Error	06h	POST error 0Fh	Sensor Specific 6Fh	POST error	As	–
Critical Interrupt Sensor	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI Bus Error	As & De	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Uncorrectable ECC	As	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–
Session Audit	0Ah	Session Audit 2Ah	Sensor Specific 6Fh	00: Session Activation 01: Session Deactivation	As	–
BB +1.2V	10h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +1.25V_A	11h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +1.8V	13h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
BB +1.8V Standby	14h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +2.5V	15h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +3.3V	16h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +3.3V Auxillary	17h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +5V	18h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +5V Standby	19h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +12V	1Ah	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB +12V VRM	1Bh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB -12V	1Ch	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB VBAT	1Dh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
BB Temp	30h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Front Panel Temp	31h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Fan Boost BB Temp	32h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Fan Boost Front Panel Temp	33h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog
Tach Fan 1	40h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Tach Fan 2	41h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Tach Fan 3	42h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Tach Fan 4	43h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Tach Fan 5	44h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Tach Fan 6	45h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Digital Fan 1	50h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 2	51h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Digital Fan 3	52h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 4	53h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 5	54h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
Digital Fan 6	55h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–
LVDS SCSI channel terminator power	60h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Power Supply Status 1 (SC5200)	70h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Power Supply Status 2 (SC5200)	71h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Power Supply Status 3 (SC5200)	72h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–
Power Cage Fan 1	73h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Power Cage Fan 2	74h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Power Cage Temp	76h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Processor Missing	80h	Module / Board 15h	Digital Discrete 03h	State Asserted State Deasserted	As	–
System ACPI Power State	82h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–
System Event	83h	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset) PEF Action	As	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Button	84h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–
SMI Timeout	85h	SMI Timeout F3h	Digital Discrete 03h	State Asserted State Deasserted	As	–
Sensor Failure	86h	Sensor Failure F6h	OEM Sensor Specific 73h	°C device not found °C device error detected °C Bus Timeout	As	–
NMI Signal State	87h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–
SMI Signal State	88h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–
Front Side Bus Speed Mismatch	89h	BSEL Mismatch F7h	Digital Discrete 03h	State Asserted	As	–
Proc 1 Status	90h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1, FRB2, FRB3 Disabled Terminator Presence	As & De	–
Proc 2 Status	91h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1, FRB2, FRB3, Disabled Terminator Presence	As & De	–
Proc 1 Core Temp	98h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Proc 2 Core Temp	99h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Fan Boost Proc 1 Core Temp	A0h	OEM C7h	Threshold 01h	[u,l][nc]	As & De	Analog
Fan Boost Proc 2 Core Temp	A1h	OEM C7h	Threshold 01h	[u,l][nc]	As & De	Analog
Processor 1 Fan	A8h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Processor 2 Fan	A9h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog
Proc Vccp	B8h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets
Processor HOT	C0h	Temp 01h	Digital Discrete 03h	State Asserted State Deasserted	As & De	–
DIMM 1	E0h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 2	E1h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 3	E2h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–
DIMM 4	E3h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–

Appendix 6: Server Board SE7501HG2 Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Power Unit Status	01h	Power Unit 09h	Sensor Specific 6Fh	Power Off Power Cycle A/C Lost Soft Power Control Fault Power Unit Failure	As	–	Trig Offset	A	X
Power Unit Redundancy	02h	Power Unit 09h	Generic 0Bh	Redundancy lost	As	–	Trig Offset	A	X
Watchdog	03h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power Cycle Timer Interrupt	As & De	–	Trig Offset	A	X
Platform Security Violation	04h	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Secure mode violation attempt Out-of-band access password violation	As	–	Trig Offset	A	X
Physical Security Violation	05h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion LAN Leash Lost	As & De	General Chassis Intrusion LAN Leash Lost	Trig Offset	A	X
POST Error	06h	POST error 0Fh	Sensor Specific 6Fh	POST error	As	–	POST Code	A	–
Critical Interrupt Sensor	07h	Critical Interrupt 13h	Sensor Specific 6Fh	Front Panel NMI Bus Error	As & De	–	Trig Offset	A	–
Memory	08h	Memory 0Ch	Sensor Specific 6Fh	Uncorrectable ECC	As	–	Trig Offset	A	–
Event Logging Disabled	09h	Event Logging Disabled 10h	Sensor Specific 6Fh	Correctable Memory Error Logging Disabled Log Area Reset/Cleared	As	–	Trig Offset	A	X
Session Audit	0Ah	Session Audit 2Ah	Sensor Specific 6Fh	00: Session Activation 01: Session Deactivation	As	–	As defined by IPMI	A	X
BB +1.2V	10h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
BB +1.25V_A	11h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +1.8V	12h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +1.8V Standby	13h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
BB +2.5V	14h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +3.3V	15h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +3.3V Auxillary	16h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +5V	17h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +5V Standby	18h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
BB +12V	19h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB +12V VRM	1Ah	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB -12V	1Bh	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
BB VBAT	1Ch	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
BB Temp	30h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
Front Panel Temp	31h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
Fan Boost BB Temp	32h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog	–	A	–
Fan Boost Front Panel Temp	33h	OEM C7h	Threshold 01h	[u][nc]	As & De	Analog	–	A	–
Tach Fan 1	40h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–
Tach Fan 2	41h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–
Tach Fan 3	42h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–
Tach Fan 4	43h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–
Tach Fan 5	44h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–
Tach Fan 6	45h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Digital Fan 1	50h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 2	51h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 3	52h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 4	53h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 5	54h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
Digital Fan 6	55h	Fan 04h	Digital Discrete 06h	Performance Met or Lags	As & De	–	Trig Offset	M	–
LVDS SCSI A channel terminator power	60h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
LVDS SCSI B channel terminator power	61h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
Power Supply Status 1	70h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–	Trig Offset	A	X
Power Supply Status 2	71h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–	Trig Offset	A	X
Power Supply Status 3	72h	Power Supply 08h	Sensor Specific 6Fh	Presence Failure Predictive Fail A/C Lost	As & De	–	Trig Offset	A	X
Power Cage Fan 1	73h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
Power Cage Fan 2	74h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	–
Power Cage Temp	76h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	X
Processor Missing	80h	Module / Board 15h	Digital Discrete 03h	State Asserted State Deasserted	As	–	Trig Offset	A	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
System ACPI Power State	82h	System ACPI Power State 22h	Sensor Specific 6Fh	S0 / G0 S1 S4 S5 / G2 G3 Mechanical Off	As	–	Trig Offset	A	X
System Event	83h	System Event 12h	Sensor Specific 6Fh	OEM System Boot Event (Hard Reset) PEF Action	As	–	Trig Offset	A	–
Button	84h	Button 14h	Sensor Specific 6Fh	Power Button Sleep Button Reset Button	As	–	Trig Offset	A	X
SMI Timeout	85h	SMI Timeout F3h	Digital Discrete 03h	State Asserted State Deasserted	As	–	Trig Offset	A	–
Sensor Failure	86h	Sensor Failure F6h	OEM Sensor Specific 73h	I ² C device not found I ² C device error detected I ² C Bus Timeout	As	–	Trig Offset	A	X
NMI Signal State	87h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–	–	–	–
SMI Signal State	88h	OEM C0h	Digital Discrete 03h	State Asserted State Deasserted	–	–	–	–	–
Front Side Bus Speed Mismatch	89h	BSEL Mismatch F7h	Digital Discrete 03h	State Asserted	As	–	Trig Offset	A	–
Proc 1 Status	90h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1, FRB2, FRB3 Disabled Terminator Presence	As & De	–	Trig Offset	M	X
Proc 2 Status	91h	Processor 07h	Sensor Specific 6Fh	Presence Thermal Trip IERR, FRB1, FRB2, FRB3, Disabled Terminator Presence	As & De	–	Trig Offset	M	X
Proc 1 Core Temp	98h	Temp 01h	Threshold 01h	[u,]l[c,nc]	As & De	Analog	R, T	A	–

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
Proc 2 Core Temp	99h	Temp 01h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	-
Fan Boost Proc 1 Core Temp	A0h	OEM C7h	Threshold 01h	[u,l][nc]	As & De	Analog	-	A	-
Fan Boost Proc 2 Core Temp	A1h	OEM C7h	Threshold 01h	[u,l][nc]	As & De	Analog	-	A	-
Processor 1 Fan	A8h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	-
Processor 2 Fan	A9h	Fan 04h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	M	-
Proc Vccp	B8h	Voltage 02h	Threshold 01h	[u,l][c,nc]	As & De	Analog	R, T	A	-
Processor HOT	C0h	Temp 01h	Digital Discrete 03h	State Asserted State Deasserted	As & De	-	Trig Offset	M	-
Fan Redundancy	D0	Fan 04h	Generic 0Bh	Redundancy Regained Redundancy lost Redundancy Degraded	As	-	Trig Offset	A	-
Fan 1 Presence	D8h	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-
Fan 2 Presence	D9h	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-
Fan 3 Presence	DAh	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-
Fan 4 Presence	DBh	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-
Fan 5 Presence	DCh	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-
Fan 6 Presence	DDh	Slot/Connector 21h	Sensor Specific 6Fh	Fault Status asserted Identify Status Asserted	As	-	Trig Offset	A	-

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	Rearm	Standby
DIMM 1	E0h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 2	E1h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 3	E2h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 4	E3h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 5	E4h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–
DIMM 6	E5h	Slot Connector 21h	Sensor Specific 6Fh	Fault Status Asserted Device Installed Disabled	As	–	Trig Offset	A	–

Appendix 7: Server Board SE7210TP1-E Sensors

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData
Physical Security Violation	01	Physical Security 05h	Sensor Specific 6Fh	LAN Leash Lost	As	LAN Leash Lost	Trig Offset
Platform Security Violation	02	Platform Security Violation Attempt 06h	Sensor Specific 6Fh	Out-of-band access password violation	As	–	Trig Offset
Power Unit Status	03	Power Unit 09h	Sensor Specific 6Fh	Power On/Off Power cycle AC Lost	As	–	Trig Offset
Button	04h	Button 14h	Sensor Specific 6Fh	Power Button Reset Button	As	–	Trig Offset
Watchdog	05h	Watchdog2 23h	Sensor Specific 6Fh	Timer Expired Hard Reset Power Down Power cycle Timer Interrupt	As	–	Trig Offset

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	PEF Action
Physical Security Violation	07h	Physical Security 05h	Sensor Specific 6Fh	General Chassis Intrusion	As	General Chassis Intrusion	Trig Offset	LAN Alert
BB +1.5V	08	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
BB +3.3V	09h	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
BB +5V	0Ah	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
BB +12V	0Bh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
MCH Vtt	0Ch	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action

Sensor Name	Sensor #	Sensor Type	Event / Reading Type	Event Offset Triggers	Assert / Deassert	Readable Value / Offsets	EventData	PEF Action
BB VCCP CPU1	0Dh	Voltage 02h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
BB Temp	0Eh	Temp 01h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 1	0Fh	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 2	10h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 3	11h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 4	12h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 5	13h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
Tach Fan 6	14h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	Fault LED Action
System Event	15h	System Event 12h	Sensor Specific 6Fh	• PEF Action	As	–	Trig Offset	–
Proc 1 IERR	16h	Processor 07h	Sensor Specific 6Fh	• IERR	As	–	Trig Offset	Fault LED Action
Proc 1 Thermal trip	17h	Processor 07h	Sensor Specific 6Fh	Thermal Trip	As	–	Trig Offset	Cooling Fault LED Action
Processor 1 Fan	18h	Fan 04h	Threshold 01h	[u,l][nr, c,nc]	As & De	Analog	R, T	System Fault LED
Processor HOT	19h	Temp 01h	Digital Discrete 03h	State Asserted State Deasserted	As & De	–	Trig Offset	System Fault LED
Diagnostic interrupt Button	1Ah	Button 14h	Sensor Specific 6Fh	FP NMI Button	As	–	Trig Offset	diagnostic Interrupt Action) NMI Generation
Chassis Identify Button	1Bh	Button 14h	Sensor Specific 6Fh	FP ID Button	As	–	Trig Offset	ID LED Action

Appendix 8: DMTF Groups and OIDs

This appendix contains tables listing all supported simple network management protocol (SNMP) management information base (MIB) object identifier (OID) and associated MIB groups and attributes. The tables also list the type and access privilege of each attribute.

- The first section below lists the basebrd4.mib file OIDs used for the Windows operating system on the server side. Open Unix and NetWare use the same OIDs as Windows.
- The second section lists the mapbase4.mib file's OIDs for the Linux operating system on the server side.

For SNMP configuration and usage information refer to the *Intel Server Management Install and User Guide*.

Windows/Open Unix/NetWare

The following table contains supported dmtf groups and MIB OIDs in the basebrd4.mib for Windows/Open Unix/NetWare.

Major SNMP group: private.enterprises.intel.products.server-management.software.basebrd4.dmtfGroups:

