Installation and User Guide

for

Intel® Server Management (ISM)

Ver. 5.8

Legal Information

Contents

1. Introduction

Intel® Server Management (ISM) is a server management tool implemented with client-server architecture. This guide explains how to install ISM and use the software to:

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

Platform Compatibility

The ISM features depend on which version of ISM is running on which platform. Compatibility may be an issue when a current version of the ISM console manages a network of systems that are running older versions of ISM. (Earlier versions were named Intel® Server Control, or ISC.) For a list of features available in this release, see the *ISM v5.x Technical Product Specification* and/or *Monthly Specification Updates*.

New ISM Features

This release of ISM features support for the SE7210TP1-E server platform. This platform uses a mini-Baseboard Management Controller (mBMC) as compared to servers that use a full BMC. Consequently, managing the SE7210TP1-E server (or any other server that uses the mini BMC) 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 SE7210TP1-E server platform. Throughout this manual, server management features not supported when managing the SE7210TP1-E server platform are noted.

Getting the Latest Information and Support

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

On the web site, under Intel Server Management software, look for Specifications and Errata, then see the ISM Specification Update.

For technical details about ISM, see the Technical Product Specification at the same web site location. If you have questions or need help using ISM, contact your service representative.

System Requirements

ISM contains two parts:

- ISM Console Software, which runs on one or more client systems, can be installed on these operating systems:
  - Windows† XP Professional
  - Windows 2000 Advanced Server, Service Pack 3
  - Windows 2000 Professional, Service Pack 3
  - Windows Server 2003, Enterprise Edition
- ISM Server Instrumentation Software, which is installed on the servers to be managed, can run on these operating systems. Always verify the supported operating system for your server in the README.TXT:
  - Windows 2000 Server, Service Pack 3
  - Windows Server 2003, Enterprise Edition
  - Novell NetWare†[1] 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†[2] server 8.0

Support for SNMP-Based Third-Party Server Management Software

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

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

The default ISM installation incorporates the integration software for these enterprise tools if it detects that they are installed on your system. In a custom installation, you can select the appropriate checkbox for integrating H-P OpenView Agent or CA Unicenter Agent.

NOTE

Regardless of the type of installation you choose (remote, custom, etc), the CA Unicenter software will only be installed on the local machine. Remote installation is not supported. Installation requires user interaction with a CA Unicenter-specific dialog. ISM installation will halt until you answer this dialog, then installation will resume.

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

---

[1] The Novell NetWare operating system is not supported on the SE7210TP1-E server platform.

[2] The Caldera OpenUnix operating systems is not supported on the SE7210TP1-E server platform.

On the console system(s) other than Network Node Manager and CA Unicenter, when configuring SNMP you must integrate MIB files into the SNMP management consoles (see page 24). SNMP services must also be installed and configured on the console system to enable Platform Event Traps used for ISM LAN Alerts (see page 30).

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

Console OS and Minimum Hardware Requirements

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

- Windows 2000 Advanced Server or Professional (Service Pack 3) or Windows XP Professional or Windows Server 2003, Enterprise Edition
- Intel® Pentium® microprocessor, Intel® Celeron® microprocessor, or higher
- At least 256 MB of RAM
- At least 120 MB of available disk space for the entire set of software
- Microsoft Windows-compatible modem must be used if you connect to servers by modem

Managed Server Requirements

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

For any server you need a login account with root or administrative privileges. The following requirements must be met for a managed server, depending on the OS. These are the requirements to install ISM, not to install the OS or other packages:

Windows Server Requirements

- Windows 2000 Advanced Server (Service Pack 3) or Windows Server 2003, Enterprise Edition
- 256 MB of RAM
- 120 MB of available disk space
- Windows SNMP service is required for connectivity with an SNMP-based third-party management console or to enable LAN Alerts (see pages 24 and 30)

NetWare Server Requirements

- NetWare[3] 6.0 Service Pack 1 or NetWare 5.1 Service Pack 3
- At least 96 MB of RAM
- At least 60 MB of available disk space
- The Transportation Independent Remote Procedure Call (TIRPC) runtime library for ONC RPC must be installed and running on NetWare before installing ISM (see page 15)

[3] The NetWare operating system is not supported on the SE-7210TP1-E server platform.

Linux Server Requirements

- Red Hat Linux 8.0 or AS 2.1[4]
- 32 MB of RAM
- 60 MB of available disk space

UNIX† Server Requirements

- Caldera OpenUnix 8.0[5]
- 32 MB of RAM
- 60 MB of available disk space

Overview of the Configuration and Installation Process

ISM configuration and installation involves both server and client systems as described below.

On Server Systems

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

1. Boot the server from the System Resource CD and run the Server Configuration Wizard. This process includes installation or update of the Service Partition[6] (described on page 131).
2. Install the server's operating system if one is not installed and prepare for ISM installation.
3. Install ISM from the ISM CD. For Windows-based systems, you can install ISM remotely on the server from the Console system as described below. For other operating systems you will have to take some manual steps on each server during the installation or install ISM individually on each server system (see page 16).
4. Do OS-specific configuration after the installation (see page 22).
5. Repeat the steps above for each server.

---

[4] If the kernel on the SE7210TP1-E server platform is not the kernel shipped with the Red Hat Linux 8.0 or AS 2.1 operating system you must download the correct driver and recompile it. For instructions on where to find the driver and on how to recompile it, see http://support.intel.com/support/motherboards/server/isc/software.htm.

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

[6] The Service Partition is not supported on the SE7210TP1-E server platform.

On Console Systems

For consoles that have an operating system the most straightforward way to configure the console and install the ISM software is:

1. Install any third-party enterprise management software (see page 8) with which ISM will integrate. This step is optional.
2. Install ISM software. For Windows-based systems, you can install console software and server instrumentation software locally or remotely, either from a console or server system (see page 16).
3. Do OS-specific configuration after the installation (see page 24).
4. Enable the LAN-Alert Viewer if you will use it on console systems (see page 30).

Connecting Consoles to Servers

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

- Local Area Network (LAN)
- Analog telephone modem (serial connection)[7]
- Local direct connection through a serial port[8]
- Intelligent Chassis Management Bus (ICMB)[9]

For typical management activities, a LAN is the preferred connection. In some cases where the network is inoperable or the OS is down, or for other emergency access, a modem or direct serial connection can let you manage a server from a console. An ICMB connection allows you to manage servers that are otherwise not supported by ISM, such as servers running non-supported operating systems. For any remote Out-of-Band management using the server management tools Direct Platform Control (DPC), Client System Setup Utility* (CSSU), or Command-Line Interface (CLI), the NIC1 port must be used.

[7] Serial connections are not supported on the SE7210TP1-E server platform.

[8] Direct connections are not supported on the SE7210TP1-E server platform.

[9] The ICMB is not supported on the SE7210TP1-E server platform.

2. Installation Steps

Step 1. Boot from the System Resource CD and Run the Configuration Wizard

1. Insert the System Resource CD in the server CD drive and reboot the system.

   When the server boots from the System Resource CD, the Server Configuration Wizard automatically launches. During start-up, the wizard probes the server to find out what should be configured. Depending on the state of the server the wizard will display the appropriate screens during the configuration process. For detailed information about fields in a particular screen, press the Configuration Wizard's help button.

2. The Configuration Wizard Start Screen describes the overall server preparation process. After reading through this process click the Continue button.

3. Make sure the Server Configuration Wizard is selected and click the Continue button to start the configuration process. Follow the directions on each screen. After you have supplied all the information on a given screen, click the Continue button to move forward in the process.

4. The wizard allows you to choose what you want to configure on the server. You will need to select the configuration options according to how you want to communicate with the server. For example, it is not necessary to configure the serial channel or set up alerting over the serial channel if you intend to use only a LAN connection for server management. However, if you want these alerting features over the serial channel you must select this channel for configuration and perform the configuration later in the wizard.

   The following steps outline the wizard's operation:

   a. Select which options to configure. The wizard selects default options for this server based on its initial probing during startup. Be sure that you select everything you want the wizard to allow you to configure.
   b. Set the date and time.
   c. Load the Sensor Data Records (SDRs).
   d. Load Field Replaceable Units Data Records (FRUs).
   e. Configure the LAN IP Address information.
   f. Configure remote server management options available over the LAN Channel. If you are going to use the Serial over LAN[10] (SOL) Redirection Mode through the Command Line Interpreter you must set the SOL baud rate to match the baud rate set in the BIOS on the managed server.
   g. Configure Alert Paging over the LAN Channel.
   h. Configure the Serial/Modem Channel.
   i. Configure remote server management options available over the Serial/Modem Channel.

[10] The Serial Over LAN feature is not supported on the SE7210TP1-E server platform.

j. Configure Alerting over the Serial/Modem Channel.
k. Set a system asset tag, if desired.
l. Install or update the Service Partition. This task is a two-step process with a server reboot between the two steps.
m. Save the configuration to a floppy disk for use with similar servers.
n. Save the configuration to the server.

Step 2. Install the Server's Operating System

If the server does not have an operating system installed, the Configuration Wizard displays a message to remove the System Resource CD, insert the bootable media that contains the operating system, and then reboot the system to complete installation of the operating system.

If the server already has an operating system installed, then you can just remove the CD and let the server reboot after configuration.

Be sure to disable the firewall (if applicable) on the server in order for the managing console to connect to the managed server.

Step 3. Prepare for ISM Installation

On a new server, before installing ISM and after running the Configuration Wizard and installing the server operating system, perform these steps:

1. Use the OS to configure communication links between the client console and the server, such as modems, LAN connections, etc. To use a direct serial link[11], you will need a null-modem cable. For a modem or serial link, you must configure a serial connection on both the managed server and the client workstation. For emergency communications with a server that has been powered off (note that the server must still be plugged in), the server's modem must remain powered on.
2. If you will use LAN Alerts (see page 30) or a third-party management software package, install and configure SNMP. Be sure to configure the service to automatically start or manually start the SNMP service (daemon) through the server's operating system, see the documentation specific to your OS.

   For Windows 2000 and Windows Server 2003 systems, install SNMP as follows:

   a. Open the Control panel and select the Add/Remove Programs applet.
   b. Click on the Add/Remove Windows Components icon.
   c. Click the Management and Monitoring Tools checkbox and then the Next button.

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

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

[11] Direct serial links are not supported on the SE7210TP1-E server platform.

3. Install and configure any third-party management software package you will use (this item is optional, see page 8).
4. Follow the preparation steps in the following sections for your specific operating systems.

Windows Preparation

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

Simple File Sharing on Windows XP Consoles

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

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

To avoid an installation failure, you can do any of the following:

- Install ISM locally instead of remotely
- Disable the Simple File Sharing capability on the remote system
- Make sure the remote system is part of a DOMAIN

NetWare Preparation

Before installing ISM on systems running NetWare[12], the Transportation Independent Remote Procedure Call (TIRPC) runtime library for ONC RPC or a substitute file set for NetWare must be installed and running. To install the TIRPC library, follow these steps:

1. Go to the *http://support.intel.com/* site and make the following selections:
   - Servers
   - Server Management and Maintenance
   - Intel Server Management
   - Software Drivers
   - Legacy Software Drivers
   - Transport Independent Remote Procedure Call (TIRPC) (listed under "Other Software")
2. Get the compressed (zipped) files TIRPC-IN.EXE, NLM4.EXE and INTRANET.EXE.
3. TIRPC installation:
   a. Unzip the TIRPC-IN.EXE file, including its subdirectories, to an empty floppy disk, using the –d option in the command line to preserve the directory structure
   b. Run NWCONFIG on the NetWare Server
   c. Select "Product Options"
   d. Select "Install a product not listed"
   e. Specify the source directory: "a:\"
   f. Select the package: "NetWare 4.0 TIRPC Runtime and Configuration files"
   g. Specify the destination directory: "sys:System"
   h. Wait for the installation to complete
   i. Exit NWCONFIG

[12] The NetWare operating system is not supported on the SE7210TP1-E server platform.

4. Installation of the INTRANET.EXE file:
   a. Unzip the INTRANET.EXE file to an empty floppy disk
   b. From a remote system, map a drive to the NetWare server
   c. Insert the floppy with INTRANET files in the remote system
   d. Copy all NLM files from the floppy to the SYS:System directory on the NetWare server
5. Configuration for TIRPC:
   a. Run NWCONFIG on the NetWare server
   b. Select "edit AUTOEXEC.NCF"
   c. Add the line "LOAD SPX_ND" before the LOAD/BIND or INITSYS.NCF statements (also called network initialization)
   d. Add the line "RPCSTART.NCF" after the LOAD/BIND or INITSYS.NCF statements , and include TCP/IP configuration if you want TIRPC to work over TCP/IP
   e. Add the line "ONCSP" after rpcstart.ncf
   f. Exit NWCONFIG
   g. Restart the server

OpenUnix Preparation

Before installing ISM on OpenUnix[13] systems, do the following on each server:

- Mcopy must be installed on each server. Please refer to the *man* page for doscp for download and install instruction for mcopy. Mcopy can also be installed by installing the mtools package from the OpenUnix 8.0 Skunkware 8 CD-ROM.
- Desktop Management Interface (DMI) must be installed on each server. By default, OpenUnix systems have DMI access set to read-only. This setting prevents ISM from changing sensor thresholds, enabling the watchdog timer, and executing other functions. To allow ISM to operate correctly, DMI access write permission must be enabled after the DMI installation.

Follow these steps:

1. Log in as 'root'.
2. Stop the DMI Service Provider (`dmi stop`).
3. Open the file /etc/rc2.d/S89dmi for editing.
4. In the dmistart() function, change the line `$DMI_PATH $@` to read `$DMI_PATH $@ -w`.
5. Save the file and restart the DMI Service Provider (`dmi start`). This change will remain valid for all future sessions.

Linux Preparation

If the kernel on the SE7210TP1-E server platform is not the kernel shipped with the Red Hat Linux 8.0 or AS 2.1 operating system you must download the correct driver and recompile it. For instructions on where to find the driver and on how to recompile it, see http://support.intel.com/support/motherboards/server/isc/software.htm.

[13] The OpenUnix operating system is not supported on the SE7210TP1-E server platform.

Step 4. Install ISM

ISM is delivered on its own CD which is separate from the System Resource CD. The ISM package contains both console and server instrumentation software. The default installation always attempts to install both console and server parts of the software if it detects that the system is a valid server (it contains a baseboard management controller chip, or BMC, etc.). If the system is not determined to be a server, only the console parts of the software are installed. When installing from a Windows-based system, you can specify automatic remote installation over the network to other systems that run supported Windows or NetWare operating systems (see page 9). For OpenUnix or Linux servers, you must individually install ISM on each system. Choose the installation instructions below according to the operating systems you use.