S.No	Group	Attribute	OID	Type	Access Privilege
1	tComponentid.eComponentid	a1Manufacturer	1.3.6.1.4.1.343.2.10.3.4.1.1.1.1	DmiDisplaystring	Read-Only
2		a1Product	1.3.6.1.4.1.343.2.10.3.4.1.1.1.2	DmiDisplaystring	Read-Only
3		a1Version	1.3.6.1.4.1.343.2.10.3.4.1.1.1.3	DmiDisplaystring	Read-Only
4		a1SerialNumber	1.3.6.1.4.1.343.2.10.3.4.1.1.1.4	DmiDisplaystring	Read-Only
5		a1Installation	1.3.6.1.4.1.343.2.10.3.4.1.1.1.5	DmiDate	Read-Only
6		a1Verify	1.3.6.1.4.1.343.2.10.3.4.1.1.1.6	Integer	Read-Only
7	tGeneralInformation.eGeneralInformation	a2SystemName	1.3.6.1.4.1.343.2.10.3.4.1.2.1.1	DmiDisplaystring	Read-Write
8		a2SystemLocation	1.3.6.1.4.1.343.2.10.3.4.1.2.1.2	DmiDisplaystring	Read-Write
9		a2SystemPrimaryUserName	1.3.6.1.4.1.343.2.10.3.4.1.2.1.3	DmiDisplaystring	Read-Write
10		a2SystemPrimaryUserPhone	1.3.6.1.4.1.343.2.10.3.4.1.2.1.4	DmiDisplaystring	Read-Write
11		a2SystemBootupTime	1.3.6.1.4.1.343.2.10.3.4.1.2.1.5	DmiDate	Read-Write
12		a2SystemDateTime	1.3.6.1.4.1.343.2.10.3.4.1.2.1.6	DmiDate	Read-Write
13	tSystemBios.eSystemBios	a4BiosIndex	1.3.6.1.4.1.343.2.10.3.4.1.4.1.1	DmiInteger	Read-Only
14		a4BiosManufacturer	1.3.6.1.4.1.343.2.10.3.4.1.4.1.2	DmiDisplaystring	Read-Only
15		a4BiosVersion	1.3.6.1.4.1.343.2.10.3.4.1.4.1.3	DmiDisplaystring	Read-Only
16		a4BiosRomSize	1.3.6.1.4.1.343.2.10.3.4.1.4.1.4	DmiInteger	Read-Only
17		a4BiosStartingAddress	1.3.6.1.4.1.343.2.10.3.4.1.4.1.5	DmiInteger64	Read-Only
18		a4BiosEndingAddress	1.3.6.1.4.1.343.2.10.3.4.1.4.1.6	DmiInteger64	Read-Only
19		a4BiosLoaderVersion	1.3.6.1.4.1.343.2.10.3.4.1.4.1.7	DmiDisplaystring	Read-Only
20		a4BiosReleaseDate	1.3.6.1.4.1.343.2.10.3.4.1.4.1.8	DmiDate	Read-Only
21		a4PrimaryBios	1.3.6.1.4.1.343.2.10.3.4.1.4.1.9	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
22	tSystemBiosCharacteristics.eSystemBiosCharacteristics	a5BiosCharacteristicIndex	1.3.6.1.4.1.343.2.10.3.4.1.5.1.1	DmiInteger	Read-Only
23		a5BiosNumber	1.3.6.1.4.1.343.2.10.3.4.1.5.1.2	DmiInteger	Read-Only
24		a5BiosCharacteristic	1.3.6.1.4.1.343.2.10.3.4.1.5.1.3	Integer	Read-Only
25		a5BiosCharacteristicDescription	1.3.6.1.4.1.343.2.10.3.4.1.5.1.4	DmiDisplaystring	Read-Only
26	tProcessor.eProcessor	a6ProcessorIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.1	DmiInteger	Read-Only
27		a6ProcessorType	1.3.6.1.4.1.343.2.10.3.4.1.6.1.2	Integer	Read-Only
28		a6ProcessorFamily	1.3.6.1.4.1.343.2.10.3.4.1.6.1.3	Integer	Read-Only
29		a6ProcessorVersionInformation	1.3.6.1.4.1.343.2.10.3.4.1.6.1.4	DmiDisplaystring	Read-Only
30		a6MaximumSpeed	1.3.6.1.4.1.343.2.10.3.4.1.6.1.5	DmiInteger	Read-Only
31		a6CurrentSpeed	1.3.6.1.4.1.343.2.10.3.4.1.6.1.6	DmiInteger	Read-Only
32		a6ProcessorUpgrade	1.3.6.1.4.1.343.2.10.3.4.1.6.1.7	Integer	Read-Only
33		a6FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.8	DmiInteger	Read-Only
34		a6OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.9	DmiInteger	Read-Only
35		a6Level1CacheIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.10	DmiInteger	Read-Only
36		a6Level2CacheIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.11	DmiInteger	Read-Only
37		a6Level3CacheIndex	1.3.6.1.4.1.343.2.10.3.4.1.6.1.12	DmiInteger	Read-Only
38		a6Status	1.3.6.1.4.1.343.2.10.3.4.1.6.1.13	Integer	Read-Only
39	Motherboard.eMotherboard	a7NumberOfExpansionSlots	1.3.6.1.4.1.343.2.10.3.4.1.7.1.1	DmiInteger	Read-Only
40		a7FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.7.1.2	DmiInteger	Read-Only
41		a7OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.7.1.3	DmiInteger	Read-Only
42	tSystemCache.eSystemCache	a10SystemCacheIndex	1.3.6.1.4.1.343.2.10.3.4.1.10.1.1	DmiInteger	Read-Only
43		a10SystemCacheLevel	1.3.6.1.4.1.343.2.10.3.4.1.10.1.2	Integer	Read-Only
44		a10SystemCacheSpeed	1.3.6.1.4.1.343.2.10.3.4.1.10.1.3	DmiInteger	Read-Only
45		a10SystemCacheSize	1.3.6.1.4.1.343.2.10.3.4.1.10.1.4	DmiInteger	Read-Only
46		a10SystemCacheWritePolicy	1.3.6.1.4.1.343.2.10.3.4.1.10.1.5	Integer	Read-Only
47		a10SystemCacheErrorCorrection	1.3.6.1.4.1.343.2.10.3.4.1.10.1.6	Integer	Read-Only
48		a10FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.10.1.7	DmiInteger	Read-Only
49		a10OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.10.1.8	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
50		a10SystemCacheType	1.3.6.1.4.1.343.2.10.3.4.1.10.1.9	Integer	Read-Only
51	tPowerSupply.ePowerSupply	a17PowerSupplyIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.1	DmiInteger	Read-Only
52		a17FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.2	DmiInteger	Read-Only
53		a17OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.3	DmiInteger	Read-Only
54		a17PowerUnitIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.4	DmiInteger	Read-Only
55		a17PowerSupplyType	1.3.6.1.4.1.343.2.10.3.4.1.17.1.5	Integer	Read-Only
56		a17InputVoltageCapabilityDescription	1.3.6.1.4.1.343.2.10.3.4.1.17.1.6	DmiDisplaystring	Read-Only
57		a17Range1InputVoltageLow	1.3.6.1.4.1.343.2.10.3.4.1.17.1.7	DmiInteger	Read-Only
58		a17Range1InputVoltageHigh	1.3.6.1.4.1.343.2.10.3.4.1.17.1.8	DmiInteger	Read-Only
59		a17Range1VoltageProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.9	DmiInteger	Read-Only
60		a17Range1ElectricalCurrentProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.10	DmiInteger	Read-Only
61		a17Range2InputVoltageLow	1.3.6.1.4.1.343.2.10.3.4.1.17.1.11	DmiInteger	Read-Only
62		a17Range2InputVoltageHigh	1.3.6.1.4.1.343.2.10.3.4.1.17.1.12	DmiInteger	Read-Only
63		a17Range2VoltageProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.13	DmiInteger	Read-Only
64		a17Range2CurrentProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.17.1.14	DmiInteger	Read-Only
65		a17ActiveInputVoltageRange	1.3.6.1.4.1.343.2.10.3.4.1.17.1.15	Integer	Read-Only
66		a17InputVoltageRangeSwitching	1.3.6.1.4.1.343.2.10.3.4.1.17.1.16	Integer	Read-Only
67		a17Range1InputFrequencyLow	1.3.6.1.4.1.343.2.10.3.4.1.17.1.17	DmiInteger	Read-Only
68		a17Range1InputFrequencyHigh	1.3.6.1.4.1.343.2.10.3.4.1.17.1.18	DmiInteger	Read-Only
69		a17Range2InputFrequencyLow	1.3.6.1.4.1.343.2.10.3.4.1.17.1.19	DmiInteger	Read-Only
70		a17Range2InputFrequencyHigh	1.3.6.1.4.1.343.2.10.3.4.1.17.1.20	DmiInteger	Read-Only
71		a17TotalOutputPower	1.3.6.1.4.1.343.2.10.3.4.1.17.1.21	DmiInteger	Read-Only
72	tSystemSlots.eSystemSlots	a19SlotIndex	1.3.6.1.4.1.343.2.10.3.4.1.19.1.1	DmiInteger	Read-Only
73		a19SlotType	1.3.6.1.4.1.343.2.10.3.4.1.19.1.2	DmiInteger64	Read-Only
74		a19SlotWidth	1.3.6.1.4.1.343.2.10.3.4.1.19.1.3	Integer	Read-Only
75		a19CurrentUsage	1.3.6.1.4.1.343.2.10.3.4.1.19.1.4	Integer	Read-Only
76		a19SlotDescription	1.3.6.1.4.1.343.2.10.3.4.1.19.1.5	DmiDisplaystring	Read-Only
77		a19SlotCategory	1.3.6.1.4.1.343.2.10.3.4.1.19.1.6	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
78		a19VirtualSlot	1.3.6.1.4.1.343.2.10.3.4.1.19.1.7	Integer	Read-Only
79		a19ResourceUserId	1.3.6.1.4.1.343.2.10.3.4.1.19.1.8	DmiInteger	Read-Only
80		a19VccMixedVoltageSupport	1.3.6.1.4.1.343.2.10.3.4.1.19.1.9	DmiInteger64	Read-Only
81		a19VppMixedVoltageSupport	1.3.6.1.4.1.343.2.10.3.4.1.19.1.10	DmiInteger64	Read-Only
82		a19SlotThermalRating	1.3.6.1.4.1.343.2.10.3.4.1.19.1.11	DmiInteger	Read-Only
83		a19OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.19.1.12	DmiInteger	Read-Only
84		a19SlotPowerState	1.3.6.1.4.1.343.2.10.3.4.1.19.1.13	Integer	Read-Only
85		a19SlotFaultState	1.3.6.1.4.1.343.2.10.3.4.1.19.1.14	Integer	Read-Only
86		a19SlotSwitchStatus	1.3.6.1.4.1.343.2.10.3.4.1.19.1.15	Integer	Read-Only
87	tCoolingUnitGlobalTable.eCoolingUnitGlobalTable	a28CoolingUnitIndex	1.3.6.1.4.1.343.2.10.3.4.1.28.1.1	DmiInteger	Read-Only
88		a28CoolingUnitStatus	1.3.6.1.4.1.343.2.10.3.4.1.28.1.2	Integer	Read-Only
89	tFieldReplaceableUnit.eFieldReplaceableUnit	a30FruIndex	1.3.6.1.4.1.343.2.10.3.4.1.30.1.1	DmiInteger	Read-Only
90		a30DeviceGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.30.1.2	DmiInteger	Read-Only
91		a30Description	1.3.6.1.4.1.343.2.10.3.4.1.30.1.3	DmiDisplaystring	Read-Only
92		a30Manufacturer	1.3.6.1.4.1.343.2.10.3.4.1.30.1.4	DmiDisplaystring	Read-Only
93		a30Model	1.3.6.1.4.1.343.2.10.3.4.1.30.1.5	DmiDisplaystring	Read-Only
94		a30PartNumber	1.3.6.1.4.1.343.2.10.3.4.1.30.1.6	DmiDisplaystring	Read-Only
95		a30FruSerialNumber	1.3.6.1.4.1.343.2.10.3.4.1.30.1.7	DmiDisplaystring	Read-Only
96		a30RevisionLevel	1.3.6.1.4.1.343.2.10.3.4.1.30.1.8	DmiDisplaystring	Read-Only
97		a30WarrantyStartDate	1.3.6.1.4.1.343.2.10.3.4.1.30.1.9	DmiDate	Read-Only
98		a30WarrantyDuration	1.3.6.1.4.1.343.2.10.3.4.1.30.1.10	DmiInteger	Read-Only
99		a30SupportPhoneNumber	1.3.6.1.4.1.343.2.10.3.4.1.30.1.11	DmiDisplaystring	Read-Only
100		a30FruInternetUniformResourceLocator	1.3.6.1.4.1.343.2.10.3.4.1.30.1.12	DmiDisplaystring	Read-Only
101	tOperationalState.eOperationalState	a31OperationalStateInstanceIndex	1.3.6.1.4.1.343.2.10.3.4.1.31.1.1	DmiInteger	Read-Only
102		a31DeviceGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.31.1.2	DmiInteger	Read-Only
103		a31OperationalStatus	1.3.6.1.4.1.343.2.10.3.4.1.31.1.3	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
104		a31UsageState	1.3.6.1.4.1.343.2.10.3.4.1.31.1.4	Integer	Read-Only
105		a31AvailabilityStatus	1.3.6.1.4.1.343.2.10.3.4.1.31.1.5	Integer	Read-Only
106		a31AdministrativeState	1.3.6.1.4.1.343.2.10.3.4.1.31.1.6	Integer	Read-Only
107		a31FatalErrorCount	1.3.6.1.4.1.343.2.10.3.4.1.31.1.7	DmiCounter	Read-Only
108		a31MajorErrorCount	1.3.6.1.4.1.343.2.10.3.4.1.31.1.8	DmiCounter	Read-Only
109		a31WarningErrorCount	1.3.6.1.4.1.343.2.10.3.4.1.31.1.9	DmiCounter	Read-Only
110		a31CurrentErrorStatus	1.3.6.1.4.1.343.2.10.3.4.1.31.1.10	Integer	Read-Only
111		a31DevicePredictedFailureStatus	1.3.6.1.4.1.343.2.10.3.4.1.31.1.11	Integer	Read-Only
112	tPhysicalMemoryArray.ePhysicalMemoryArray	a34MemoryArrayTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.34.1.1	DmiInteger	Read-Only
113		a34MemoryArrayLocation	1.3.6.1.4.1.343.2.10.3.4.1.34.1.2	Integer	Read-Only
114		a34MemoryArrayUse	1.3.6.1.4.1.343.2.10.3.4.1.34.1.3	Integer	Read-Only
115		a34MaximumMemoryCapacity	1.3.6.1.4.1.343.2.10.3.4.1.34.1.4	DmiInteger	Read-Only
116		a34NumberOfMemoryDeviceSockets	1.3.6.1.4.1.343.2.10.3.4.1.34.1.5	DmiInteger	Read-Only
117		a34NumberOfMemoryDeviceSocketsUsed	1.3.6.1.4.1.343.2.10.3.4.1.34.1.6	DmiInteger	Read-Only
118		a34MemoryErrorCorrection	1.3.6.1.4.1.343.2.10.3.4.1.34.1.7	Integer	Read-Only
119		a34ArrayErrorType	1.3.6.1.4.1.343.2.10.3.4.1.34.1.8	Integer	Read-Only
120		a34LastErrorUpdate	1.3.6.1.4.1.343.2.10.3.4.1.34.1.9	Integer	Read-Only
121		a34ErrorOperation	1.3.6.1.4.1.343.2.10.3.4.1.34.1.10	Integer	Read-Only
122		a34ErrorDataSize	1.3.6.1.4.1.343.2.10.3.4.1.34.1.11	DmiInteger	Read-Only
123		a34ErrorData	1.3.6.1.4.1.343.2.10.3.4.1.34.1.12	DmiOctetstring	Read-Only
124		a34VendorSyndrome	1.3.6.1.4.1.343.2.10.3.4.1.34.1.13	DmiOctetstring	Read-Only
125		a34ErrorAddress	1.3.6.1.4.1.343.2.10.3.4.1.34.1.14	DmiInteger64	Read-Only
126		a34ErrorResolution	1.3.6.1.4.1.343.2.10.3.4.1.34.1.15	DmiInteger	Read-Only
127		a34FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.34.1.16	DmiInteger	Read-Only
128		a34OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.34.1.17	DmiInteger	Read-Only
129	tMemoryArrayMappedAddresses.eMemoryArrayMappedAddresses	a35MemoryArrayMappedAddressesTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.35.1.1	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
130			1.3.6.1.4.1.343.2.10.3.4.1.35.1.2	DmiInteger	Read-Only
131			1.3.6.1.4.1.343.2.10.3.4.1.35.1.3	DmiInteger	Read-Only
132			1.3.6.1.4.1.343.2.10.3.4.1.35.1.4	DmiInteger	Read-Only
133			1.3.6.1.4.1.343.2.10.3.4.1.35.1.5	DmiInteger	Read-Only
134			1.3.6.1.4.1.343.2.10.3.4.1.35.1.6	DmiInteger	Read-Only
135			1.3.6.1.4.1.343.2.10.3.4.1.35.1.7	DmiInteger	Read-Only
136	tMemoryDevice.eMemoryDevice	a36MemoryDeviceTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.36.1.1	DmiInteger	Read-Only
137		a36MemoryArrayIndex	1.3.6.1.4.1.343.2.10.3.4.1.36.1.2	DmiInteger	Read-Only
138		a36DeviceLocator	1.3.6.1.4.1.343.2.10.3.4.1.36.1.3	DmiDisplaystring	Read-Only
139		a36BankLocator	1.3.6.1.4.1.343.2.10.3.4.1.36.1.4	DmiDisplaystring	Read-Only
140		a36Size	1.3.6.1.4.1.343.2.10.3.4.1.36.1.5	DmiInteger	Read-Only
141		a36FormFactor	1.3.6.1.4.1.343.2.10.3.4.1.36.1.6	Integer	Read-Only
142		a36TotalWidth	1.3.6.1.4.1.343.2.10.3.4.1.36.1.7	DmiInteger	Read-Only
143		a36DataWidth	1.3.6.1.4.1.343.2.10.3.4.1.36.1.8	DmiInteger	Read-Only
144		a36MemoryType	1.3.6.1.4.1.343.2.10.3.4.1.36.1.9	Integer	Read-Only
145		a36TypeDetail	1.3.6.1.4.1.343.2.10.3.4.1.36.1.10	Integer	Read-Only
146		a36DeviceSet	1.3.6.1.4.1.343.2.10.3.4.1.36.1.11	DmiInteger	Read-Only
147		a36DeviceErrorType	1.3.6.1.4.1.343.2.10.3.4.1.36.1.12	Integer	Read-Only
148		a36ErrorGranularity	1.3.6.1.4.1.343.2.10.3.4.1.36.1.13	Integer	Read-Only
149		a36LastErrorUpdate	1.3.6.1.4.1.343.2.10.3.4.1.36.1.14	Integer	Read-Only
150		a36ErrorOperation	1.3.6.1.4.1.343.2.10.3.4.1.36.1.15	Integer	Read-Only
151		a36ErrorDataSize	1.3.6.1.4.1.343.2.10.3.4.1.36.1.16	DmiInteger	Read-Only
152		a36ErrorData	1.3.6.1.4.1.343.2.10.3.4.1.36.1.17	DmiOctetstring	Read-Only
153		a36VendorSyndrome	1.3.6.1.4.1.343.2.10.3.4.1.36.1.18	DmiOctetstring	Read-Only
154		a36DeviceErrorAddress	1.3.6.1.4.1.343.2.10.3.4.1.36.1.19	DmiInteger	Read-Only
155		a36ArrayErrorAddress	1.3.6.1.4.1.343.2.10.3.4.1.36.1.20	DmiInteger	Read-Only
156		a36ErrorResolution	1.3.6.1.4.1.343.2.10.3.4.1.36.1.21	DmiInteger	Read-Only
157		a36FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.36.1.22	DmiInteger	Read-Only
158		a36OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.36.1.23	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
159	tMemoryDeviceMappedAddressesMemoryDeviceMappedAddresses	a37MemoryDeviceMappedAddressesTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.37.1.1	DmiInteger	Read-Only
160		a37MemoryDeviceSetId	1.3.6.1.4.1.343.2.10.3.4.1.37.1.2	DmiInteger	Read-Only
161		a37Partition	1.3.6.1.4.1.343.2.10.3.4.1.37.1.3	DmiInteger	Read-Only
162		a37MappedRangeStartingAddresses	1.3.6.1.4.1.343.2.10.3.4.1.37.1.4	DmiInteger	Read-Only
163		a37MappedRangeEndingAddress	1.3.6.1.4.1.343.2.10.3.4.1.37.1.5	DmiInteger	Read-Only
164		a37PartitionRowPosition	1.3.6.1.4.1.343.2.10.3.4.1.37.1.6	DmiInteger	Read-Only
165		a37InterleavePosition	1.3.6.1.4.1.343.2.10.3.4.1.37.1.7	DmiInteger	Read-Only
166		a37DataDepth	1.3.6.1.4.1.343.2.10.3.4.1.37.1.8	DmiInteger	Read-Only
167		a50Power-onPasswordStatus	1.3.6.1.4.1.343.2.10.3.4.1.50.1.1	Integer	Read-Only
168		a50KeyboardPasswordStatus	1.3.6.1.4.1.343.2.10.3.4.1.50.1.2	Integer	Read-Only
169		a50AdministratorPasswordStatus	1.3.6.1.4.1.343.2.10.3.4.1.50.1.3	Integer	Read-Only
170		a50FrontPanelResetStatus	1.3.6.1.4.1.343.2.10.3.4.1.50.1.4	Integer	Read-Write
171		a52PowerControlRequest	1.3.6.1.4.1.343.2.10.3.4.1.52.1.1	Integer	Read-Write
172		a52TimedPower-onAvailable	1.3.6.1.4.1.343.2.10.3.4.1.52.1.2	Integer	Read-Only
173		a52TimeToNextScheduledPower-on	1.3.6.1.4.1.343.2.10.3.4.1.52.1.3	DmiInteger	Read-Write
174		a54VoltageProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.54.1.1	DmiInteger	Read-Only
175		a54VoltageProbeLocation	1.3.6.1.4.1.343.2.10.3.4.1.54.1.2	Integer	Read-Only
176		a54VoltageProbeDescription	1.3.6.1.4.1.343.2.10.3.4.1.54.1.3	DmiDisplaystring	Read-Only
177		a54VoltageStatus	1.3.6.1.4.1.343.2.10.3.4.1.54.1.4	Integer	Read-Only
178		a54VoltageProbeVoltageLevel	1.3.6.1.4.1.343.2.10.3.4.1.54.1.5	DmiInteger	Read-Only
179		a54MonitoredVoltageNominalLevel	1.3.6.1.4.1.343.2.10.3.4.1.54.1.6	DmiInteger	Read-Only
180		a54MonitoredVoltageNormalMaximum	1.3.6.1.4.1.343.2.10.3.4.1.54.1.7	DmiInteger	Read-Only
181		a54MonitoredVoltageNormalMinimum	1.3.6.1.4.1.343.2.10.3.4.1.54.1.8	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
182		a54VoltageProbeMaximum	1.3.6.1.4.1.343.2.10.3.4.1.54.1.9	DmiInteger	Read-Only
183		a54VoltageProbeMinimum	1.3.6.1.4.1.343.2.10.3.4.1.54.1.10	DmiInteger	Read-Only
184		a54VoltageLevelLowerThreshold-Non-critic	1.3.6.1.4.1.343.2.10.3.4.1.54.1.11	DmiInteger	Read-Write
185		a54VoltageLevelUpperThreshold-Non-critic	1.3.6.1.4.1.343.2.10.3.4.1.54.1.12	DmiInteger	Read-Write
186		a54VoltageLevelLowerThreshold-Critical	1.3.6.1.4.1.343.2.10.3.4.1.54.1.13	DmiInteger	Read-Write
187		a54VoltageLevelUpperThreshold-Critical	1.3.6.1.4.1.343.2.10.3.4.1.54.1.14	DmiInteger	Read-Write
188		a54VoltageLevelLowerThreshold-Non-recove	1.3.6.1.4.1.343.2.10.3.4.1.54.1.15	DmiInteger	Read-Write
189		a54VoltageLevelUpperThreshold-Non-recove	1.3.6.1.4.1.343.2.10.3.4.1.54.1.16	DmiInteger	Read-Write
190		a54VoltageProbeResolution	1.3.6.1.4.1.343.2.10.3.4.1.54.1.17	DmiInteger	Read-Write
191		a54VoltageProbeTolerance	1.3.6.1.4.1.343.2.10.3.4.1.54.1.18	DmiInteger	Read-Write
192		a54VoltageProbeAccuracy	1.3.6.1.4.1.343.2.10.3.4.1.54.1.19	DmiInteger	Read-Write
193		a54FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.54.1.20	DmiInteger	Read-Only
194		a54OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.54.1.21	DmiInteger	Read-Only
195	tTemperatureProbe.eTemperatureProbe	a55TemperatureProbeTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.55.1.1	DmiInteger	Read-Only
196		a55TemperatureProbeLocation	1.3.6.1.4.1.343.2.10.3.4.1.55.1.2	Integer	Read-Only
197		a55TemperatureProbeDescription	1.3.6.1.4.1.343.2.10.3.4.1.55.1.3	DmiDisplaystring	Read-Only
198		a55TemperatureStatus	1.3.6.1.4.1.343.2.10.3.4.1.55.1.4	Integer	Read-Only
199		a55TemperatureProbeTemperatureReading	1.3.6.1.4.1.343.2.10.3.4.1.55.1.5	DmiInteger	Read-Only
200		a55MonitoredTemperatureNominalReading	1.3.6.1.4.1.343.2.10.3.4.1.55.1.6	DmiInteger	Read-Only
201		a55MonitoredTemperatureNormalMaximum	1.3.6.1.4.1.343.2.10.3.4.1.55.1.7	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
202		a55MonitoredTemperatureNormalMinimum	1.3.6.1.4.1.343.2.10.3.4.1.55.1.8	DmiInteger	Read-Only
203		a55TemperatureProbeMaximum	1.3.6.1.4.1.343.2.10.3.4.1.55.1.9	DmiInteger	Read-Only
204		a55TemperatureProbeMinimum	1.3.6.1.4.1.343.2.10.3.4.1.55.1.10	DmiInteger	Read-Only
205		a55TemperatureLowerThreshold-Non-critica	1.3.6.1.4.1.343.2.10.3.4.1.55.1.11	DmiInteger	Read-Write
206		a55TemperatureUpperThreshold-Non-critica	1.3.6.1.4.1.343.2.10.3.4.1.55.1.12	DmiInteger	Read-Write
207		a55TemperatureLowerThreshold-Critical	1.3.6.1.4.1.343.2.10.3.4.1.55.1.13	DmiInteger	Read-Write
208		a55TemperatureUpperThreshold-Critical	1.3.6.1.4.1.343.2.10.3.4.1.55.1.14	DmiInteger	Read-Write
209		a55TemperatureLowerThreshold-Non-recover	1.3.6.1.4.1.343.2.10.3.4.1.55.1.15	DmiInteger	Read-Write
210		a55TemperatureUpperThreshold-Non-recover	1.3.6.1.4.1.343.2.10.3.4.1.55.1.16	DmiInteger	Read-Write
211		a55TemperatureProbeResolution	1.3.6.1.4.1.343.2.10.3.4.1.55.1.17	DmiInteger	Read-Write
212		a55TemperatureProbeTolerance	1.3.6.1.4.1.343.2.10.3.4.1.55.1.18	DmiInteger	Read-Write
213		a55TemperatureProbeAccuracy	1.3.6.1.4.1.343.2.10.3.4.1.55.1.19	DmiInteger	Read-Write
214		a55FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.55.1.20	DmiInteger	Read-Only
215		a55OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.55.1.21	DmiInteger	Read-Only
216	tPhysicalContainerGlobalTable.e PhysicalContainerGlobalTable	a64ContainerOrChassisType	1.3.6.1.4.1.343.2.10.3.4.1.64.1.1	Integer	Read-Only
217		a64AssetTag	1.3.6.1.4.1.343.2.10.3.4.1.64.1.2	DmiDisplaystring	Read-Write
218		a64ChassisLockPresent	1.3.6.1.4.1.343.2.10.3.4.1.64.1.3	Integer	Read-Only
219		a64BootupState	1.3.6.1.4.1.343.2.10.3.4.1.64.1.4	Integer	Read-Only
220		a64PowerState	1.3.6.1.4.1.343.2.10.3.4.1.64.1.5	Integer	Read-Only
221		a64ThermalState	1.3.6.1.4.1.343.2.10.3.4.1.64.1.6	Integer	Read-Only
222		a64FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.64.1.7	DmiInteger	Read-Only
223		a64OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.64.1.8	DmiInteger	Read-Only
224		a64ContainerIndex	1.3.6.1.4.1.343.2.10.3.4.1.64.1.9	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
225		a64ContainerName	1.3.6.1.4.1.343.2.10.3.4.1.64.1.10	DmiDisplaystring	Read-Write
226		a64ContainerLocation	1.3.6.1.4.1.343.2.10.3.4.1.64.1.11	DmiDisplaystring	Read-Write
227		a64ContainerSecurityStatus	1.3.6.1.4.1.343.2.10.3.4.1.64.1.12	Integer	Read-Only
228	tOperatingSystem.eOperatingSystem	a66OperatingSystemIndex	1.3.6.1.4.1.343.2.10.3.4.1.66.1.1	DmiInteger	Read-Only
229		a66OperatingSystemName	1.3.6.1.4.1.343.2.10.3.4.1.66.1.2	DmiDisplaystring	Read-Only
230		a66OperatingSystemVersion	1.3.6.1.4.1.343.2.10.3.4.1.66.1.3	DmiDisplaystring	Read-Only
231		a66PrimaryOperatingSystem	1.3.6.1.4.1.343.2.10.3.4.1.66.1.4	Integer	Read-Only
232		a66OperatingSystemBootDeviceStorageType	1.3.6.1.4.1.343.2.10.3.4.1.66.1.5	Integer	Read-Only
233		a66OperatingSystemBootDeviceIndex	1.3.6.1.4.1.343.2.10.3.4.1.66.1.6	DmiInteger	Read-Only
234		a66OperatingSystemBootPartitionIndex	1.3.6.1.4.1.343.2.10.3.4.1.66.1.7	DmiInteger	Read-Only
235		a66OperatingSystemDescription	1.3.6.1.4.1.343.2.10.3.4.1.66.1.8	DmiDisplaystring	Read-Only
236	tPowerUnitGlobalTable.ePowerUnitGlobalTable	a67PowerUnitIndex	1.3.6.1.4.1.343.2.10.3.4.1.67.1.1	DmiInteger	Read-Only
237		a67PowerUnitRedundancyStatus	1.3.6.1.4.1.343.2.10.3.4.1.67.1.2	Integer	Read-Only
238	tParallelPorts.eParallelPorts	a74ParallelPortIndex	1.3.6.1.4.1.343.2.10.3.4.1.74.1.1	DmiInteger	Read-Only
239		a74ParallelBaseloAddress	1.3.6.1.4.1.343.2.10.3.4.1.74.1.2	DmiInteger64	Read-Only
240		a74IrqUsed	1.3.6.1.4.1.343.2.10.3.4.1.74.1.3	DmiInteger	Read-Only
241		a74LogicalName	1.3.6.1.4.1.343.2.10.3.4.1.74.1.4	DmiDisplaystring	Read-Only
242		a74ConnectorType	1.3.6.1.4.1.343.2.10.3.4.1.74.1.5	Integer	Read-Only
243		a74ConnectorPinout	1.3.6.1.4.1.343.2.10.3.4.1.74.1.6	Integer	Read-Only
244		a74DmaSupport	1.3.6.1.4.1.343.2.10.3.4.1.74.1.7	Integer	Read-Only
245		a74ParallelPortCapabilities	1.3.6.1.4.1.343.2.10.3.4.1.74.1.8	DmiInteger	Read-Only
246		a74OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.74.1.9	DmiInteger	Read-Only
247		a74ParallelPortSecuritySettings	1.3.6.1.4.1.343.2.10.3.4.1.74.1.10	Integer	Read-Only
248	tSerialPorts.eSerialPorts	a75SerialPortIndex	1.3.6.1.4.1.343.2.10.3.4.1.75.1.1	DmiInteger	Read-Only
249		a75SerialBaseloAddress	1.3.6.1.4.1.343.2.10.3.4.1.75.1.2	DmiInteger64	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
250		a75IrqUsed	1.3.6.1.4.1.343.2.10.3.4.1.75.1.3	DmiInteger	Read-Only
251		a75LogicalName	1.3.6.1.4.1.343.2.10.3.4.1.75.1.4	DmiDisplaystring	Read-Only
252		a75ConnectorType	1.3.6.1.4.1.343.2.10.3.4.1.75.1.5	Integer	Read-Only
253		a75MaximumSpeed	1.3.6.1.4.1.343.2.10.3.4.1.75.1.6	DmiInteger	Read-Only
254		a75SerialPortCapabilities	1.3.6.1.4.1.343.2.10.3.4.1.75.1.7	Integer	Read-Only
255		a75OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.75.1.8	DmiInteger	Read-Only
256		a75SerialPortSecuritySettings	1.3.6.1.4.1.343.2.10.3.4.1.75.1.9	Integer	Read-Only
257	tCoolingDevice.eCoolingDevice	a81CoolingDeviceTableIndex	1.3.6.1.4.1.343.2.10.3.4.1.81.1.1	DmiInteger	Read-Only
258		a81FruGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.81.1.2	DmiInteger	Read-Only
259		a81OperationalGroupIndex	1.3.6.1.4.1.343.2.10.3.4.1.81.1.3	DmiInteger	Read-Only
260		a81CoolingUnitIndex	1.3.6.1.4.1.343.2.10.3.4.1.81.1.4	DmiInteger	Read-Only
261		a81CoolingDeviceType	1.3.6.1.4.1.343.2.10.3.4.1.81.1.5		Read-Only
262		a81TemperatureProbeIndex	1.3.6.1.4.1.343.2.10.3.4.1.81.1.6	DmiInteger	Read-Only
263	tEventGenerationForProcessor.e EventGenerationForProcessor.e EventGenerationForProcessor_O V_v1traps_	trap1ForProcessor	1.3.6.1.4.1.343.2.10.3.4.1.100.1.0. 256	Notification Type	
264		Trap2ForProcessor	1.3.6.1.4.1.343.2.10.3.4.1.100.1.0. 256	Notification Type	
265		Trap3ForProcessor	1.3.6.1.4.1.343.2.10.3.4.1.100.1.0. 256	Notification Type	
266		Trap4ForProcessor	1.3.6.1.4.1.343.2.10.3.4.1.100.1.0. 256	Notification Type	
267	tEventGenerationForProcessor.e EventGenerationForProcessor	a100EventType	1.3.6.1.4.1.343.2.10.3.4.1.100.1.1	Integer	Read-Only
268		a100EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.100.1.2	Integer	Read-Only
269		a100EventState-based	1.3.6.1.4.1.343.2.10.3.4.1.100.1.3	Integer	Read-Only
270		a100EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.100.1.4	DmiInteger	Read-Only
271		a100AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.100.1.5	DmiDisplaystring	Read-Only
272		a100EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.100.1.6	Integer	Read-Only
273		a100EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.100.1.7	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
274		a100InstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.100.1.9	Integer	Read-Only
275		a100EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.100.1.10	DmiDisplaystring	Read-Only
276	EventGenerationForPowerSupply.eEventGenerationForPowerSupply.eEventGenerationForPowerSupply_OV_v1traps_	trap1ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.256	Notification Type	
277		Trap2ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.257	Notification Type	
278		Trap3ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.258	Notification Type	
279		Trap4ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.259	Notification Type	
280		Trap5ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.260	Notification Type	
281		Trap6ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.261	Notification Type	
282		Trap7ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.262	Notification Type	
283		Trap8ForPowerSupply	1.3.6.1.4.1.343.2.10.3.4.1.104.1.0.263	Notification Type	
284	tEventGenerationForPowerSupply.eEventGenerationForPowerSupply	a104EventType	1.3.6.1.4.1.343.2.10.3.4.1.104.1.1	Integer	Read-Only
285		a104EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.104.1.2	Integer	Read-Only
286		a104IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.104.1.3	Integer	Read-Only
287		a104EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.104.1.4	DmiInteger	Read-Only
288		a104AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.104.1.5	DmiDisplaystring	Read-Only
289		a104EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.104.1.6	Integer	Read-Only
290		a104EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.104.1.7	Integer	Read-Only
291		a104IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.104.1.9	Integer	Read-Only
292		a104EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.104.1.10	DmiDisplaystring	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
293	tEventGenerationForPhysicalMemory.eEventGenerationForPhysicalMemory.eEventGenerationForPhysicalMemory_OV_v1traps_	trap1ForPhysicalMemory	1.3.6.1.4.1.343.2.10.3.4.1.108.1.0.256	Notification Type	
294		trap2ForPhysicalMemory	1.3.6.1.4.1.343.2.10.3.4.1.108.1.0.257	Notification Type	
295		trap3ForPhysicalMemory	1.3.6.1.4.1.343.2.10.3.4.1.108.1.0.258	Notification Type	
296		trap4ForPhysicalMemory	1.3.6.1.4.1.343.2.10.3.4.1.108.1.0.259	Notification Type	
297		trap5ForPhysicalMemory	1.3.6.1.4.1.343.2.10.3.4.1.108.1.0.260	Notification Type	
298	tEventGenerationForPhysicalMemory.eEventGenerationForPhysicalMemory	a108EventType	1.3.6.1.4.1.343.2.10.3.4.1.108.1.1	Integer	Read-Only
299		a108EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.108.1.2	Integer	Read-Only
300		a108IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.108.1.3	Integer	Read-Only
301		a108EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.108.1.4	DmiInteger	Read-Only
302		a108AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.108.1.5	DmiDisplaystring	Read-Only
303		a108EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.108.1.6	Integer	Read-Only
304		a108EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.108.1.7	Integer	Read-Only
305		a108IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.108.1.9	Integer	Read-Only
306		a108EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.108.1.10	DmiDisplaystring	Read-Only
307	tEventGenerationForVoltageProbe.eEventGenerationForVoltageProbe.eEventGenerationForVoltageProbe_OV_v1traps_	trap1ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.256	Notification Type	
308		Trap3ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.258	Notification Type	
309					
310		trap4ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.259	Notification Type	

S.No	Group	Attribute	OID	Type	Access Privilege
311		Trap5ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.260	Notification Type	
312		Trap6ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.261	Notification Type	
313		Trap7ForVoltageProbe	1.3.6.1.4.1.343.2.10.3.4.1.113.1.0.261	Notification Type	
314	tEventGenerationForVoltageProbe.eEventGenerationForVoltageProbe	a113EventType	1.3.6.1.4.1.343.2.10.3.4.1.113.1.1	Integer	Read-Only
315		a113EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.113.1.2	Integer	Read-Only
316		a113IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.113.1.3	Integer	Read-Only
317		a113EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.113.1.4	DmiInteger	Read-Only
318		a113AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.113.1.5	DmiDisplaystring	Read-Only
319		a113EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.113.1.6	Integer	Read-Only
320		a113EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.113.1.7	Integer	Read-Only
321		a113IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.113.1.9	Integer	Read-Only
322		a113EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.113.1.10	DmiDisplaystring	Read-Only
323	tEventGenerationForTemperatureProbe.eEventGenerationForTemperatureProbe.eEventGenerationForTemperatureProbe_OV_v1traps_	trap1ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.256	Notification Type	
324		Trap2ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.257	Notification Type	
225		Trap3ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.258	Notification Type	
326		Trap4ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.259	Notification Type	
327		Trap5ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.260	Notification Type	
328		Trap6ForTemperatureProbe	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.261	Notification Type	