Each remote server on which you plan to install the ISM package must first be configured locally through the Server Configuration Wizard as described on page 13.

Installation for Windows Consoles and Windows or NetWare Servers

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

Use the instructions below to install remotely to Windows or NetWare[14] servers. To install locally to a NetWare server, simply run the setup.exe file on that server and ignore any details below that apply to remote installation.

⟹ NOTE

As of this release of ISM, on Windows Server 2003, the "Driver Signing Options" under System Properties should be changed to "Ignore - Install the software anyway and don't ask for my approval" before running the ISM 5.8 installation program." This is required until "signed" drivers have been made available. If performing a remote installation to a Windows 2003 system, ensure this setting is changed on the target machine.

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

Dialogs and Prompts During Windows Installation

- If prompted whether to run the program from its current location or download to disk, select "Run this program from its current location" (the CD) and click OK.
- If you receive a Security Warning asking whether you want to install and run SETUP.EXE from the CD, click Yes.

[14] The NetWare operating system is not supported on SE7210TP1-E server platforms.

- You will receive a prompt to select Local Install Only, Multiple System Install, or Custom Install. Select one and click Next, then read and accept the License Agreement.
  - — Local Install Only automatically selects your local system and installs all ISM components.
  - — Multiple System Install prompts for systems on the network which you can add to the installation, including the local system. It installs all ISM components on all systems that you add to the list. As you specify each server, a dialog prompts you for a login. Connect as a user with supervisor rights for each Windows or NetWare server. Otherwise the ISM installation will fail on that server. Select all the servers to be installed and follow the instructions on the screen to continue.
  - — Custom Install allows you to choose the parts of ISM to install (for an overview of the ISM components, see page 29). On this screen you can also select the support software that integrates ISM with H-P OpenView and/or CA Unicenter TNG. And, you can install the One-Boot Flash Update utility[15] from this screen (see page 27). After selecting the software components, select multiple systems on which to install as described above.
- If support (the integration agent) for the CA Unicenter TNG package is being installed on the local machine, the installation requires that you answer a CA Unicenter-specific dialog. ISM installation will halt until you answer this dialog, then installation will resume.
- The installation automatically reboots remote Windows servers and will reboot the local system unless you choose to stop it. Remote NetWare servers require a manual reboot following the first phase of ISM installation after ISM files have been copied to the target server.
- When installation is complete, view the file logfile.log in the installation directory of each system to verify that ISM installed correctly. The default installation directory for Windows is Program Files\intel\ServerManagement, however, you might have specified a different directory during installation.

Installation for OpenUnix Servers

On OpenUnix[16] systems follow these steps to install ISM:

1. Insert the ISM CD into the OpenUnix server CD drive.
2. Enter the mkdir command as follows:
   ```
   mkdir /cdrom
   ```
3. Enter the mount command as follows:
   ```
   mount –r –F cdfs /dev/cdrom/cdrom1 /cdrom
   ```
4. The ISM package is located in /cdrom/CD/Software/OpenUNIX/ismou.pkg; to install ISM, enter the command:
   ```
   pkgadd –d /cdrom/ism/software/openunix/ismou.pkg
   ```
5. Follow the onscreen instructions, which prompt you to read and accept a license agreement.
6. After a successful installation, you are prompted to reboot the system. First unmount the CDROM so you can remove the CD, then reboot the system:
   ```
   unmount /cdrom
   shutdown
   ```

[15] The One Boot Flash Update Utility is not supported on the SE7210TP1-E server platform.

[16] The OpenUnix operating system is not supported on the SE7210TP1-E server platform.

Installation for Linux Servers

For installation on systems using Red Hat Linux, install ISM individually on the Windows console using the directions above. Then install individually on each Linux server. You cannot do a remote installation of ISM onto a Linux server from the console. Server installation includes two parts: first you must install the Linux DMI service provider. Then you must install the ISM platform instrumentation software itself.

Depending on your configuration, you might install other software components on the server. Perform the following steps to work through the installation scenarios.

NOTE

This section refers to filenames that include version numbers. Note that these numbers, and therefore the filenames, may change as different versions of Linux are supported.

1. Insert the ISM CD into the Linux server CD-ROM drive.
2. The CD should automatically be mounted by the system. If not, you can mount the CD using either of the following methods:
   - Enter the mount command as follows:
     ```
     mount /mnt/cdrom
     ```
   - Use the Disk Management utility. To invoke this utility click the footprint icon, select **System**, and then select the **Disk Management** menu option. Click the Mount button beside /mnt/cdrom.
3. If you do not have a Terminal Command Line window open, click the icon in the operating system's tool bar to open the window.
4. Install the DMI Service Provider by following the instructions in Installing the DMI Service Provider on page 20.
5. Install the ISM PI server instrumentation software by following the instructions in Installing ISM PI Server Instrumentation Software on Linux on page 20.
6. If you plan on using the server to connect to other servers and to use the Command Line Interface (CLI) feature to communicate with them install the ISM CLI software by following the instructions in Installing ISM Command Line Interface Software on Linux on page 20.
7. If you are using a third-party SNMP management console to manage the server on which you are installing ISM, do the following:
   - Remove the Linux default SNMP packages by following the instructions in Removing the Default SNMP Packages Previously Installed by Red Hat on page 20.
   - Install the optional SNMP package by following the instructions in Installing the SNMP Package on page 21.
   - Install the DMI-to-SNMP Mapper by following the instructions in Installing the DMItoSNMP Mapper on page 21.

Installing the DMI Service Provider

1. Change your working directory by entering the following command:

   ```
   cd /mnt/cdrom/Software/linux/dmisnmp
   ```

2. Install the DMI service provider package located in the /Software/linux/dmisnmp directory on the ISM CD by using the rpm command. For example, the following command installs a version of the DMI service provider package:

   ```
   rpm –i dmisp-1.0-6.i386.rpm
   ```

   If you encounter errors concerning the libsnmp.so.0, use the `--nodeps` flag.

Installing ISM PI Server Instrumentation Software on Linux

1. Run the ISM install script from the Linux directory by entering the following commands at the command-line prompt:

   ```
   cd /mnt/cdrom/Software/linux/PI
   ./installme
   ```

2. Follow the instructions on your screen. The script prompts you to read and accept a license agreement. Next, the ISM install program determines the version of the Red Hat Linux kernel running on your server and installs the right version of the IPMI driver on your server. The script then proceeds to install the ISM package (e.g., ism-5.*x*-1.i386.rpm) on your server. In case the installation of the driver fails, the script displays appropriate error messages and then terminates without installing the ISM package. **DO NOT REBOOT AT THIS TIME**.

Installing ISM Command Line Interface Software on Linux

NOTE

The ISM Command Line Interface (CLI) feature applies only when managing other servers. You cannot use the CLI feature to manage the server on which CLI is installed.

1. Run the ISM CLI install script from the Linux directory by entering the following commands at the command-line prompt:

   ```
   cd /mnt/cdrom/Software/linux/cli
   ./installme
   ```

2. Follow the instructions on your screen. The script prompts you to read and accept a license agreement. Next, the ISM install program determines the version of the Red Hat Linux kernel running on your system and installs the right version of CLI on your system. In case the installation of the driver fails, the script displays appropriate error messages and then terminates without installing the CLI package. **DO NOT REBOOT AT THIS TIME**.