S.No	Group	Attribute	OID	Type	Access Privilege
329		Trap7ForTemperatureProb	1.3.6.1.4.1.343.2.10.3.4.1.114.1.0.262	Notification Type	
330	tEventGenerationForTemperatureProbe.eEventGenerationForTemperatureProbe	a114EventType	1.3.6.1.4.1.343.2.10.3.4.1.114.1.1	Integer	Read-Only
331		a114EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.114.1.2	Integer	Read-Only
332		a114IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.114.1.3	Integer	Read-Only
333		a114EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.114.1.4	DmiInteger	Read-Only
334		a114AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.114.1.5	DmiDisplaystring	Read-Only
335		a114EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.114.1.6	Integer	Read-Only
336		a114EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.114.1.7	Integer	Read-Only
337		a114IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.114.1.9	Integer	Read-Only
338		a114EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.114.1.10	DmiDisplaystring	Read-Only
339	tEventGenerationForPhysicalContainer.eEventGenerationForPhysicalContainer.eEventGenerationForPhysicalContainer_OV_v1traps	trap1ForPhysicalContainer	1.3.6.1.4.1.343.2.10.3.4.1.116.1.0.6	Notification Type	
340		trap2ForPhysicalContainer	1.3.6.1.4.1.343.2.10.3.4.1.116.1.0.7	Notification Type	
341	tEventGenerationForPhysicalContainer.eEventGenerationForPhysicalContainer	a116EventType	1.3.6.1.4.1.343.2.10.3.4.1.116.1.1	Integer	Read-Only
342		a116EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.116.1.2	Integer	Read-Only
343		a116IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.116.1.3	Integer	Read-Only
344		a116EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.116.1.4	DmiInteger	Read-Only
345		a116AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.116.1.5	DmiDisplaystring	Read-Only
346		a116EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.116.1.6	Integer	Read-Only
347		a116EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.116.1.7	Integer	Read-Only
348		a116IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.116.1.9	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
349		a116EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.116.1.10	DmiDisplaystring	Read-Only
350	tEventGenerationForCoolingDevice.eEventGenerationForCoolingDevice	a140EventType	1.3.6.1.4.1.343.2.10.3.4.1.140.1.1	Integer	Read-Only
351		a140EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.140.1.2	Integer	Read-Only
352		a140IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.140.1.3	Integer	Read-Only
353		a140EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.140.1.4	DmiIntege	Read-Only
354		a140AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.140.1.5	DmiDisplaystring	Read-Only
355		a140EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.140.1.6	Integer	Read-Only
356		a140EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.140.1.7	Integer	Read-Only
357	tEventGenerationForPowerUnit.eEventGenerationForPowerUnit.eEventGenerationForPowerUnit_OV_v1traps_	trap1ForPowerUnit	1.3.6.1.4.1.343.2.10.3.4.1.201.1.0.1	Notification Type	
358		trap2ForPowerUnit	1.3.6.1.4.1.343.2.10.3.4.1.201.1.0.2	Notification Type	
359		trap3ForPowerUnit	1.3.6.1.4.1.343.2.10.3.4.1.201.1.0.3	Notification Type	
360		trap4ForPowerUnit	1.3.6.1.4.1.343.2.10.3.4.1.201.1.0.4	Notification Type	
361		trap5ForPowerUnit	1.3.6.1.4.1.343.2.10.3.4.1.201.1.0.5	Notification Type	
362	tEventGenerationForPowerUnit.eEventGenerationForPowerUnit	a201EventType	1.3.6.1.4.1.343.2.10.3.4.1.201.1.1	Integer	Read-Only
363		a201EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.201.1.2	Integer	Read-Only
364		a201IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.201.1.3	Integer	Read-Only
365		a201EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.201.1.4	DmiInteger	Read-Only
366		a201AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.201.1.5	DmiDisplaystring	Read-Only
367		a201EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.201.1.6	Integer	Read-Only
368		a201EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.201.1.7	Integer	Read-Only
369		a201IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.201.1.9	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
370		a201EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.201.1.10	DmiDisplaystring	Read-Only
371	tEventGenerationForCoolingSensors.eEventGenerationForCoolingSensors.eEventGenerationForCoolingSensors_OV_v1traps_	trap1ForCoolingSensors	1.3.6.1.4.1.343.2.10.3.4.1.202.1.0.256	Notification Type	
372		trap1ForCoolingSensors	1.3.6.1.4.1.343.2.10.3.4.1.202.1.0.257	Notification Type	
373	tEventGenerationForCoolingSensors.eEventGenerationForCoolingSensors	a202EventType	1.3.6.1.4.1.343.2.10.3.4.1.202.1.1	Integer	Read-Only
374		a202EventSeverity	1.3.6.1.4.1.343.2.10.3.4.1.202.1.2	Integer	Read-Only
375		a202IsEventState-based	1.3.6.1.4.1.343.2.10.3.4.1.202.1.3	Integer	Read-Only
376		a202EventStateKey	1.3.6.1.4.1.343.2.10.3.4.1.202.1.4	DmiInteger	Read-Only
377		a202AssociatedGroup	1.3.6.1.4.1.343.2.10.3.4.1.202.1.5	DmiDisplaystring	Read-Only
378		a202EventSystem	1.3.6.1.4.1.343.2.10.3.4.1.202.1.6	Integer	Read-Only
379		a202EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.202.1.7	Integer	Read-Only
380		a202IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.202.1.9	Integer	Read-Only
381		a202EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.202.1.10	DmiDisplaystring	Read-Only
382	tEventGenerationForSystemSlots.eEventGenerationForSystemSlots.eEventGenerationForSystemSlots_OV_v1traps_	trap1ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.1	Notification Type	
383		trap2ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.2	Notification Type	
384		trap3ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.3	Notification Type	
385		trap4ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.4	Notification Type	
386		trap5ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.5	Notification Type	

S.No	Group	Attribute	OID	Type	Access Privilege
387		trap6ForSystemSlots	1.3.6.1.4.1.343.2.10.3.4.1.205.1.0.6	Notification Type	
388		a205EventSubsystem	1.3.6.1.4.1.343.2.10.3.4.1.205.1.7	Integer	Read-Only
389		a205IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.3.4.1.205.1.9	Integer	Read-Only
390		a205EventMessage	1.3.6.1.4.1.343.2.10.3.4.1.205.1.10	DmiDisplaystring	Read-Only
391	tSystemControl.eSystemControl	a1004Selfid	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.1	DmiInteger	Read-Only
392		a1004ResetSystem	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.2	DmiOctetstring	Read-Write
393		a1004TimedResetIncrement	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.3	DmiInteger	Read-Only
394		a1004TimedResetResolution	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.4	DmiInteger	Read-Only
395		a1004TimeUntilSystemReset	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.5	DmiInteger	Read-Write
396		a1004SystemPowerCapabilities	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.6	Integer	Read-Only
397		a1004SystemPowerStatus	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.7	Integer	Read-Only
398		a1004EventLoggingCapability	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.8	Integer	Read-Only
399		a1004WatchdogTimerIncrement	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.9	DmiInteger	Read-Only
400		a1004WatchdogTimerResolution	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.10	DmiInteger	Read-Only
401		a1004WatchdogUpdateInterval	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.11	DmiInteger	Read-Write
402		a1004UseSystemWatchdogFeature	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.12	Integer	Read-Write
403		a1004ResetSystemAfterDelay	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.13	DmiOctetstring	Read-Write

S.No	Group	Attribute	OID	Type	Access Privilege
404		a1004SavePersistentData	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.15	Integer	Read-Write
405		a1004RestoreFactoryDefaults	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.16	DmiOctetstring	Read-Write
406		a1004ShutdownOs	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.17	DmiOctetstring	Read-Write
407		a1004ShutdownOsAndPowerOff	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.18	DmiOctetstring	Read-Write
408		a1004ShutdownOsAndHardwareReset	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.19	DmiOctetstring	Read-Write
409		a1004IssueAHardwareNmi	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.20	DmiOctetstring	Read-Write
410		a1004ImmediatePowerDown	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.21	DmiOctetstring	Read-Write
411		a1004Challenge	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.22	DmiOctetstring	Read-Only
412		a1004VerifyPrivilege	1.3.6.1.4.1.343.2.10.3.4.1.1004.1.23	DmiOctetstring	Read-Write
413		a1005CfmRating	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.7	DmiInteger	Read-Only
414		a1005FanUnits	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.8	Integer	Read-Only
415		a1005MaximumReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.9	DmiInteger	Read-Only
416		a1005MinimumReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.10	DmiInteger	Read-Only
417		a1005CurrentReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.11	DmiInteger	Read-Only
418		a1005SensorAccuracy	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.13	DmiInteger	Read-Write
419		a1005SensorTolerancePlus	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.14	DmiInteger	Read-Write

S.No	Group	Attribute	OID	Type	Access Privilege
420		a1005SensorToleranceMinus	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.15	DmiInteger	Read-Write
421		a1005Non-criticalThreshold	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.16	DmiInteger	Read-Write
422		a1005CriticalThreshold	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.17	DmiInteger	Read-Write
423		a1005Non-recoverableThreshold	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.18	DmiInteger	Read-Write
424		a1005CoolingSensorDescription	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.19	DmiDisplaystring	Read-Only
425		a1005NominalReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.21	DmiInteger	Read-Only
426		a1005LowestNormalReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.22	DmiInteger	Read-Only
427		a1005HighestNormalReading	1.3.6.1.4.1.343.2.10.3.4.1.1005.1.23	DmiInteger	Read-Only
428	tSystemEventLog.eSystemEventLog	a1006Selfid	1.3.6.1.4.1.343.2.10.3.4.1.1006.1.1	DmiInteger	Read-Only
429		a1006Timestamp	1.3.6.1.4.1.343.2.10.3.4.1.1006.1.2	DmiDate	Read-Only
430		a1006RecordType	1.3.6.1.4.1.343.2.10.3.4.1.1006.1.3	DmiInteger	Read-Only
431		a1006RecordLength	1.3.6.1.4.1.343.2.10.3.4.1.1006.1.4	DmiInteger	Read-Only
432		a1006RecordData	1.3.6.1.4.1.343.2.10.3.4.1.1006.1.5	DmiOctetstring	Read-Only
433	tPciHotplugDevice.ePciHotplugDevice	a1008PciHotplugDeviceIndex	1.3.6.1.4.1.343.2.10.3.4.1.1008.1.1	DmiInteger	
434		a1008PciHotplugSlotNumber	1.3.6.1.4.1.343.2.10.3.4.1.1008.1.2	DmiInteger	Read-Only
435		a1008DeviceManufacturer	1.3.6.1.4.1.343.2.10.3.4.1.1008.1.3	DmiDisplaystring	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
436		a1008DeviceType	1.3.6.1.4.1.343.2.10.3.4.1.1008.1.4	DmiDisplaystring	Read-Only
437		a1008DeviceRevision	1.3.6.1.4.1.343.2.10.3.4.1.1008.1.5	DmiDisplaystring	Read-Only
438	tPagingConfig.ePagingConfig	a1010PagingSupported	1.3.6.1.4.1.343.2.10.3.4.1.1010.1.1	Integer	Read-Only
439		a1010DefaultPepString	1.3.6.1.4.1.343.2.10.3.4.1.1010.1.2	DmiDisplaystring	Read-Write
440		a1010GlobalPaging	1.3.6.1.4.1.343.2.10.3.4.1.1010.1.3	Integer	Read-Write
441	tLocalPagingConfig.eLocalPagingConfig	a1011PepString1	1.3.6.1.4.1.343.2.10.3.4.1.1011.1.1	DmiDisplaystring	Read-Write
442		a1011PepString2	1.3.6.1.4.1.343.2.10.3.4.1.1011.1.2	DmiDisplaystring	Read-Write
443		a1011RepeatCount	1.3.6.1.4.1.343.2.10.3.4.1.1011.1.3	DmiInteger	Read-Write
444		a1011RepeatInterval	1.3.6.1.4.1.343.2.10.3.4.1.1011.1.4	DmiInteger	Read-Write
445		a1011TestString	1.3.6.1.4.1.343.2.10.3.4.1.1011.1.5	DmiDisplaystring	Read-Write
446	tEmailConfig.eEmailConfig	a1012SmtServer	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.1	DmiDisplaystring	Read-Write
447		a1012EmailFromAddress	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.2	DmiDisplaystring	Read-Write
448		a1012EmailToAddress	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.3	DmiDisplaystring	Read-Write
449		a1012EmailSubject	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.4	DmiDisplaystring	Read-Write
450		a1012EmailMessage	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.5	DmiDisplaystring	Read-Write
451		a1012TestEmail	1.3.6.1.4.1.343.2.10.3.4.1.1012.1.6	DmiInteger	Read-Write

S.No	Group	Attribute	OID	Type	Access Privilege
452	tDpcDiscovery.eDpcDiscovery	a9000DpcDialNumberString	1.3.6.1.4.1.343.2.10.3.4.1.9000.1.1	DmiDisplaystring	Read-Write
453		a9000DpcServicePartitionPresenceFlag	1.3.6.1.4.1.343.2.10.3.4.1.9000.1.2	Integer	Read-Only
454		a9000ScanServicePartitionFlag	1.3.6.1.4.1.343.2.10.3.4.1.9000.1.3	Integer	Read-Write
455		a9000BootServicePartitionFlag	1.3.6.1.4.1.343.2.10.3.4.1.9000.1.4	Integer	Read-Write

Linux

The following table contains supported dmtf groups and MIB OIDs in mapbase4.mib for Linux

Intel

Major group : private.enterprises.intel.products.server-management: (Intel group)

S.No	Group	Attribute	OID	Type	Access Privilege
1	dmtfGroups.tSystemControl	Selfid	1.3.6.1.4.1.343.2.10.7.2.1.1	DmiInteger	Read-Only
2		ResetSystem	1.3.6.1.4.1.343.2.10.7.2.1.2	DmiOctetstring	Read-Write
3		TimedResetIncrement	1.3.6.1.4.1.343.2.10.7.2.1.3	DmiInteger	Read-Only
4		TimedResetResolution	1.3.6.1.4.1.343.2.10.7.2.1.4	DmiInteger	Read-Only
5		TimeUntilSystemReset	1.3.6.1.4.1.343.2.10.7.2.1.5	DmiInteger	Read-Write
6		SystemPowerCapabilities	1.3.6.1.4.1.343.2.10.7.2.1.6	Integer	Read-Only
7		SystemPowerStatus	1.3.6.1.4.1.343.2.10.7.2.1.7	Integer	Read-Only
8		EventLoggingCapability	1.3.6.1.4.1.343.2.10.7.2.1.8	Integer	Read-Only
9		WatchdogTimerIncrement	1.3.6.1.4.1.343.2.10.7.2.1.9	DmiInteger	Read-Only
10		WatchdogTimerResolution	1.3.6.1.4.1.343.2.10.7.2.1.10	DmiInteger	Read-Only
11		WatchdogUpdateInterval	1.3.6.1.4.1.343.2.10.7.2.1.11	DmiInteger	Read-Write
12		UseSystemWatchdogFeature	1.3.6.1.4.1.343.2.10.7.2.1.12	Integer	Read-Write
13		ResetSystemAfterDelay	1.3.6.1.4.1.343.2.10.7.2.1.13	DmiOctetstring	Read-Write
14		SavePersistentData	1.3.6.1.4.1.343.2.10.7.2.1.15	Integer	Read-Write
15		RestoreFactoryDefaults	1.3.6.1.4.1.343.2.10.7.2.1.16	DmiOctetstring	Read-Write
16		ShutdownOs	1.3.6.1.4.1.343.2.10.7.2.1.17	DmiOctetstring	Read-Write
17		ShutdownOsAndPowerOff	1.3.6.1.4.1.343.2.10.7.2.1.18	DmiOctetstring	Read-Write
18		ShutdownOsAndHardwareReset	1.3.6.1.4.1.343.2.10.7.2.1.19	DmiOctetstring	Read-Write
19		IssueAHardwareNmi	1.3.6.1.4.1.343.2.10.7.2.1.20	DmiOctetstring	Read-Write
20		ImmediatePowerDown	1.3.6.1.4.1.343.2.10.7.2.1.21	DmiOctetstring	Read-Write
21		Challenge	1.3.6.1.4.1.343.2.10.7.2.1.22	DmiOctetstring	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
22		VerifyPrivilege	1.3.6.1.4.1.343.2.10.7.2.1.23	DmiOctetstring	Read-Write
23	tCoolingSensors.tCoolingSensorsTraps	notification1ForCoolingSensors	1.3.6.1.4.1.343.2.10.7.3.0.256	Notification Type	
24		notification2ForCoolingSensors	1.3.6.1.4.1.343.2.10.7.3.0.257	Notification Type	
25	tCoolingSensors.eCoolingSensors	Selfid	1.3.6.1.4.1.343.2.10.7.3.1.1	DmiInteger	Read-Only
26		FruGroupIndex	1.3.6.1.4.1.343.2.10.7.3.1.2	DmiInteger	Read-Only
27		OperationalGroupIndex	1.3.6.1.4.1.343.2.10.7.3.1.3	DmiInteger	Read-Only
28		CoolingDeviceType	1.3.6.1.4.1.343.2.10.7.3.1.6	Integer	Read-Only
29		CfmRating	1.3.6.1.4.1.343.2.10.7.3.1.7	DmiInteger	Read-Only
30		FanUnits	1.3.6.1.4.1.343.2.10.7.3.1.8	Integer	Read-Only
31		MaximumReading	1.3.6.1.4.1.343.2.10.7.3.1.9	DmiInteger	Read-Only
32		MinimumReading	1.3.6.1.4.1.343.2.10.7.3.1.10	DmiInteger	Read-Only
33		CurrentReading	1.3.6.1.4.1.343.2.10.7.3.1.11	DmiInteger	Read-Only
34		SensorAccuracy	1.3.6.1.4.1.343.2.10.7.3.1.13	DmiInteger	Read-Write
35		SensorTolerancePlus	1.3.6.1.4.1.343.2.10.7.3.1.14	DmiInteger	Read-Write
36		SensorToleranceMinus	1.3.6.1.4.1.343.2.10.7.3.1.15	DmiInteger	Read-Write
37		Non-criticalThreshold	1.3.6.1.4.1.343.2.10.7.3.1.16	DmiInteger	Read-Write
38		CriticalThreshold	1.3.6.1.4.1.343.2.10.7.3.1.17	DmiInteger	Read-Write
39		Non-recoverableThreshold	1.3.6.1.4.1.343.2.10.7.3.1.18	DmiInteger	Read-Write
40		CoolingSensorDescription	1.3.6.1.4.1.343.2.10.7.3.1.19	DmiDisplaystring	Read-Only
41		NominalReading	1.3.6.1.4.1.343.2.10.7.3.1.21	DmiInteger	Read-Only
42		LowestNormalReading	1.3.6.1.4.1.343.2.10.7.3.1.22	DmiInteger	Read-Only
43		HighestNormalReading	1.3.6.1.4.1.343.2.10.7.3.1.23	DmiInteger	Read-Only
44		RecordType	1.3.6.1.4.1.343.2.10.7.4.1.3	DmiInteger	Read-Only
45		RecordLength	1.3.6.1.4.1.343.2.10.7.4.1.4	DmiInteger	Read-Only
46		RecordData	1.3.6.1.4.1.343.2.10.7.4.1.5	DmiOctetstring	Read-Only
47	tPagingConfig.ePagingConfig	PagingSupported	1.3.6.1.4.1.343.2.10.7.5.1.1	Integer	Read-Only
48		DefaultPepString	1.3.6.1.4.1.343.2.10.7.5.1.2	DmiDisplaystring	Read-Write
49		GlobalPaging	1.3.6.1.4.1.343.2.10.7.5.1.3	Integer	Read-Write

S.No	Group	Attribute	OID	Type	Access Privilege
50		PepStringSize	1.3.6.1.4.1.343.2.10.7.5.1.4	DmiInteger	Read-Only
51		TestPage	1.3.6.1.4.1.343.2.10.7.5.1.5	DmiInteger	Read-Write
52		IssuePaging	1.3.6.1.4.1.343.2.10.7.5.1.6	Integer	Read-Write
53	tLocalPagingConfig.eLocalPagingConfig	PepString1	1.3.6.1.4.1.343.2.10.7.6.1.1	DmiDisplaystring	Read-Write
54		PepString2	1.3.6.1.4.1.343.2.10.7.6.1.2	DmiDisplaystring	Read-Write
55		RepeatCount	1.3.6.1.4.1.343.2.10.7.6.1.3	DmiInteger	Read-Write
56		RepeatInterval	1.3.6.1.4.1.343.2.10.7.6.1.4	DmiInteger	Read-Write
57		TestString	1.3.6.1.4.1.343.2.10.7.6.1.5	DmiDisplaystring	Read-Write
58	tEmailConfig.eEmailConfig	SmtServer	1.3.6.1.4.1.343.2.10.7.7.1.1	DmiDisplaystring	Read-Write
59		EmailFromAddress	1.3.6.1.4.1.343.2.10.7.7.1.2	DmiDisplaystring	Read-Write
60		EmailToAddress	1.3.6.1.4.1.343.2.10.7.7.1.3	DmiDisplaystring	Read-Write
61		EmailSubject	1.3.6.1.4.1.343.2.10.7.7.1.4	DmiDisplaystring	Read-Write
62		EmailMessage	1.3.6.1.4.1.343.2.10.7.7.1.5	DmiDisplaystring	Read-Write
63		TestEmail	1.3.6.1.4.1.343.2.10.7.7.1.6	DmiInteger	Read-Write
64	tDpcDiscovery.eDpcDiscovery	DpcDialNumberString	1.3.6.1.4.1.343.2.10.7.17.1.1	DmiDisplaystring	Read-Write
65		DpcServicePartitionPresenceFlag	1.3.6.1.4.1.343.2.10.7.17.1.2	Integer	Read-Only
66		ScanServicePartitionFlag	1.3.6.1.4.1.343.2.10.7.17.1.3	Integer	Read-Write
67		BootServicePartitionFlag	1.3.6.1.4.1.343.2.10.7.17.1.4	Integer	Read-Write
68	tPciHotplugDevice.ePciHotplugDevice	PciHotplugDeviceIndex	1.3.6.1.4.1.343.2.10.7.18.1.1	DmiInteger	Read-Only
69		PciHotplugSlotNumber	1.3.6.1.4.1.343.2.10.7.18.1.2	DmiInteger	Read-Only
70		DeviceManufacturer	1.3.6.1.4.1.343.2.10.7.18.1.3	DmiDisplaystring	Read-Only
71		DeviceType	1.3.6.1.4.1.343.2.10.7.18.1.4	DmiDisplaystring	Read-Only
72		DeviceRevision	1.3.6.1.4.1.343.2.10.7.18.1.5	DmiDisplaystring	Read-Only
73	tEventGenerationForCoolingSensors.eEventGenerationForCoolingSensors	EventType	1.3.6.1.4.1.343.2.10.7.202.1.1	Integer	Read-Only
74		EventSeverity	1.3.6.1.4.1.343.2.10.7.202.1.2	Integer	Read-Only
75		sEventState-based	1.3.6.1.4.1.343.2.10.7.202.1.3	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
76		EventStateKey	1.3.6.1.4.1.343.2.10.7.202.1.4	DmiInteger	Read-Only
77		AssociatedGroup	1.3.6.1.4.1.343.2.10.7.202.1.5	DmiDisplaystring	Read-Only
78		EventSystem	1.3.6.1.4.1.343.2.10.7.202.1.6	Integer	Read-Only
79		EventSubsystem	1.3.6.1.4.1.343.2.10.7.202.1.7	Integer	Read-Only
80		IsInstanceDataPresent	1.3.6.1.4.1.343.2.10.7.202.1.9	Integer	Read-Only
81		EventMessage	1.3.6.1.4.1.343.2.10.7.202.1.10	DmiDisplaystring	Read-Only

DMTF

Major group : enterprises.dmtf.dmtfStdMifs.mapperdmtfGroups: (dmtf group)

S.No	Group	Attribute	OID	Type	Access Privilege
1	tGeneralInformation.eGeneralInformation	SystemName	1.3.6.1.4.1.412.2.4.1.1.1	DmiDisplaystring	Read-Write
2		SystemLocation	1.3.6.1.4.1.412.2.4.1.1.2	DmiDisplaystring	Read-Write
3		SystemPrimaryUserName	1.3.6.1.4.1.412.2.4.1.1.3	DmiDisplaystring	Read-Write
4		SystemPrimaryUserPhone	1.3.6.1.4.1.412.2.4.1.1.4	DmiDisplaystring	Read-Write
5		SystemBootupTime	1.3.6.1.4.1.412.2.4.1.1.5	DmiDate	Read-Only
6		SystemDateTime	1.3.6.1.4.1.412.2.4.1.1.6	DmiDate	Read-Write
7	tOperatingSystem.eOperatingSystem	OperatingSystemIndex	1.3.6.1.4.1.412.2.4.2.1.1	DmiInteger	Read-Only
8		OperatingSystemName	1.3.6.1.4.1.412.2.4.2.1.2	DmiDisplaystring	Read-Only
9		OperatingSystemVersion	1.3.6.1.4.1.412.2.4.2.1.3	DmiDisplaystring	Read-Only
10		PrimaryOperatingSystem	1.3.6.1.4.1.412.2.4.2.1.4	Intege	Read-Only
11		OperatingSystemBootDeviceStorage Type	1.3.6.1.4.1.412.2.4.2.1.5	Intege	Read-Only
12		OperatingSystemBootDeviceIndex	1.3.6.1.4.1.412.2.4.2.1.6	DmiInteger	Read-Only
13		OperatingSystemBootPartitionIndex	1.3.6.1.4.1.412.2.4.2.1.7	DmiInteger	Read-Only
14		OperatingSystemDescription	1.3.6.1.4.1.412.2.4.2.1.8	DmiDisplaystring	Read-Only
15	tSystemBios.eSystemBios	BiosIndex	1.3.6.1.4.1.412.2.4.3.1.1	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
16		BiosManufacturer	1.3.6.1.4.1.412.2.4.3.1.2	DmiDisplaystring	Read-Only
17		BiosVersion	1.3.6.1.4.1.412.2.4.3.1.3	DmiDisplaystring	Read-Only
18		BiosRomSize	1.3.6.1.4.1.412.2.4.3.1.4	DmiInteger	Read-Only
19		BiosStartingAddress	1.3.6.1.4.1.412.2.4.3.1.5	DmiInteger64	Read-Only
20		BiosStartingAddress	1.3.6.1.4.1.412.2.4.3.1.6	DmiInteger64	Read-Only
21		BiosLoaderVersion	1.3.6.1.4.1.412.2.4.3.1.7	DmiDisplaystring	Read-Only
22		BiosReleaseDate	1.3.6.1.4.1.412.2.4.3.1.8	DmiDate	Read-Only
23		PrimaryBios	1.3.6.1.4.1.412.2.4.3.1.9	Integer	Read-Only
24	TsystemBiosCharacteristic s.eSystemBiosCharacteristi cs	BiosCharacteristicIndex	1.3.6.1.4.1.412.2.4.4.1.1	DmiInteger	Read-Only
25		BiosNumber	1.3.6.1.4.1.412.2.4.4.1.2	DmiInteger	Read-Only
26		BiosCharacteristic	1.3.6.1.4.1.412.2.4.4.1.3	Integer	Read-Only
27		BiosCharacteristicDescription	1.3.6.1.4.1.412.2.4.4.1.4	DmiDisplaystring	Read-Only
28	tProcessor.tProcessorTrap s	notification1ForProcessor	1.3.6.1.4.1.412.2.4.5.0.256	Notification Type	
29		Notification2ForProcessor	1.3.6.1.4.1.412.2.4.5.0.257	Notification Type	
30		Notification3ForProcessor	1.3.6.1.4.1.412.2.4.5.0.258	Notification Type	
31		Notification4ForProcessor	1.3.6.1.4.1.412.2.4.5.0.259	Notification Type	
32	tProcessor.eProcessor	a6ProcessorIndex	1.3.6.1.4.1.412.2.4.5.1.1	DmiInteger	
33		ProcessorType	1.3.6.1.4.1.412.2.4.5.1.2	Integer	
34		ProcessorFamily	1.3.6.1.4.1.412.2.4.5.1.3	Integer	
35		ProcessorVersionInformation	1.3.6.1.4.1.412.2.4.5.1.4	DmiDisplaystring	
36		MaximumSpeed	1.3.6.1.4.1.412.2.4.5.1.5	DmiInteger	
37		CurrentSpeed	1.3.6.1.4.1.412.2.4.5.1.6	DmiInteger	
38		ProcessorUpgrade	1.3.6.1.4.1.412.2.4.5.1.7	Integer	
39		FruGroupIndex	1.3.6.1.4.1.412.2.4.5.1.8	DmiInteger	
40		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.5.1.9	DmiInteger	
41		Level1CacheIndex	1.3.6.1.4.1.412.2.4.5.1.10	DmiInteger	
42		Level2CacheIndex	1.3.6.1.4.1.412.2.4.5.1.11	DmiInteger	
43		Level3CacheIndex	1.3.6.1.4.1.412.2.4.5.1.12	DmiInteger	

S.No	Group	Attribute	OID	Type	Access Privilege
44		Status	1.3.6.1.4.1.412.2.4.5.1.13	Integer	
45	tMotherboard.eMotherboard	NumberOfExpansionSlots	1.3.6.1.4.1.412.2.4.6.1.1	DmiInteger	Read-Only
46		FruGroupIndex	1.3.6.1.4.1.412.2.4.6.1.2	DmiInteger	Read-Only
47		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.6.1.3	DmiInteger	Read-Only
48	tSystemCache.eSystemCache	SystemCacheIndex	1.3.6.1.4.1.412.2.4.9.1.1	DmiInteger	Read-Only
49		SystemCacheLevel	1.3.6.1.4.1.412.2.4.9.1.2	Integer	Read-Only
50		SystemCacheSpeed	1.3.6.1.4.1.412.2.4.9.1.3	DmiInteger	Read-Only
51		SystemCacheSize	1.3.6.1.4.1.412.2.4.9.1.4	DmiInteger	Read-Only
52		SystemCacheWritePolicy	1.3.6.1.4.1.412.2.4.9.1.5	Integer	Read-Only
53		SystemCacheErrorCorrection	1.3.6.1.4.1.412.2.4.9.1.6	Integer	Read-Only
54		FruGroupIndex	1.3.6.1.4.1.412.2.4.9.1.7	DmiInteger	Read-Only
55		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.9.1.8	DmiInteger	Read-Only
56		SystemCacheType	1.3.6.1.4.1.412.2.4.9.1.9	Integer	Read-Only
57	tParallelPorts.eParallelPorts	ParallelPortIndex	1.3.6.1.4.1.412.2.4.10.1.1	DmiInteger	
58		ParallelBaseIoAddress	1.3.6.1.4.1.412.2.4.10.1.2	DmiInteger64	
59		IrqUsed	1.3.6.1.4.1.412.2.4.10.1.3	DmiInteger	
60		LogicalName	1.3.6.1.4.1.412.2.4.10.1.4	DmiInteger64	
61		ConnectorType	1.3.6.1.4.1.412.2.4.10.1.5	Integer	
62		ConnectorPinout	1.3.6.1.4.1.412.2.4.10.1.6	Integer	
63		DmaSupport	1.3.6.1.4.1.412.2.4.10.1.7	Integer	
64		ParallelPortCapabilities	1.3.6.1.4.1.412.2.4.10.1.8	DmiInteger	
65		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.10.1.9	DmiInteger	
66		ParallelPortSecuritySettings	1.3.6.1.4.1.412.2.4.10.1.10	Integer	
67	tSerialPorts.eSerialPorts	SerialPortIndex	1.3.6.1.4.1.412.2.4.11.1.1	DmiInteger	
68		SerialBaseIoAddress	1.3.6.1.4.1.412.2.4.11.1.2	DmiInteger64	
69		IrqUsed	1.3.6.1.4.1.412.2.4.11.1.3	DmiInteger	
70		LogicalName	1.3.6.1.4.1.412.2.4.11.1.4	DmiDisplaystring	
71		ConnectorType	1.3.6.1.4.1.412.2.4.11.1.5	Integer	