Removing the Default SNMP Packages Previously Installed by Red Hat

Red Hat installs the UCD-SNMP or NET-SNMP packages by default. ISM needs the SMUX subagent, which is not delivered in the default SNMP package. Therefore, this package will have to be removed so the correct one can be installed.

NOTE

The ucd-snmp or net-snmp (whichever applicable) package is often installed by default and will likely need to be uninstalled. If you uninstall ucd-snmp or net-snmp, you must also remove all related snmp and DMI packages. To determine the existence of these packages, use the commands:

```
rpm –qa | grep dmi
rpm –qa | grep snmp
```

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

To remove the default SNMP packages previously installed by Red Hat, use the following commands:

```
rpm –e ucd-snmp (or net-snmp)
rpm –e ucd-snmp-utils (or net-snmp-utils)
```

Installing the SNMP Package

Locate and install the ucd-snmp RPM, ucd-snmp-utils RPM packages. These packages are also located in the /Software/linux/dmisnmp directory on the ISM CD. Use the rpm command to install each package. For example, the following commands install versions of these packages. (Note that the numbers in these filenames may change for different versions of Linux supported.):

```
rpm –i ucd-snmp-4.2.4-3.i386.rpm
rpm –i ucd-snmp-utils-4.2.4-3.i386.rpm
```

Installing the DMItoSNMP Mapper

1. Install the DMI-to-SNMP Mapper located in the /Software/linux/dmisnmp directory on the ISM CD by using the following rpm command

   ```
   rpm –i dmi2snmp-1.0-15.i386.rpm
   ```

2. To make the snmpd daemon startup at runlevels 3, 4, and 5, add the following symbolic links by executing the commands below:

   ```
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc3.d/S20snmpd
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc4.d/S20snmpd
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc5.d/S20snmpd
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc3.d/K20snmpd
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc4.d/K20snmpd
   ln -s /etc/rc.d/init.d/snmpd /etc/rc.d/rc5.d/K20snmpd
   ```

Step 5. Configure Servers After Installing ISM

SNMP Installation

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

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

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

NIC SNMP Installation

In order to receive SNMP traps for network interface card (NIC) events, you must install specific NIC SNMP software from the following Intel web site:

http://support.intel.com/support/network/adapter/1000/software.htm

Download the Native SNMP software for your operating system and follow the installation and configuration instructions included in the download package.

Customizing Windows Servers After Setup

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

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

Customizing NetWare Servers After Setup

The PIC installation installs support for third-party instrumentation on the NetWare[17] server but does not enable the instrumentation support. To enable support for any or all instrumentation, you must edit the AUTOEXEC.NCF file in the SYS:SYSTEM directory as follows:

Make sure the following line appears (add it if necessary):

```
rpcstart.ncf
```

Before the line:

```
isc_on.ncf
```

[17] The NetWare operating system is not supported on the SE7210TP1-E server platform.

To enable the Adaptec† SCSI instrumentation, edit the ISC_ON.NCF file in the SYS:SYSTEM directory and remove the word REM from these lines:

```
REM load nwaspi
REM load iomgr
REM load ciodmi
```

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

1. Change the `ReadOnly` entry in the *SYS:\SYSTEM\sdlink.cfg* file to `True.`
2. Reboot the server.

Customizing OpenUnix Servers After Setup

On servers running OpenUnix[18] the set action of some SNMP attributes causes the server to shutdown/power off. To globally disallow all set requests:

1. Change the `ReadOnly` entry in the /usr/local/ism/bin/sdlink.cfg file to `True`.
2. Reboot the server.

Customizing Linux Servers After Setup

1. Verify that the dmi2snmp and ucd-snmp packages are installed. For example, the files `dmi2snmp-10-15.i386.rpm` and `ucd-snmp-4.2.4-3.i386.rpm` could represent the dmi2snmp and ucd-snmp packages, respectively.
2. Open the file `/etc/snmp/snmpd.conf`. You can use any available editor such as vi, emacs, or a linux editor.
3. Search for "com2sec" and set the community string to the proper setting for your network.

```
##      sec.name          source        community
com2sec notConfigGroup    default       mycommunitystring
```

4. Search for "group" and verify that the following lines are present:

```
#       groupName         securityModel      securityName
group   notConfigGroup    v1                 notConfigUser
group   notConfigGroup    v2                 notConfigUser
```

5. Search for "view" and specify the desired subtree range (suggested range shown in bold below).

```
##          view          incl/excl     subtree      mask

view        all           included      .1     80
```

6. Search for "access" and set the "read" column to whatever you specified in the "incl/excl" column of the view line (step 4 above).

```
#       group           context sec.model sec.level prefix    read   write notif
#access notConfigGroup ""       any      noauth    exact     systemview all none
access  notConfigGroup  ""      any      noauth    exact     all     all  none
```

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

7. Add a trapsink line at the end of the file for each management console that receives traps from the managed server. Use the following syntax when adding the line:

   ```
   trapsink localhost
   ```

   Be sure to substitute appropriate strings for the host name and domain. Add "trapsink" lines for any additional hosts that will be receiving trap messages from this server.
8. Insert the following text above the "trapsink" line you added in the previous step.

   ```
   smuxpeer .1.3.6.1.4.1.412 commander
   smuxpeer .1.3.6.1.4.1.412.1.2 trapper
   ```

9. Save and close the snmpd.conf file.
10. Reboot the server.

Create an SMNPv3 User Account

1. Open the file /etc/snmp/snmpd.conf.
2. Create a user account with read-write access, which the snmpd daemon will use on the local server.
3. Set a password for the snmp daemon's user account by adding the following line to /var/ucd-snmp/snmpd.conf (be sure to stop the snmpd daemon using `/etc/rc.d/init.d/snmpd stop` before editing the file):

```
createUser -e 0x001122(engind ID) username MD5 md5_password DES des_password
```

   For example,

   ```
   createUser  -e 0x001122 janedoe   MD5  mysecretpass
   ```

   Once you have added the line, restart the snmpd daemon using the following command.

   ```
   /etc/rc.d/init.d/snmpd start
   ```

NOTE

The set action of some SNMP attributes causes the server to shutdown/power off. To globally disallow all set requests, edit the /etc/rc.d/init.d/dmi2snmpd *file as follows:*

Under the case for start, change the line ./dmi2snmpd *which starts the DMI to SNMP translator daemon to* ./dmi2snmpd –w.

4. Reboot the server.

Step 6. Configure Console Systems After Installing ISM

Configure SNMP for LanAlert Viewer

If you will use the LanAlert Viewer to receive alerts on a Windows console, you will need to enable SNMP services on that console system (see page 30 for information about LAN Alerts). Verify that "SNMP Service" and "SNMP Trap Service" are running on the console system. If they are not, install these services using the Windows installation CD. This lets you receive special SNMP traps as generated by the server firmware that will report on changes in server health or condition.

For information about the format of SNMP traps used by LanAlert, see the ISM Technical Product Specification, available at Intel's Web support site (page 7).

Load MIB Files for SNMP Integration

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

- BASEBRD4.MIB
- IOMMIB.MIB: (Adaptec SCSI used with ISM 5.5.3 and 5.5.4)
- CIO400I.MIB: (Adaptec SCSI used with all other ISM and ISC releases)
- FTDMISVCI.MIBL (Promise† IDE)
- ICMBFEAT.MIB
- LRA.MIB
- RMTCHAS.MIB
- SHA.MIB
- SYMBIOS4.MIB: (LSI† Logic)

⟹ NOTE

For the Intel® LAN Adapter, use the MIB file included in the software download package that you downloaded as part of the NIC SNMP software installation, described on page 7.