S.No	Group	Attribute	OID	Type	Access Privilege
72		MaximumSpeed	1.3.6.1.4.1.412.2.4.11.1.6	DmiInteger	
73		SerialPortCapabilities	1.3.6.1.4.1.412.2.4.11.1.7	Integer	
74		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.11.1.8	DmiInteger	
75		SerialPortSecuritySettings	1.3.6.1.4.1.412.2.4.11.1.9	Integer	
76	tPowerSupply.tPowerSupply Traps	notification1ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.256	Notification Type	
77		notification2ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.257	Notification Type	
78		notification3ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.258	Notification Type	
79		notification4ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.259	Notification Type	
80		notification5ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.260	Notification Type	
81		notification6ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.261	Notification Type	
82		notification7ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.262	Notification Type	
83		notification8ForPowerSupply	1.3.6.1.4.1.412.2.4.16.0.263	Notification Type	
84	tPowerSupply.ePowerSupply	PowerSupplyIndex	1.3.6.1.4.1.412.2.4.16.1.1	DmiInteger	Read-Only
85		FruGroupIndex	1.3.6.1.4.1.412.2.4.16.1.2	DmiInteger	Read-Only
86		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.16.1.3	DmiInteger	Read-Only
87		PowerUnitIndex	1.3.6.1.4.1.412.2.4.16.1.4	DmiInteger	Read-Only
88		PowerSupplyType	1.3.6.1.4.1.412.2.4.16.1.5	Integer	Read-Only
89		InputVoltageCapabilityDescription	1.3.6.1.4.1.412.2.4.16.1.6	DmiDisplaystring	Read-Only
90		Range1InputVoltageLow	1.3.6.1.4.1.412.2.4.16.1.7	DmiInteger	Read-Only
91		Range1InputVoltageHigh	1.3.6.1.4.1.412.2.4.16.1.8	DmiInteger	Read-Only
92		Range1VoltageProbeIndex	1.3.6.1.4.1.412.2.4.16.1.9	DmiInteger	Read-Only
93		Range1ElectricalCurrentProbeIndex	1.3.6.1.4.1.412.2.4.16.1.10	DmiInteger	Read-Only
94		Range2InputVoltageLow	1.3.6.1.4.1.412.2.4.16.1.11	DmiInteger	Read-Only
95		Range2InputVoltageHigh	1.3.6.1.4.1.412.2.4.16.1.12	DmiInteger	Read-Only
96		Range2VoltageProbeIndex	1.3.6.1.4.1.412.2.4.16.1.13	DmiInteger	Read-Only
97		Range2CurrentProbeIndex	1.3.6.1.4.1.412.2.4.16.1.14	DmiInteger	Read-Only
98		ActiveInputVoltageRange	1.3.6.1.4.1.412.2.4.16.1.15	Integer	Read-Only
99		InputVoltageRangeSwitching	1.3.6.1.4.1.412.2.4.16.1.16	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
100		Range1InputFrequencyLow	1.3.6.1.4.1.412.2.4.16.1.17	DmiInteger	Read-Only
101		Range1InputFrequencyHigh	1.3.6.1.4.1.412.2.4.16.1.18	DmiInteger	Read-Only
102		Range2InputFrequencyLow	1.3.6.1.4.1.412.2.4.16.1.19	DmiInteger	Read-Only
103		Range2InputFrequencyHigh	1.3.6.1.4.1.412.2.4.16.1.20	DmiInteger	Read-Only
104		TotalOutputPower	1.3.6.1.4.1.412.2.4.16.1.21	DmiInteger	Read-Only
105	tCoolingDevice.eCoolingDevice	CoolingDeviceTableIndex	1.3.6.1.4.1.412.2.4.17.1.1	DmiInteger	Read-Only
106		FruGroupIndex	1.3.6.1.4.1.412.2.4.17.1.2	DmiInteger	Read-Only
107		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.17.1.3	DmiInteger	Read-Only
108		CoolingUnitIndex	1.3.6.1.4.1.412.2.4.17.1.4	DmiInteger	Read-Only
109		CoolingDeviceType	1.3.6.1.4.1.412.2.4.17.1.5	Integer	Read-Only
110		TemperatureProbeIndex	1.3.6.1.4.1.412.2.4.17.1.6	DmiInteger	Read-Only
111	tSystemSlots.tSystemSlotsTraps	notification1ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.1	Notification Type	
112		notification2ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.2	Notification Type	
113		notification3ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.3	Notification Type	
114		notification4ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.4	Notification Type	
115		notification5ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.5	Notification Type	
116		notification6ForSystemSlots	1.3.6.1.4.1.412.2.4.18.0.6	Notification Type	
117	tSystemSlots.eSystemSlots	SlotIndex	1.3.6.1.4.1.412.2.4.18.1.1	DmiInteger	Read-Only
118		SlotType	1.3.6.1.4.1.412.2.4.18.1.2	DmiInteger64	Read-Only
119		SlotWidth	1.3.6.1.4.1.412.2.4.18.1.3	Integer	Read-Only
120		CurrentUsage	1.3.6.1.4.1.412.2.4.18.1.4	Integer	Read-Only
121		SlotDescription	1.3.6.1.4.1.412.2.4.18.1.5	DmiDisplaystring	Read-Only
122		SlotCategory	1.3.6.1.4.1.412.2.4.18.1.6	Integer	Read-Only
123		VirtualSlot	1.3.6.1.4.1.412.2.4.18.1.7	Integer	Read-Only
124		ResourceUserId	1.3.6.1.4.1.412.2.4.18.1.8	DmiInteger	Read-Only
125		VccMixedVoltageSupport	1.3.6.1.4.1.412.2.4.18.1.9	DmiInteger64	Read-Only
126		VppMixedVoltageSupport	1.3.6.1.4.1.412.2.4.18.1.10	DmiInteger64	Read-Only
127		SlotThermalRating	1.3.6.1.4.1.412.2.4.18.1.11	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
128		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.18.1.12	DmiInteger	Read-Only
129		SlotPowerState	1.3.6.1.4.1.412.2.4.18.1.13	Integer	Read-Only
130		SlotFaultState	1.3.6.1.4.1.412.2.4.18.1.14	Integer	Read-Only
131		SlotSwitchStatus	1.3.6.1.4.1.412.2.4.18.1.15	Integer	Read-Only
132	tFieldReplaceableUnit.eFieldReplaceableUnit	FruIndex	1.3.6.1.4.1.412.2.4.29.1.1	DmiInteger	Read-Only
133		DeviceGroupIndex	1.3.6.1.4.1.412.2.4.29.1.2	DmiInteger	Read-Only
134		Description	1.3.6.1.4.1.412.2.4.29.1.3	DmiDisplaystring	Read-Only
135		Manufacturer	1.3.6.1.4.1.412.2.4.29.1.4	DmiDisplaystring	Read-Only
136		Model	1.3.6.1.4.1.412.2.4.29.1.5	DmiDisplaystring	Read-Only
137		PartNumber	1.3.6.1.4.1.412.2.4.29.1.6	DmiDisplaystring	Read-Only
138		FruSerialNumber	1.3.6.1.4.1.412.2.4.29.1.7	DmiDisplaystring	Read-Only
139		RevisionLevel	1.3.6.1.4.1.412.2.4.29.1.8	DmiDisplaystring	Read-Only
140		WarrantyStartDate	1.3.6.1.4.1.412.2.4.29.1.9	DmiDate	Read-Only
141		WarrantyDuration	1.3.6.1.4.1.412.2.4.29.1.10	DmiInteger	Read-Only
142		SupportPhoneNumber	1.3.6.1.4.1.412.2.4.29.1.11	DmiDisplaystring	Read-Only
143		FruInternetUniformResourceLocator	1.3.6.1.4.1.412.2.4.29.1.12	DmiDisplaystring	Read-Only
144	tOperationalState.eOperationalState	OperationalStateInstanceIndex	1.3.6.1.4.1.412.2.4.30.1.1	DmiInteger	Read-Only
145		DeviceGroupIndex	1.3.6.1.4.1.412.2.4.30.1.2	DmiInteger	Read-Only
146		OperationalStatus	1.3.6.1.4.1.412.2.4.30.1.3	Integer	Read-Only
147		UsageState	1.3.6.1.4.1.412.2.4.30.1.4	Integer	Read-Only
148		AvailabilityStatus	1.3.6.1.4.1.412.2.4.30.1.5	Integer	Read-Only
149		AdministrativeState	1.3.6.1.4.1.412.2.4.30.1.6	Integer	Read-Only
150		FatalErrorCount	1.3.6.1.4.1.412.2.4.30.1.7	DmiCounter	Read-Only
151		MajorErrorCount	1.3.6.1.4.1.412.2.4.30.1.8	DmiCounter	Read-Only
152		WarningErrorCount	1.3.6.1.4.1.412.2.4.30.1.9	DmiCounter	Read-Only
153		CurrentErrorStatus	1.3.6.1.4.1.412.2.4.30.1.10	Integer	Read-Only
154		DevicePredictedFailureStatus	1.3.6.1.4.1.412.2.4.30.1.11	Integer	Read-Only
155	tPhysicalMemoryArray.tPhysicalMemoryArrayTraps	notification1ForPhysicalMemory	1.3.6.1.4.1.412.2.4.33.0.256	Notification Type	

S.No	Group	Attribute	OID	Type	Access Privilege
156		notification2ForPhysicalMemory	1.3.6.1.4.1.412.2.4.33.0.257	Notification Type	
157		notification3ForPhysicalMemory	1.3.6.1.4.1.412.2.4.33.0.258	Notification Type	
158		notification4ForPhysicalMemory	1.3.6.1.4.1.412.2.4.33.0.259	Notification Type	
159		notification5ForPhysicalMemory	1.3.6.1.4.1.412.2.4.33.0.260	Notification Type	
160	tPhysicalMemoryArray.ePhysicalMemoryArray	MemoryArrayTableIndex	1.3.6.1.4.1.412.2.4.33.1.1	DmiInteger	Read-Only
161		MemoryArrayLocation	1.3.6.1.4.1.412.2.4.33.1.2	Integer	Read-Only
162		MemoryArrayUse	1.3.6.1.4.1.412.2.4.33.1.3	Integer	Read-Only
163		MaximumMemoryCapacity	1.3.6.1.4.1.412.2.4.33.1.4	DmiInteger	Read-Only
164		NumberOfMemoryDeviceSockets	1.3.6.1.4.1.412.2.4.33.1.5	DmiInteger	Read-Only
165		NumberOfMemoryDeviceSocketsUsed	1.3.6.1.4.1.412.2.4.33.1.6	DmiInteger	Read-Only
166		MemoryErrorCorrection	1.3.6.1.4.1.412.2.4.33.1.7	Integer	Read-Only
167		ArrayErrorType	1.3.6.1.4.1.412.2.4.33.1.8	Integer	Read-Only
168		LastErrorUpdate	1.3.6.1.4.1.412.2.4.33.1.9	Integer	Read-Only
169		ErrorOperation	1.3.6.1.4.1.412.2.4.33.1.10	Integer	Read-Only
170		ErrorDataSize	1.3.6.1.4.1.412.2.4.33.1.11	DmiInteger	Read-Only
171		ErrorData	1.3.6.1.4.1.412.2.4.33.1.12	DmiOctetstring	Read-Only
172		VendorSyndrome	1.3.6.1.4.1.412.2.4.33.1.13	DmiOctetstring	Read-Only
173		ErrorAddress	1.3.6.1.4.1.412.2.4.33.1.14	DmiInteger64	Read-Only
174		ErrorResolution	1.3.6.1.4.1.412.2.4.33.1.15	DmiInteger	Read-Only
175		FruGroupIndex	1.3.6.1.4.1.412.2.4.33.1.16	DmiInteger	Read-Only
176		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.33.1.17	DmiInteger	Read-Only
177	tMemoryArrayMappedAddresses.eMemoryArrayMappedAddresses	MemoryArrayMappedAddressesTableIndex	1.3.6.1.4.1.412.2.4.34.1.1	DmiInteger	Read-Only
178		MemoryArrayIndex	1.3.6.1.4.1.412.2.4.34.1.2	DmiInteger	Read-Only
179		MappedRangeStartingAddress	1.3.6.1.4.1.412.2.4.34.1.3	DmiInteger	Read-Only
180		MappedRangeEndingAddress	1.3.6.1.4.1.412.2.4.34.1.4	DmiInteger	Read-Only
181		PartitionId	1.3.6.1.4.1.412.2.4.34.1.5	DmiInteger	Read-Only
182		PartitionWidth	1.3.6.1.4.1.412.2.4.34.1.6	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
183		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.34.1.7	DmiInteger	Read-Only
184	tMemoryDevice.eMemoryDevice	MemoryDeviceTableIndex	1.3.6.1.4.1.412.2.4.35.1.1	DmiInteger	Read-Only
185		MemoryArrayIndex	1.3.6.1.4.1.412.2.4.35.1.2	DmiInteger	Read-Only
186		DeviceLocator	1.3.6.1.4.1.412.2.4.35.1.3	DmiDisplaystring	Read-Only
187		BankLocator	1.3.6.1.4.1.412.2.4.35.1.4	DmiDisplaystring	Read-Only
188		Size	1.3.6.1.4.1.412.2.4.35.1.5	DmiInteger	Read-Only
189		FormFactor	1.3.6.1.4.1.412.2.4.35.1.6	Integer	Read-Only
190		TotalWidth	1.3.6.1.4.1.412.2.4.35.1.7	DmiInteger	Read-Only
191		DataWidth	1.3.6.1.4.1.412.2.4.35.1.8	DmiInteger	Read-Only
192		MemoryType	1.3.6.1.4.1.412.2.4.35.1.9	Integer	Read-Only
193		TypeDetail	1.3.6.1.4.1.412.2.4.35.1.10	Integer	Read-Only
194		DeviceSet	1.3.6.1.4.1.412.2.4.35.1.11	DmiInteger	Read-Only
195		DeviceErrorType	1.3.6.1.4.1.412.2.4.35.1.12	Integer	Read-Only
196		ErrorGranularity	1.3.6.1.4.1.412.2.4.35.1.13	Integer	Read-Only
197		LastErrorUpdate	1.3.6.1.4.1.412.2.4.35.1.14	Integer	Read-Only
198		ErrorOperation	1.3.6.1.4.1.412.2.4.35.1.15	Integer	Read-Only
199		ErrorDataSize	1.3.6.1.4.1.412.2.4.35.1.16	DmiInteger	Read-Only
200		ErrorData	1.3.6.1.4.1.412.2.4.35.1.17	DmiOctetstring	Read-Only
201		VendorSyndrome	1.3.6.1.4.1.412.2.4.35.1.18	DmiOctetstring	Read-Only
202		DeviceErrorAddress	1.3.6.1.4.1.412.2.4.35.1.19	DmiInteger	Read-Only
203		ArrayErrorAddress	1.3.6.1.4.1.412.2.4.35.1.20	DmiInteger	Read-Only
204		ErrorResolution	1.3.6.1.4.1.412.2.4.35.1.21	DmiInteger	Read-Only
205		FruGroupIndex	1.3.6.1.4.1.412.2.4.35.1.22	DmiInteger	Read-Only
206		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.35.1.23	DmiInteger	Read-Only
207	tMemoryDeviceMappedAddresses.eMemoryDeviceMappedAddresses	MemoryDeviceMappedAddressesTableIndex	1.3.6.1.4.1.412.2.4.36.1.1	DmiInteger	Read-Only
208		MemoryDeviceSetId	1.3.6.1.4.1.412.2.4.36.1.2	DmiInteger	Read-Only
209		Partition	1.3.6.1.4.1.412.2.4.36.1.3	DmiInteger	Read-Only
210		MappedRangeStartingAddress	1.3.6.1.4.1.412.2.4.36.1.4	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
211		MappedRangeEndingAddress	1.3.6.1.4.1.412.2.4.36.1.5	DmiInteger	Read-Only
212		PartitionRowPosition	1.3.6.1.4.1.412.2.4.36.1.6	DmiInteger	Read-Only
213		InterleavePosition	1.3.6.1.4.1.412.2.4.36.1.7	DmiInteger	Read-Only
214		DataDepth	1.3.6.1.4.1.412.2.4.36.1.8	DmiInteger	Read-Only
215	tSystemPowerControls.eSystemPowerControls	PowerControlRequest	1.3.6.1.4.1.412.2.4.51.1.1	Integer	Read-Write
216		TimedPower-onAvailable	1.3.6.1.4.1.412.2.4.51.1.2	Integer	Read-Only
217		TimeToNextScheduledPower-on	1.3.6.1.4.1.412.2.4.51.1.3	DmiInteger	Read-Write
218	tVoltageProbe.tVoltageProbeTraps	notification1ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.256	Notification Type	
219		ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.257	Notification Type	
220		notification3ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.258	Notification Type	
221		notification4ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.259	Notification Type	
222		notification5ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.260	Notification Type	
223		notification6ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.261	Notification Type	
224		notification7ForVoltageProbe	1.3.6.1.4.1.412.2.4.53.0.262	Notification Type	
225	tVoltageProbe.eVoltageProbe	VoltageProbeIndex	1.3.6.1.4.1.412.2.4.53.1.1	DmiInteger	Read-Only
226		VoltageProbeLocation	1.3.6.1.4.1.412.2.4.53.1.2		Read-Only
227		VoltageProbeDescription	1.3.6.1.4.1.412.2.4.53.1.3		Read-Only
228		VoltageStatus	1.3.6.1.4.1.412.2.4.53.1.4		Read-Only
229		VoltageProbeVoltageLevel	1.3.6.1.4.1.412.2.4.53.1.5	DmiInteger	Read-Only
230		MonitoredVoltageNominalLevel	1.3.6.1.4.1.412.2.4.53.1.6	DmiInteger	Read-Only
231		MonitoredVoltageNormalMaximum	1.3.6.1.4.1.412.2.4.53.1.7	DmiInteger	Read-Only
232		MonitoredVoltageNormalMinimum	1.3.6.1.4.1.412.2.4.53.1.8	DmiInteger	Read-Only
233		VoltageProbeMaximum	1.3.6.1.4.1.412.2.4.53.1.9	DmiInteger	Read-Only
234		VoltageProbeMinimum	1.3.6.1.4.1.412.2.4.53.1.10	DmiInteger	Read-Only
235		VoltageLevelLowerThreshold-Non-critic	1.3.6.1.4.1.412.2.4.53.1.11	DmiInteger	Read-Write
236		VoltageLevelUpperThreshold-Non-critic	1.3.6.1.4.1.412.2.4.53.1.12	DmiInteger	Read-Write

S.No	Group	Attribute	OID	Type	Access Privilege
237		VoltageLevelLowerThreshold-Critical	1.3.6.1.4.1.412.2.4.53.1.13	DmiInteger	Read-Write
238		VoltageLevelUpperThreshold-Critical	1.3.6.1.4.1.412.2.4.53.1.14	DmiInteger	Read-Write
239		VoltageLevelLowerThreshold-Non-recover	1.3.6.1.4.1.412.2.4.53.1.15	DmiInteger	Read-Write
240		VoltageLevelUpperThreshold-Non-recover	1.3.6.1.4.1.412.2.4.53.1.16	DmiInteger	Read-Write
241		VoltageProbeResolution	1.3.6.1.4.1.412.2.4.53.1.17	DmiInteger	Read-Write
242		VoltageProbeTolerance	1.3.6.1.4.1.412.2.4.53.1.18	DmiInteger	Read-Write
243		VoltageProbeAccuracy	1.3.6.1.4.1.412.2.4.53.1.19	DmiInteger	Read-Write
244		FruGroupIndex	1.3.6.1.4.1.412.2.4.53.1.20	DmiInteger	Read-Only
245		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.53.1.21	DmiInteger	Read-Only
246	tTemperatureProbe.tTemperatureProbeTraps	notification1ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.256	Notification Type	
247		notification2ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.257	Notification Type	
248		notification3ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.258	Notification Type	
249		notification4ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.259	Notification Type	
250		notification5ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.260	Notification Type	
251		notification6ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.261	Notification Type	
252		notification7ForTemperatureProbe	1.3.6.1.4.1.412.2.4.54.0.262	Notification Type	
253	tTemperatureProbe.eTemperatureProbe	TemperatureProbeTableIndex	1.3.6.1.4.1.412.2.4.54.1.1	DmiInteger	Read-Only
254		TemperatureProbeLocation	1.3.6.1.4.1.412.2.4.54.1.2	Integer	Read-Only
255		TemperatureProbeDescription	1.3.6.1.4.1.412.2.4.54.1.3	DmiDisplaystring	Read-Only
256		TemperatureStatus	1.3.6.1.4.1.412.2.4.54.1.4	Integer	Read-Only
257		TemperatureProbeTemperatureReading	1.3.6.1.4.1.412.2.4.54.1.5	DmiInteger	Read-Only
258		MonitoredTemperatureNominalReading	1.3.6.1.4.1.412.2.4.54.1.6	DmiInteger	Read-Only
259		MonitoredTemperatureNormalMinimum	1.3.6.1.4.1.412.2.4.54.1.8	DmiInteger	Read-Only
260		TemperatureProbeMaximum	1.3.6.1.4.1.412.2.4.54.1.9	DmiInteger	Read-Only
261		TemperatureProbeMinimum	1.3.6.1.4.1.412.2.4.54.1.10	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
262		TemperatureLowerThreshold-Non-critical	1.3.6.1.4.1.412.2.4.54.1.11	DmiInteger	Read-Only
263		TemperatureUpperThreshold-Non-critical	1.3.6.1.4.1.412.2.4.54.1.12	DmiInteger	Read-Write
264		TemperatureLowerThreshold-Critical	1.3.6.1.4.1.412.2.4.54.1.13	DmiInteger	Read-Write
265		TemperatureUpperThreshold-Critical	1.3.6.1.4.1.412.2.4.54.1.14	DmiInteger	Read-Write
266		TemperatureLowerThreshold-Non-recover	1.3.6.1.4.1.412.2.4.54.1.15	DmiInteger	Read-Write
267		TemperatureUpperThreshold-Non-recover	1.3.6.1.4.1.412.2.4.54.1.16	DmiInteger	Read-Write
268		TemperatureProbeResolution	1.3.6.1.4.1.412.2.4.54.1.17	DmiInteger	Read-Write
269		TemperatureProbeTolerance	1.3.6.1.4.1.412.2.4.54.1.18	DmiInteger	Read-Write
270		TemperatureProbeAccuracy	1.3.6.1.4.1.412.2.4.54.1.19	DmiInteger	Read-Write
271		FruGroupIndex	1.3.6.1.4.1.412.2.4.54.1.20	DmiInteger	Read-Only
272		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.54.1.21	DmiInteger	Read-Only
273	tPhysicalContainerGlobalTable.tPhysicalContainerGlobalTableTraps	notification1ForPhysicalContainer	1.3.6.1.4.1.412.2.4.63.0.6	Notification Type	
274		notification2ForPhysicalContainer	1.3.6.1.4.1.412.2.4.63.0.256	Notification Type	
275	tPhysicalContainerGlobalTable.ePhysicalContainerGlobalTable	ContainerOrChassisType	1.3.6.1.4.1.412.2.4.63.1.1	Integer	Read-Only
276		AssetTag	1.3.6.1.4.1.412.2.4.63.1.2	DmiDisplaystring	Read-Write
277		ChassisLockPresent	1.3.6.1.4.1.412.2.4.63.1.3	Integer	Read-Only
278		BootupState	1.3.6.1.4.1.412.2.4.63.1.4	Integer	Read-Only
279		PowerState	1.3.6.1.4.1.412.2.4.63.1.5	Integer	Read-Only
280		ThermalState	1.3.6.1.4.1.412.2.4.63.1.6	Integer	Read-Only
281		FruGroupIndex	1.3.6.1.4.1.412.2.4.63.1.7	DmiInteger	Read-Only
282		OperationalGroupIndex	1.3.6.1.4.1.412.2.4.63.1.8	DmiInteger	Read-Only
283		ContainerIndex	1.3.6.1.4.1.412.2.4.63.1.9	DmiInteger	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
284		ContainerName	1.3.6.1.4.1.412.2.4.63.1.10	DmiDisplaystring	Read-Write
285		ContainerLocation	1.3.6.1.4.1.412.2.4.63.1.11	DmiDisplaystring	Read-Write
286		ContainerSecurityStatus	1.3.6.1.4.1.412.2.4.63.1.12	Integer	Read-Only
287					
288	tPowerUnitGlobalTable.tPowerUnitGlobalTableTraps	Notification1ForPowerUnit	1.3.6.1.4.1.412.2.4.66.0.1	Notification Type	
289		notification2ForPowerUnit	1.3.6.1.4.1.412.2.4.66.0.2	Notification Type	
290		notification3ForPowerUnit	1.3.6.1.4.1.412.2.4.66.0.3	Notification Type	
291		notification4ForPowerUnit	1.3.6.1.4.1.412.2.4.66.0.4	Notification Type	
292		notification5ForPowerUnit	1.3.6.1.4.1.412.2.4.66.0.5	Notification Type	
293	tPowerUnitGlobalTable.ePowerUnitGlobalTable	PowerUnitIndex	1.3.6.1.4.1.412.2.4.66.1.1	DmiInteger	Read-Only
294		PowerUnitRedundancyStatus	1.3.6.1.4.1.412.2.4.66.1.2	Integer	Read-Only
295	mapperdmfGroups.tCoolingUnitGlobalTable	CoolingUnitIndex	1.3.6.1.4.1.412.2.4.66.1.3	DmiInteger	Read-Only
296		CoolingUnitStatus	1.3.6.1.4.1.412.2.4.66.1.4	Integer	Read-Only
297					
298	tEventGenerationForProcessor.eEventGenerationForProcessor	EventType	1.3.6.1.4.1.412.2.4.100.1.1	Integer	
299		EventSeverity	1.3.6.1.4.1.412.2.4.100.1.2	Integer	Read-Only
300		EventState-based	1.3.6.1.4.1.412.2.4.100.1.3	Integer	Read-Only
301		EventStateKey	1.3.6.1.4.1.412.2.4.100.1.4	DmiInteger	Read-Only
302		AssociatedGroup	1.3.6.1.4.1.412.2.4.100.1.5	DmiDisplaystring	Read-Only
303		EventSystem	1.3.6.1.4.1.412.2.4.100.1.6	Integer	Read-Only
304		EventSubsystem	1.3.6.1.4.1.412.2.4.100.1.7	Integer	Read-Only
305		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.100.1.9	Integer	Read-Only
306		EventMessage	1.3.6.1.4.1.412.2.4.100.1.10	DmiDisplaystring	Read-Only
307	tEventGenerationForPowerSupply.eEventGenerationForPowerSupply	EventType	1.3.6.1.4.1.412.2.4.104.1.1	Integer	Read-Only
308		EventSeverity	1.3.6.1.4.1.412.2.4.104.1.2	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
309		EventState-based	1.3.6.1.4.1.412.2.4.104.1.3	Integer	Read-Only
310		EventStateKey	1.3.6.1.4.1.412.2.4.104.1.4	DmiInteger	Read-Only
311		AssociatedGroup	1.3.6.1.4.1.412.2.4.104.1.5	DmiDisplaystring	Read-Only
312		EventSystem	1.3.6.1.4.1.412.2.4.104.1.6	Integer	Read-Only
313		EventSubsystem	1.3.6.1.4.1.412.2.4.104.1.7	Integer	Read-Only
314		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.104.1.9	Integer	Read-Only
315		EventMessage	1.3.6.1.4.1.412.2.4.104.1.10	DmiDisplaystring	Read-Only
316	tEventGenerationForPhysicalMemory.eEventGenerationForPhysicalMemory	EventType	1.3.6.1.4.1.412.2.4.108.1.1	Integer	Read-Only
317		EventSeverity	1.3.6.1.4.1.412.2.4.108.1.2	Integer	Read-Only
318		EventState-based	1.3.6.1.4.1.412.2.4.108.1.3	Integer	Read-Only
319		EventStateKey	1.3.6.1.4.1.412.2.4.108.1.4	DmiInteger	Read-Only
320		AssociatedGroup	1.3.6.1.4.1.412.2.4.108.1.5	DmiDisplaystring	Read-Only
321		EventSystem	1.3.6.1.4.1.412.2.4.108.1.6	Integer	Read-Only
322		EventSubsystem	1.3.6.1.4.1.412.2.4.108.1.7	Integer	Read-Only
323		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.108.1.9	Integer	Read-Only
324		EventMessage	1.3.6.1.4.1.412.2.4.108.1.10	DmiDisplaystring	Read-Only
325	tEventGenerationForVoltageProbe.eEventGenerationForVoltageProbe	EventType	1.3.6.1.4.1.412.2.4.113.1.1	Integer	Read-Only
326		EventSeverity	1.3.6.1.4.1.412.2.4.113.1.2	Integer	Read-Only
327		IsEventState-based	1.3.6.1.4.1.412.2.4.113.1.3	Integer	Read-Only
328		EventStateKey	1.3.6.1.4.1.412.2.4.113.1.4	DmiInteger	Read-Only
329		AssociatedGroup	1.3.6.1.4.1.412.2.4.113.1.5	DmiDisplaystring	Read-Only
330		EventSystem	1.3.6.1.4.1.412.2.4.113.1.6	Integer	Read-Only
331		EventSubsystem	1.3.6.1.4.1.412.2.4.113.1.7	Integer	Read-Only
332		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.113.1.	Integer	Read-Only
333		EventMessage	1.3.6.1.4.1.412.2.4.113.1.10	DmiDisplaystring	Read-Only
334	tEventGenerationForTemperatureProbe.eEventGenerati	EventType	1.3.6.1.4.1.412.2.4.114.1.1	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
	onForTemperatureProbe				
335		EventSeverity	1.3.6.1.4.1.412.2.4.114.1.2	Integer	Read-Only
336		EventState-based	1.3.6.1.4.1.412.2.4.114.1.3	Integer	Read-Only
337		EventStateKey	1.3.6.1.4.1.412.2.4.114.1.4	DmiInteger	Read-Only
338		AssociatedGroup	1.3.6.1.4.1.412.2.4.114.1.5	DmiDisplaystring	Read-Only
339		EventSystem	1.3.6.1.4.1.412.2.4.114.1.6	Integer	Read-Only
340		EventSubsystem	1.3.6.1.4.1.412.2.4.114.1.7	Integer	Read-Only
341		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.114.1.9	Integer	Read-Only
342		EventMessage	1.3.6.1.4.1.412.2.4.114.1.10	DmiDisplaystring	Read-Only
343	tEventGenerationForPhysicalContainer.eEventGenerationForPhysicalContainer	EventType	1.3.6.1.4.1.412.2.4.116.1.1	Integer	Read-Only
344		EventSeverity	1.3.6.1.4.1.412.2.4.116.1.2	Integer	Read-Only
345		IsEventState-based	1.3.6.1.4.1.412.2.4.116.1.3	Integer	Read-Only
346		EventStateKey	1.3.6.1.4.1.412.2.4.116.1.4	DmiInteger	Read-Only
347		AssociatedGroup	1.3.6.1.4.1.412.2.4.116.1.5	DmiDisplaystring	Read-Only
348		EventSystem	1.3.6.1.4.1.412.2.4.116.1.6	Integer	Read-Only
349		EventSubsystem	1.3.6.1.4.1.412.2.4.116.1.7	Integer	Read-Only
350		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.116.1.9	Integer	Read-Only
351		EventMessage	1.3.6.1.4.1.412.2.4.116.1.10	DmiDisplaystring	Read-Only
352	tEventGenerationForCoolingDevice.eEventGenerationForCoolingDevice	EventType	1.3.6.1.4.1.412.2.4.140.1.1	Integer	Read-Only
353		EventSeverity	1.3.6.1.4.1.412.2.4.140.1.2	Integer	Read-Only
354		IsEventState-based	1.3.6.1.4.1.412.2.4.140.1.3	Integer	Read-Only
355		EventStateKey	1.3.6.1.4.1.412.2.4.140.1.4	DmiInteger	Read-Only
356		AssociatedGroup	1.3.6.1.4.1.412.2.4.140.1.5	DmiDisplaystring	Read-Only
357		EventSystem	1.3.6.1.4.1.412.2.4.140.1.6	Integer	Read-Only
358		EventSubsystem	1.3.6.1.4.1.412.2.4.140.1.7	Integer	Read-Only
359	tEventGenerationForPowerUnit.eEventGenerationForP	EventType	1.3.6.1.4.1.412.2.4.201.1.1	Integer	Read-Only