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

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

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

⟹ NOTE

Make sure to load the most current MIB files released with ISM to support current features. If you loaded files from an earlier release, unload them and reload from the current CD.

Support for Linux Servers

To capture the DMI information on Linux servers to be managed by PIC software, the following MIB files must also be loaded in the third-party management software tool (H-P OpenView or CA Unicenter TNG) as described above.

- MAPBASE4.MIB
- MAPLRA.MIB
- MAPSHA.MIB

Uninstalling ISM

Uninstalling ISM from Windows or NetWare Systems

To uninstall ISM itself or components of ISM from servers running Windows or NetWare[19], run the uninstall.exe file that is installed with the system. You can also select ISM Full Uninstall from the Windows Start menu or use the Add/Remove Programs utility in the Control Panel. You can uninstall ISM from Windows or NetWare servers either locally (one at a time) or remotely from a Windows console system.

Uninstalling ISM from OpenUnix Systems

You must uninstall ISM locally from each OpenUnix[20] system. To do so:

1. Log in as 'root'.
2. Enter the command:
   ```
   pkgrm ism
   ```
3. Follow the instructions on the screen.

Uninstalling ISM from Linux Systems

You must uninstall ISM locally from each Linux system. To do so:

1. Log in as 'root'.
2. Enter a series of commands as listed below to remove installed packages. (Some packages might not be installed.) After each command, you will receive a prompt to reboot the system. You need not reboot until after all the packages are removed:
   ```
   rpm –e ism
   rpm –e ipmidrvr (see note below)
   rpm –e dmi2snmp
   rpm –e dmisp
   rpm –e ucd-snmp-utils
   rpm –e ucd-snmp
   ```
3. After the final command above, you may receive some error messages, which can be ignored.
4. Reboot the system.
5. The commands above remove the specific SNMP packages used by ISM. If you want to use SNMP for other purposes, reinstall it from the Linux CD.

NOTE

The ipmidrvr package is used by the One-Boot Flash Update utility. If this utility is installed concurrently with ISM, then do NOT remove the ipmidrvr package, or else the One-Boot Flash Update utility will fail to function properly.

---

[19] The NetWare operating system is not supported on the SE7210TP1-E server platform.

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

Installing the One-Boot Flash Update Utility

This section describes the installation procedure for the One-Boot Flash Update utility[21], which is described in further detail in Chapter 9 on page 127.

Windows Installation

To install this utility on Windows, simply select the checkbox on the Custom Install screen of the Windows installation program during ISM installation, as described on page 17.

NOTE

In order to run this utility, the working directory must first be set to the directory in which the utility is installed. This is required because the utility depends on certain files, which are expected to be located in the working directory. For a normal installation, the One-Boot Flash Update utility is installed in the following directory:

C:\Program Files\Intel\ServerManagement\bin\flashupdt

Linux Installation

Perform the following steps to install the One-Boot Flash Update Utility on a Linux system.

1. Verify that the w3c libraries distributed as part of Red Hat Linux 8.0 are present on the system, and if not, install them according to the Red Hat Linux documentation.
2. Insert the ISM CD into the Linux server CD-ROM drive (be sure to mount the drive first).
3. Run the utility install script from the Linux directory by entering the following commands at the command-line prompt:

```
cd /mnt/cdrom/ism/Software/linux/ofu
./installme
```

4. Follow the instructions on your screen.
   a. The script prompts you to read and accept a license agreement.
   b. Next, the script tries to verify that the w3c libraries are installed. If the w3c-libwww package is not installed, then the script will exit and display a message indicating that the w3c-www package must be installed prior to installing the One-Boot Flash Update utility.
   c. If the w3c-libwww package is already installed, then the *installme* script will install the One-Boot Flash Update utility, which is located in the rpm package with the file name ***flashupdt-1.0-1.i386.rpm***.
   d. Next the *installme* script determines the version of the Red Hat Linux kernel running on your server and installs the right version of the IPMI driver on your server, if it is not already installed. The IPMI driver for each supported kernel version is located in the *Software/linux/IPMIDriver* directory in the appropriately named RPM package, (*eg.,* ipmidrvr-x.x.x.x-1.i386.rpm). Depending on the kernel version that is running, the correct IPMI driver package will be installed.

[21] The One Boot Flash Update utility is not supported on the SE7210TP1-E server platform.

e. If the version of the kernel is the Red Hat 8.0 SMP kernel, then the *installme* script installs the SMP version of the flash update driver on your server. The flash update driver is located in the rpm package with the file name ***ofudrvr-2.4.18.14smp-1.i386.rpm***. If the kernel is not SMP, then you may recompile the flash update driver using source code available from support.intel.com.

5. Upon successful completion of the *installme* script, the utility and the flash update driver files will be located in the */usr/local/flashupdt* directory.

NOTE

In order to run this utility, the working directory must first be set to the directory in which the utility is installed. This is required because the utility depends on certain files, which are expected to be located in the working directory.

Uninstalling the One-Boot Flash Update utility from Linux Systems

You must uninstall the One-Boot Flash Update utility locally from each Linux system. To do so:

1. Log in as 'root'.
2. Enter a series of commands as listed below to remove installed packages.

```
rpm –e ofudrvr
rpm –e ipmidrvr  (see following note)
rpm –e flashupdt
```

NOTE

The ipmidrvr package is used by other ISM components. If ISM is installed concurrently with the One-Boot Flash Update utility, then do NOT remove the ipmidrvr package, or else ISM will fail to function properly.

3. Intel Server Management (ISM) Concepts

ISM Components

ISM includes the following server management tools:

NOTE

NIC1 is the LAN port for Out-of-Band management on all IA-32 systems. This is the port that must be used for all Out-of-Band remote management using DPC, CSSU[22] and CLI.

Intel Server Management Console: The ISM Console provides basic server management functions. It lets you discover servers that have ISM installed, and allows you to run Platform Instrumentation Control (PIC), Direct Platform Control (DPC), DMI Explorer, and Client System Setup Utility (CSSU). See page 31 for more information on the ISM Console.

Platform Instrumentation Control (PIC): PIC is the main administrative access for configuring alerts and monitoring the state of servers when the server operating system is running and the server is on the network. It monitors platform sensors and manages alerts based on events that you can configure. PIC communicates over the LAN to the Platform Instrumentation (PI) software on the server, using standard DMI/RPC protocols. For detailed information on using the PIC, see Chapter 4 or click the Help button in the PIC Console.

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

DPC communicates either with the serial Emergency Management Port[23] (EMP), which is a serial port for modem or direct link, or over the LAN using the onboard NIC(s) on the server. For more information on using DPC, see Chapter 5 or click the Help button in the DPC console.

Client System Setup Utility* (CSSU): CSSU is a remote interface to the SSU (described on page 131). Use CSSU for low-level configuration and updates. It communicates over a channel opened by DPC. For more information on using CSSU, see Chapter 6 or click the Help button in the Client SSU program.

DMI Explorer: DMI Explorer is an interface in the ISM Console that lets you discover DMI details about servers on the network. It is automatically installed with the ISM Console. It shows attribute values for each DMI-compliant component, and you can use it to manage third-party DMI-compliant components. If the server has a SCSI controller or LAN adapter you can view their status with DMI Explorer.

---

[22] The Client System Setup Utility (CSSU) is not supported on the SE7210TP1-E server platform.

[23] The Emergency Management Port (EMP) is not supported on the SE7210TP1-E server platform.

LAN-Alert Viewer: The LAN-Alert Viewer receives alerts over a LAN connection, as opposed to numeric pages which are sent over a serial connection. The LAN-Alert Viewer runs on the client system to monitor alerts. For more information, see page 30 or click Help in the LanAlert Viewer.

Command Line Interface (CLI): The CLI lets you manage servers from a Windows or Linux client using a command interface. You can enter commands directly or from a script. For information on installing, configuring and using the CLI, see Chapter 7.

Native Command Line[24]: Native Command Line gives you direct access to the server's Baseboard Management Controller (BMC) using text commands over a serial connection. See Chapter 8.

Setting Up and Using Alerts

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

- LAN Alerts provide a means of notification over the network to the console system.
- Platform Event Paging is a service that notifies a numeric pager.
- Email Alerting sends a notice to specified email IDs.
- System ID LED alerts use the system ID LED to indicate a system requiring attention.

LAN Alerts

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

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

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

You can configure LanAlert to detect:

- Temperature or voltage sensors out of range
- Fan failures
- Chassis intrusion (security violation)
- Power supply faults

[24] The Native Command Line feature is not supported on the SE7210TP1-E server platform.

- Uncorrectable ECC memory errors
- POST error codes or boot failures
- Watchdog Timer reset, power down, or power cycle
- System reboot

On the server you use SSU to configure:

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

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

Platform Event Paging (PEP)

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

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

To configure the paging string and event filters, use PIC or CSSU on the console, or use SSU on the managed server. The paging string includes all the information to connect to the pager as well as the message to send. Paging is one of the alert actions you can configure in the PIC. Please see the specific sections on PIC (page 37) and CSSU (page 75) for details on setting pages with these components.

Paging alerts can be configured for the same events as supported by LanAlert (page 30).

Email Alerts

You can use the PIC to configure an email address to receive alerts for any of the same events as supported by LAN-Alert and Platform Event Paging. Unlike the other two alert methods, you cannot configure email alerting with the CSSU or SSU. (For more information see page 65.)

Launching ISM Tools

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

Supported third-party management software includes:

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

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

ISM Console

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

1. Click Start, and select Programs.
2. Select Intel Server Management, and then click on ISM Console.

H-P OpenView Network Node Manager

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

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

CA Unicenter TNG

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

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

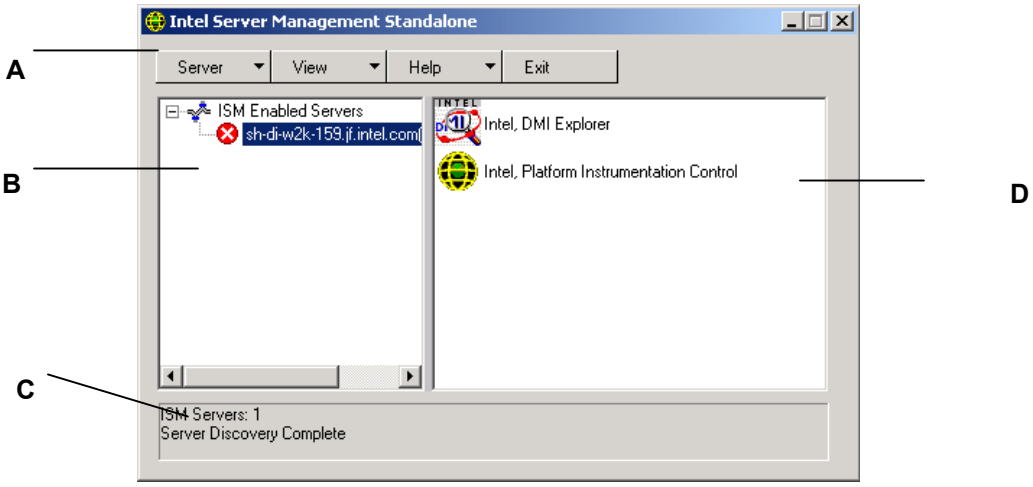
Using the ISM Console

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

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

ISM Console Main Screen

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



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

ISM Console Button Bar

The Button Bar includes the following options:

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

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

Server Menu Options

Discover

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

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

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

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

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

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

Add

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

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

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

Delete/Delete All

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

To delete a server, do the following:

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

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

Stop Discovery

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

View Menu Options

Icon View/List View

Changes the format of the icons in the Tool Pane.

The Navigation Pane

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

The Tool Pane

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

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

The Status Bar

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

4. Platform Instrumentation Control (PIC) Details

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

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

PI can also provide instrumentation data for servers connected through the Intelligent Chassis Management Bus (ICMB). PIC interacts directly with only servers running PI and a supported OS. Through that managed server, PIC can use the ICMB interface to manage other Intel servers that are not running PI or are running a supported operating system. You need a functioning LAN connection from the client system to the server running PI. (For more information about configuring ICMB, see page 57.)

NOTE

Connection to managed servers through the ICMB is not supported on SE7210TP1-E server platforms.

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

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

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

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

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

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

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

Using PIC

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

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

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

Main Menu Bar

The Main Menu Bar includes the following options:

Item	Options
File Menu	**Exit:** Exits the application
View Menu	**Toolbar:** Toggles the toolbar on or off. **Status Bar:** Toggles the status bar on or off. **Large Icons:** Displays list using large icons. **Small Icons:** Displays list using small icons. **List:** Displays items in list format. **Details:** Displays items in detail format. **Arrange Icons:** Arranges icons by name or status. **Refresh:** Triggers an immediate screen and data refresh. **Options:** Displays the view options dialog so you can configure viewing preferences, such as temperature format and display refresh rate.
Configure Menu	**Enable Front Panel Power & Reset[25]:** Toggles the front panel power and reset option. **Immediate Power Off Server:** Powers off the server and you must manually restart power or use another interface like DPC to restore power. The PIC window will disappear. **Immediate Hardware Reset Server:** Resets the server. The PIC window will disappear. **Enable Watchdog Timer:** Toggles the watchdog timer option. **Watchdog Timeout Value:** Set the watchdog timeout value, which will take effect if the timer is enabled. **Paging Configuration[26]:** Lets you configure Paging Alerts (see page 61). **Email Alert Configuration:** Lets you configure Email Alerts (see page 65). **Restore Factory Defaults:** Restores default values for threshold sensors and the Watchdog Timer.
ID LED Menu	**LED Status:** Displays the current state of system ID LED as choices in the drop down menu. • **On** - This item is only enabled, as indicated by a dot next to it, if the system ID LED is turned on (using 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. See page 54 for information on setting LED alerts.
ICMB Menu*	**View Managing Server:** Views the managed server to which PIC is directly connected (the one managing the downstream ICMB servers). **View Managed Server(s):** Views the ICMB-managed servers to which PIC is indirectly connected through the primary managed server. **Reclaim Inactive Resources:** Reclaims inactive ICMB resources on the managing server.

continued

[25] The SE7210TP1-E server platform does not support the Front Panel Power and Reset buttons.

[26] Paging Alerts are not supported on the SE7210TP1-E server platform.