S.No	Group	Attribute	OID	Type	Access Privilege
	owerUnit				
360		EventSeverity	1.3.6.1.4.1.412.2.4.201.1.2	Integer	Read-Only
361		IsEventState-based	1.3.6.1.4.1.412.2.4.201.1.3	Integer	Read-Only
362		EventStateKey	1.3.6.1.4.1.412.2.4.201.1.4	DmiInteger	Read-Only
363		AssociatedGroup	1.3.6.1.4.1.412.2.4.201.1.5	DmiDisplaystring	Read-Only
364		EventSystem	1.3.6.1.4.1.412.2.4.201.1.6	Integer	Read-Only
365		EventSubsystem	1.3.6.1.4.1.412.2.4.201.1.7	Integer	Read-Only
366		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.201.1.9	Integer	Read-Only
367		EventMessage	1.3.6.1.4.1.412.2.4.201.1.10	DmiDisplaystring	Read-Only
368	tEventGenerationForSystem Slots.eEventGenerationFor SystemSlots	EventType	1.3.6.1.4.1.412.2.4.205.1.1	Integer	Read-Only
369		EventSeverity	1.3.6.1.4.1.412.2.4.205.1.2	Integer	Read-Only
370		IsEventState-based	1.3.6.1.4.1.412.2.4.205.1.3	Integer	Read-Only
371		EventStateKey	1.3.6.1.4.1.412.2.4.205.1.4	DmiInteger	Read-Only
372		AssociatedGroup	1.3.6.1.4.1.412.2.4.205.1.5	DmiDisplaystring	Read-Only
373		EventSystem	1.3.6.1.4.1.412.2.4.205.1.6	Integer	Read-Only
374		EventSubsystem	1.3.6.1.4.1.412.2.4.205.1.7	Integer	Read-Only
375		IsInstanceDataPresent	1.3.6.1.4.1.412.2.4.205.1.9	Integer	Read-Only
376		EventMessage	1.3.6.1.4.1.412.2.4.205.1.10	DmiDisplaystring	Read-Only

Appendix 9: ISM Feature Matrix

Supported Features	SE7500WV2	SHG2	SRSH4/ SPSH4	SE7501WV2 SE7501BR2 SE7501HG2	SE7210TP1-E
ISM version at system release	5.1	5.0	5.0.1	5.5	5.8
ISM version support by web release or ECO	5.5.7	5.8	5.8	5.8	5.8
Installation Wizard	Y	Y	Y	Y	Y
System Configuration Wizard	Y	N	N	Y	Y
Online ISM help	Y	Y	Y	Y	Y
Installation and User Guide	Y	Y	Y	Y	Y
Service Partition	Y	Y	Y	Y	N
Intelligent Chassis Management Bus	Y	Y	Y	Y	N
ISM Standalone Console	Y	Y	Y	Y	Y
Server Operating Systems					
Microsoft Windows Server 2003 Enterprise Edition	N	Y	Y	Y	Y
Microsoft Windows 2000, Advanced Server, SP3	Y	Y	Y	Y	Y
Red Hat Linux server 8.0	N	N	N	Y	Y
Red Hat Linux AS 2.1	N	N	Y	Y	Y
NetWare v5.1 SP3; NetWare 6.0 SP1	Y	Y	Y	Y	N
Caldera OpenUnix server v8.0	N	N	Y	Y	N
Platform Instrumentation Control – Console Operating Systems					
Microsoft Windows Server 2003 Enterprise Edition	N	Y	Y	Y	Y
Microsoft Windows 2000, Professional, SP3	Y	Y	Y	Y	Y
Microsoft Windows XP Professional	Y	Y	Y	Y	Y
Command Line Interface – Client Operating Systems					

Supported Features	SE7500WV2	SHG2	SRSH4/ SPSH4	SE7501WV2 SE7501BR2 SE7501HG2	SE7210TP1-E
Microsoft Windows Server 2003 Enterprise Edition	N	Y	Y	Y	Y
Microsoft Windows 2000, Professional, SP3	Y	Y	Y	Y	Y
Microsoft Windows XP Professional, SP2	Y	Y	Y	Y	Y
Microsoft Windows 2000, Advanced Server, SP3	Y	Y	Y	Y	Y
Red Hat Linux, AS 2.1	N	N	N	Y	Y
Red Hat Linux, v8.0	N	N	N	Y	Y
Platform Instrumentation Control					
HP OpenView Network Node Manager 6.x	Y	Y	Y	Y	Y
CA Unicenter Framework TNG 3.0	Y	Y	Y	Y	Y
SNMP V2.0 for Enterprise Sys. Mgt. Consoles	Y	Y	Y	N	N
SNMP V3.0 for Enterprise Sys. Mgt. Consoles	N	N	N	Y	Y
Desktop Management Interface (DMI) indications	Y	Y	Y	Y	Y
Baseboard voltage status	Y	Y	Y	Y	Y
Chassis intrusion status	Y	Y	Y ²	Y	Y
Drive availability status	Y	Y	Y	Y	N
Temperature status	Y	Y	Y	Y	Y
Fan status	Y	Y	Y	Y	Y
Fan Removal/Reinsertion Status	N	N	N	N	N
PCI Hot Plug slot status	N	N	Y	N	N
Power supply health status	Y	Y	Y	Y	N
Power supply redundancy status	Y	Y	Y	Y	N
User controlled alert indications	Y	Y	Y	Y	Y
User selectable power control actions based on events	Y	Y	Y	Y	Y
Email Alerts	Y	Y	Y	Y	Y
ISM paging	Y	Y	Y	Y	Y
SMaRT Tool Interface	Y	Y	Y	Y	Y

Supported Features	SE7500WV2	SHG2	SRSH4/ SPSH4	SE7501WV2 SE7501BR2 SE7501HG2	SE7210TP1-E
Remote power control (on, off, reset)	Y	Y	Y	Y	Y
Access to non-volatile System Event Logs	Y	Y	Y	Y	Y
CHAP Compliance	Y	Y	Y	Y	Y
Passwords	Y	Y	Y	Y	Y
Baseboard voltage	Y	Y	Y	Y	Y
Fan pack-digital	N	Y	Y	N	N
Fan pack-tachometer	Y ⁴	Y	Y	Y	Y
Individual fans-digital	N	Y	Y	N	N
Individual fans-tachometer	Y ⁴	Y	Y	Y ⁴	Y
Hot swap disk drives	Y	Y	Y	Y	N
Hot swap power supply	Y	Y ²	Y	Y ⁴	N
Hot swap fans	N	Y ⁴	Y ³	N	N
IPMI v1.5 Compliant	Y	Y	Y	Y	N ⁸
System temperatures	Y	Y	Y	Y	Y
Emergency Management Port (Serial2)	Y	Y	Y	Y	N
Firmware Platform Event Paging (OS Independent)	Y	Y	Y	Y	N
Auto answer on modem	Y	Y	Y	Y	N
Console redirection	Y	Y	Y	Y	N
Power Control / Reset	Y	Y	Y	Y	Y
System Event Log manager	Y	Y	Y	Y	Y
Sensor Data Records manager	Y	Y	Y	Y	Y
Field Replaceable Unit manager	Y	Y	Y	Y	Y
Remote Sensor Access manager	Y	Y	Y	Y	Y
OOB hardware confidence tests	N	N	Y	N	N

⁸ Supports IPMI commands. Has SMBus system interface rather than KCS interface as on full BMC.

Supported Features	SE7500WV2	SHG2	SRSH4/ SPSH4	SE7501WV2 SE7501BR2 SE7501HG2	SE7210TP1-E
DOS shell access in Service Partition (command prompt)	Y	Y	Y	Y	N
File transfer	Y	Y	Y	Y	N
LAN connection (OS up or down)	Y	Y	Y	Y	Y
Modem connection (OS up or down)	Y	Y	Y	Y	N
Direct Serial cable connection (OS up or down)	Y	Y	Y	Y	N
CHAP Compliance	Y	Y	Y	Y	Y
Passwords	Y	Y	Y	Y	Y
Console redirection	Y	Y	Y	Y	N
System Event Log manager	Y	Y	Y	Y	N
Sensor Data Records manager	Y	Y	Y	Y	N
Field Replaceable Unit manager	Y	Y	Y	Y	N
Multi-Boot Manager	Y	Y	Y	Y	N
Password Manager	Y	Y	Y	Y	N
Platform Event Manager	Y	Y	Y	Y	N
Configuration Save / Restore Manager	Y	Y	Y	Y	N
FW upgrades (System Update Manager)	Y	Y	Y	Y	N
BIOS upgrades (System Update Manager)	Y	Y	Y	Y	N
LAN connection (OS up or down)	Y	Y	Y	Y	N
Modem connection (OS up or down)	Y	Y	Y	Y	N
Direct Serial cable connection (OS up or down)	Y	Y	Y	Y	N
CHAP Compliance	Y	Y	Y	Y	N
Passwords	Y	Y	Y	Y	N
Command Line Interface	Y	Y ¹	Y ¹	Y	Y
Serial over LAN	Y	N	N	Y	N
Native Command Line Interface (direct connect from communications application)	N	N	N	Y	N
LAN Alert Viewer					Y

Supported Features	SE7500WV2	SHG2	SRSH4/ SPSH4	SE7501WV2 SE7501BR2 SE7501HG2	SE7210TP1-E
OOB LAN alerts (SNMP traps)	Y	Y	Y	Y	Y

Notes

1. Available from a web download (<http://support.intel.com/support/motherboards/server/isc/software.htm>)
2. No chassis intrusion on the Server System SRSH4
3. SRSH4 only
4. SKU or chassis dependent
5. Caldera OpenUnix 8.0 is not supported on the Server Board SE7501WV2

Appendix 10: ISM v5.5 Features

Intel Server Management v5.5 was initially released to support the Intel® Server Boards SE7501WV2 and SE7501BR2 and their associated Intel® Server Chassis. The Server Board SE7501HG2 support was later added. This section outlines the features added since the release of previous ISM versions. See Appendix 7 for a matrix of ISM features by server system. Features added or enhanced in version 5.5 include the following:

- Additions to the Command Line Interface command set
- System ID LED control and alerting capabilities added to Platform Instrumentation Control
- Native Command Line Interface using direct cable connection to server board
- SNMP V3.0

Command Line Interface Enhancements

The command set used by the Command Line Interface (CLI) has been expanded. The following focuses only on the changes. See the ISM Installation and User Guide on the ISM CD for the full command set.

- `identify [-on [seconds]] [-off] [-s]`
- `[-on [seconds]]` has been extended to turn on the LED for an indefinite time. This is accomplished by entering “0” (zero) as the value for seconds.
- `[-s]` adds the ability to determine the current status of the system identify LED on the front panel of Intel server chassis. The response indicates the current LED state as ON (Application), ON (Button), or OFF.
 - `power -s`
- Displays the current power state of the remote server. On or Off
 - `sel [-c] [-num] [-f filename] [-h filename] [-clear]`
- `[-clear]` adds the ability to clear the System Event Log on the remote server

System ID LED Control

Control of the system identify LED has been added as one of the alerting capabilities from the Platform Instrumentation Control GUI. This gives users the ability to proactively turn on the LED if unexpected conditions occur on the server. As with all alerting actions in OIC, the user has full control over which alerts or actions take place for condition changes on any system sensor. Clicking on the Alert tab for individual sensors displays the list of available alert actions.

Manual control of the remote system ID LED has been added as a menu item from PIC. The ID LED menu option displays a drop-down with the following selections:

- **On:** As indicated by the dot next to it, this item is enabled only if the system ID LED is turned on with the button on the physical chassis. Otherwise it is disabled. At the same time the Off menu item and the Blink menu item will be enabled.
- **Blink:** Sends a message to blink the LED. At the same time the Off menu item will be enabled and a dot will be placed in front of Blink.

- **Off:** Sends a message to turn off the system ID LED. At the same time the Blink menu item will be enabled and a dot will be placed in front of Off.

Native Command Line

Native command line is a feature that allows the user to directly send text-based commands to the server's Baseboard Management Controller (BMC) using a serial port connection. The connection requires the use of a "Null Modem" cable connected to Serial B (Emergency Management Port). Terminal mode supports standard binary IPMI 1.5 hex-ASCII commands and specific text commands. In terminal mode the user can:

- Power the server on or off
- Reset the server
- Retrieve the server's health status
- View and configure the server boot options
- View and configure the BMC's terminal mode configuration
- Execute any platform-supported binary command specified in the Intelligent Platform Management Interface (IPMI) v1.5 specification using the hex-ASCII format

See the ISM Installation and User Guide on the ISM CD for a full description of commands.

SNMP v3.0

SNMP-based access to platform instrumentation data is provided by mapping the data from DMI to SNMP. The DMI-to-SNMP mapper is an SNMP agent that translates SNMP requests for Gets and Sets to appropriate DMI requests that are passed to the DMI service provider to be processed by the DMI based platform instrumentation stack.

The management console must load SNMP MIBs correlating to the DMI MIFs supported by the platform instrumentation providers. The mapper runs as a service or daemon on the managed server. To provide additional security and address CERT advisories affecting SNMP V1 and some V2 implementations, ISM 5.5 will not support traps that adhere to SNMP V3 format. Only V2 traps will be supported. No changes are expected to be required for either the mapper or any of the supported MIBs.

In essence, ISM 5.5 will work with the SNMP V3 implementations but will not support all the new features of SNMP V3. All features that were supported by SNMP V2 will continue to be supported by ISM 5.5 while using SNMP V3 packages. In addition, ISM 5.5 will provide the user with the facility to use the new security feature of SNMP V3. Some configuration is needed to enable this feature. This is explained in the Installation and User Guide for ISM 5.5.

ISM will support the NET-SNMP Release 4.2.4 implementation of SNMP on Red Hat Linux. Version 3 is only supported on Red Hat Linux. The same SNMP version as supported on ISM 5.1 will be supported on all other operating systems.

Appendix 11: ISM v5.5.6 Features

ISM 5.5.6 includes support for memory mirroring and memory sparing on Server Systems SRSH4 and SPSH4.

Appendix 12: ISM v5.5.7 Features

Intel Server Management v5.5.7 release contains certified Microsoft Windows drivers. This release also has fixes including a fix for the issue where a reset command from DPC or CLI to a Windows 2003 managed server resulted in the system shutting down rather than resetting.

Appendix 13: ISM v5.8 Features

ISM 5.8 features support for the Server Board SE7210TP1-E. This platform uses the National Semiconductor* PC87431M mini-Baseboard Management Controller (mBMC) as compared to the other servers supported by ISM which uses a full BMC. Consequently, managing the Server Board SE7210TP1-E with this version of ISM supports a subset of the management functionality present when managing server platforms that house the full BMC. The subset of features derives primarily from a LAN-only connection between the system running ISM and the Server Board SE7210TP1-E platform.

Features not supported on the Server Board SE7210TP1-E are as follows.

- Serial over LAN (SOL) and console redirection.
- Service Partition
- Remote Sensor Access (RSA)
- Emergency Management Port (EMP)
- Direct serial connection and modem connection
- Intelligent Chassis Management Bus (ICMB)
- Native Command Line
- Front Panel Power and Reset button monitoring
- Fan redundancy monitoring
- Redundant power supply monitoring
- No Intelligent Platform Management Bus (IPMB) bus interface. Consequently, no monitoring of the hot-swap backplane.
- Graceful shutdown
- Client SSU (CSSU)
- One user (versus 4) over LAN and one session (versus 4) over LAN. User is anonymous only.
- MD5 (rather than MD2, MD5) hash
- Number of System Event Log (SEL) entries: 92
- Support for PCI SMBus connections. PCI card firmware cannot log SEL events
- Detection of missing processor or memory
- One-Boot Flash Update Utility

Glossary

This appendix contains important terms used in the preceding chapters. For ease of use, numeric entries are listed first (e.g., “82460GX”) with alpha entries following (e.g., “AGP 4x”). Acronyms are then entered in their respective place, with non-acronyms following.

Term	Definition
BMC	Baseboard Management Controller
DMI	Desktop management interface, an industry standard management specification
DMTF	Distributed Management Task Force, Inc
DPC	Direct Platform Control
EMC	Enterprise Management Console
EMP	Emergency Management Port
ICMB	Intelligent Chassis Management Bus
ISM	Intel Server Management
IHV	Independent Hardware Vendor
IPMI	Intelligent Platform Management Interface
IPS	Internal Product Specification
I ² C bus	Inter Integrated Circuit bus. A 2-wire bi-directional serial bus developed by Philips for an independent communications path between embedded ICs on printed circuit boards and subsystems. The I ² C bus is used on Intel servers for system management and diagnostics.
LRA	Local Response Agent
mBMC	Mini Baseboard Management Controller
MIB	Management Information Base, used by SNMP for describing component instrumentation
MIF	Management Information Format file, used by DMI for describing component instrumentation
NIC	Network Interface Card
NMI	Non Maskable Interrupt
NOS	Network Operating System
OID	Object Identifier
PHP	PCI Hot Plug
PI	Platform Instrumentation
PIC	Platform Instrumentation Control
SDR	Sensor Data Record
SEL	System Event Log
SNMP	Simple Network Management Protocol, a standard network protocol for management information
SP	DMI 2.0 Service Provider (previously known as DMI Service Layer)
WFM	Wired for Management
IPSA	IP Synchronization Agent

Reference Documents

Refer to the following documents for additional information:

- Intel Server Management Installation and User Guide
- Readme.txt (ISM v5.x)
- Errata.txt (ISM v5.x)