Item	Options
SMaRT Tool	**Launch SMaRT Tool:** Launches the SMaRT Tool, a separate product provides information about your specific server hardware. If the SMaRT Tool location is not known, you will be prompted to use the Locate… menu. **Locate…:** Attempts to open the SMaRT Tool executable (SMaRT.EXE), either on the local system or on any local drive or network drive to which it is attached. Once located, the Launch SMaRT Tool option always attempts to launch it from this location.
Help Menu	**Help Topics:** Accesses PIC help topics. **About PIC:** Displays PIC version information.

Toolbar

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

Navigation Pane

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

Status Bar

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

Presentation Pane

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

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

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

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

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

  The sensor status is also represented as a colored "Health" icon: Red is critical, Yellow is noncritical, Green is OK, and Blue is unknown status.

- **Alert Actions**—Displays the currently configured alert actions for each threshold type (such as Voltage-Status Changed to Upper Critical, Voltage-Status Changed to Lower Critical).

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

Display Details

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

Health

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

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

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

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

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

Chassis

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

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

Fan Sensors

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

PIC monitors two types of fans:

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

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

- Cooling Unit redundant fan arrays—PIC can display fan redundancy status for systems equipped with multiple redundant fans in a cooling unit. See the table below for a list of cooling unit states and their meanings.

⟹ NOTE

Fan redundancy is not supported on SE7210TP1-E server platforms.

Fully Redundant	The cooling unit is fully redundant.	No severity
Redundancy Lost	The unit has lost redundancy.	Critical
Redundancy Degraded	The unit is still redundant, but not fully redundant.	Non-critical
Non-redundant Sufficient Resources From Redundant	Redundancy has been lost, but the unit still has enough fan resources to operate normally. This state is entered when one or more fans are lost.	Critical

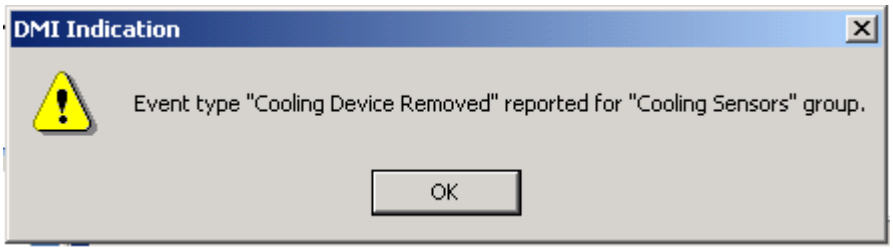
continued

Non-redundant Sufficient Resources From Insufficient Resources	The unit has regained enough fan resources to once again operate normally, but is still not fully redundant. This state is entered when one or more fans are regained.	Critical
Non-redundant Insufficient Resources	The unit is non-redundant and has insufficient fan resources to maintain normal operation.	Critical
Redundancy Degraded From Fully Redundant	The unit has lost some fan resources, but is still in a redundant state. This state is entered when one or more fans are lost.	Non-critical
Redundancy Degraded From Non-redundant	The unit has regained some fan resources and is redundant, but not fully redundant. This state is entered when one or more fans are regained.	Non-critical

For example, consider a system that requires five fans for full redundancy, but operates normally with four fans. If one fan fails, the cooling unit status is shown as Non-Redundant Sufficient Resources From Redundant, because a fan was lost. If another fan fails, leaving three fans operational, the status becomes Non-Redundant Insufficient Resources. When one of the two failed fans resumes working, the status becomes Non-Redundant Sufficient Resources From Insufficient Resources, because a fan was regained.

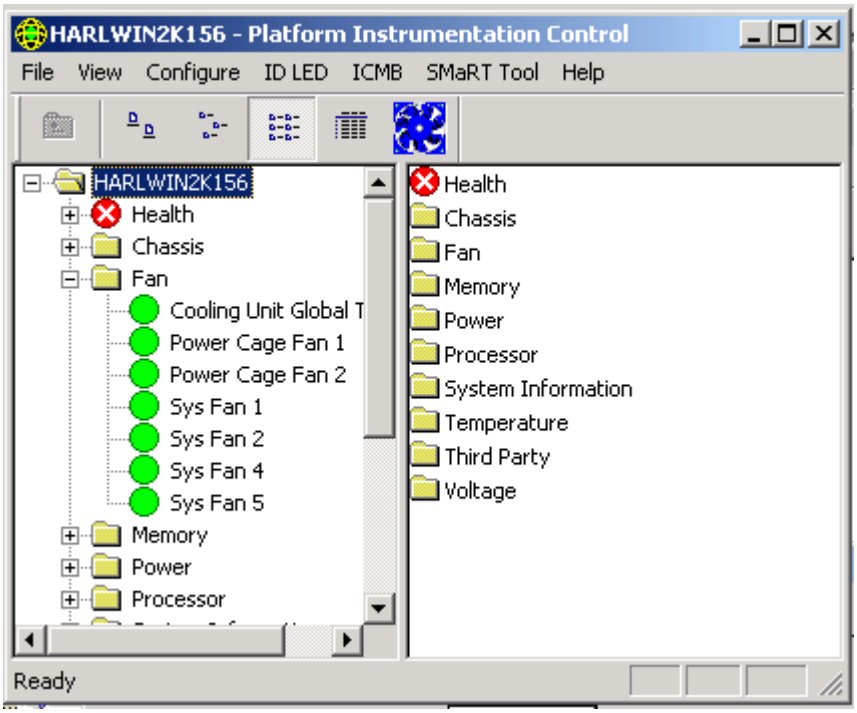
Hot Swap Fans

For systems that support Hot Swap Fans[27] (*i.e.*, fans that can be removed and reinserted while the system running), PIC displays the fan status ordered by the system's fan slot number. If a fan is removed, PIC sends an alert message to the managing console, as shown below.

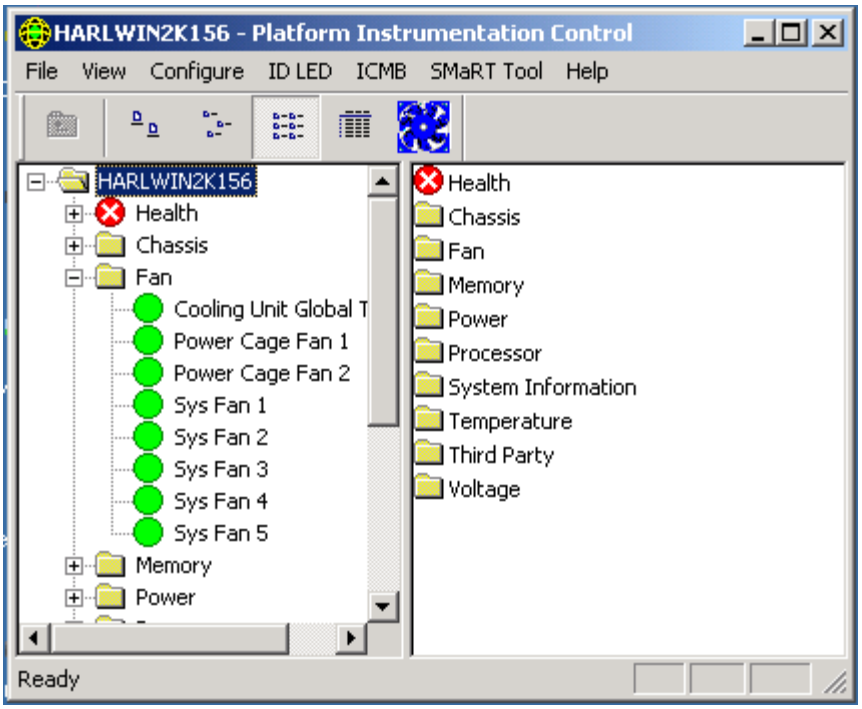


PIC also refreshes the PIC interface so that the removed fan is no longer reported. For example, if the system supports five fans, and Fan 3 is removed, PIC will display status for Fan 1, Fan 2, Fan 4, and Fan 5, with no entry at all for Fan 3.

[27] Hot Swap Fans are not supported in the SE7210TP1-E server platform.



If a fan is installed or reinstalled, PIC sends an alert to the managing console and refreshes the PIC interface, as shown below, reporting the newly installed fan.



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

The SE7210TP1-E server platform does not support the ICMB.

The ICMB provides additional troubleshooting and status capabilities by providing information that can be used to predict and identify failures on multiple servers. The ICMB is used to provide remote power control and status information on servers that cannot be normally obtained through in-band channels. This may be because the information is not provided through those channels or because the in-band channels are not available, such as when the chassis is powered down. The ICMB, as with other instrumentation described in this document, is accessed by Intel Server Control.

ICMB provides the ability to communicate information such as:

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

On SR460AC4 based systems the ICMB controller is embedded "I/O Legacy Board." On previous systems the ICMB card was plugged into a standard expansion slot and into the IPMB cable system board connector.

For more information about ICMB, see page 57.

Memory Displays

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

- Memory Devices
- Memory Arrays

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

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

Single-Bit Error (SBE) Handling

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

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

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

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

Multiple-Bit Error (MBE) Handling

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

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

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

Comparison of Single-bit Errors to Multiple-bit Errors

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

SBE and MBE Comparison

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

PCI HotPlug Device

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

Power Supply and Power Unit

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

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

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

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

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

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

Redundant Power Supply

PIC supports redundant hot swap power supplies (i.e., power supplies that can be removed and reinserted while the system is running). If a hot swap power supply is removed while the system is running, PIC sends an alert message to the console and refreshes the PIC interface to show which hot swap power supply has been removed. When a power supply is inserted or reinserted, PIC sends an alert message to the console and refreshes the PIC interface to show the status of the newly inserted power supply unit.

NOTE

The SE7210TP1-E server system does not support redundant power supplies.

Processor

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

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

System Slots

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

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

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

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

System Information

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

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

Temperature

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

Third-Party Components

Third Party onboard devices, such as the SCSI controller, can be managed by ISM. You can configure event actions for DMI indications generated by third-party Server Instrumentation installed with PI. You can also monitor third-party instrumentation via the DMI Explorer Interface. See page 56 for details about event configuration for third party instrumentation.

Voltage

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

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

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

Managing Servers with PIC

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

Viewing and Configuring Sensor Information

To view or configure a sensor, do the following:

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

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

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

Viewing System Information

To view system information (such as FRU, Operating System, BIOS, and SEL) on the managed server or a managed ICMB[28] device, do the following:

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

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

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

System Event Log

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

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

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

Configuring Thresholds

There are two basic types of thresholds:

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

To Configure a Range-Based Threshold

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

- Upper Critical
- Upper Non-critical
- Lower Non-critical
- Lower Critical

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

---

[28] The Intelligent Chassis Management Bus (ICMB) is not supported in the SE7210TP1-E server platform.

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

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

- Status Changed to OK
- Status Changed to Upper Critical
- Status Changed from OK to Upper Non-critical
- Status Changed from Critical to Upper Non-critical

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

To configure a range-based threshold:

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

NOTE

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

To Configure a State-Based Threshold

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

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

NOTE

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

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

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

Cautions in Setting Thresholds

Rounding of Threshold Values

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

Avoiding a Power On/Off Loop

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

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

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

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

OR

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

Avoiding a Reboot-Fail Retry Loop

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

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

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

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

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

Configuring Threshold Event Actions

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

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

NOTE

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

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

Notification Action	Description
Emit a beep from the managed server's speaker	Speaker beeps.
Display an alert message on the managed server	Default action for non-critical and critical indications. The message box stays up until acknowledged. On OpenUnix and Linux the alert message is displayed as a text message on the server console.
Log the event to disk	Default action for all indications. This option records the event in the standard system error log. On NetWare, PIC records the event in the System Log file, SYS$LOG.ERR which is typically in the SYS:SYSTEM folder. On Windows 2000 and Windows Server 2003, PIC records the event in the Windows System Event Log, which you can view with the Windows Event Viewer under Control Panel > Administrative Tools. On OpenUnix, events are logged in the system log file: /etc/.osm. On Linux, events are logged in the system log file: /var/log/messages.
Broadcast a message	Default action for critical indications. On NetWare, the message goes to all users currently logged into the managed server with Administrator or Supervisor privileges. On Windows 2000 and Windows Server 2003, the message goes to all the users currently logged into the managed server, including systems which have a drive mapped to the server. On OpenUnix and Linux a text message is sent to all users currently logged onto the UNIX server.
Page an administrator[29]	A page is sent to a specified pager, with a message that can include the phone number of the server, an ID number, or other numerical information.
Email	An Email with appropriate alert messages is sent to the specified users.
Set LED On or Off	The system's ID LED is set to On or Off, depending on which of the two check boxes you select. You can turn the ID LED on or off manually using PIC's ID LED menu.

Power Control Action	Description
No shutdown	Default action for all indications. Select this option if you do not want to shut down or reset the server when an event occurs.
Shutdown the OS[30]	Select this option if you want to shut down the OS gracefully (controlled, closing files and applications). On NetWare, the server is returned to DOS. On Windows 2000 and Windows Server 2003, the server is set to a state ready for manual power-off or reset. On OpenUnix and Linux standard shutdown is completed and system prompts for reboot or power off.
Shutdown the OS and power off	Select this option if you want to shutdown the OS gracefully and turn off the system power.

Continued

[29] Paging is not supported in the SE7210TP1-E server platform.

[30] The SE7210TP1-E server platform does not support a graceful shutdown of the operating system.

Power Control Action	Description
Shutdown the OS and hardware reset	Select this option if you want to shutdown the OS gracefully and reset the server via hardware.
Immediate power off	Select this option if you want to immediately power down the server. This action is an immediate power-off without a shutdown of the OS; it might corrupt files.
Immediate hardware reset	Select this option if you want to immediately reset the server via hardware. This action is an immediate hard reset without a shutdown of the OS; it might corrupt files.
Immediate NMI	Select this option if you want to cause a hardware Non-Maskable Interrupt (NMI). If this feature is not supported on the managed server, this option is grayed out.

Overriding Power Off or Shutdown Actions

You can globally override power off or shutdown actions while allowing other event actions (*e.g.*, paging[31], broadcast message, etc.) to take place. There are two ways:

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

  Windows 2000 and Windows 2003

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

  NetWare

  Set the `NotificationOnly` parameter in the *SYS:\SYSTEM\lra.cfg* file to `TRUE` and reboot the server.

  OpenUnix

  Set the `NotificationOnly` parameter in the */usr/local/ism/bin/lra.cfg* file to `TRUE` and reboot the server.

  Linux

  Set the `NotificationOnly` parameter in the */usr/local/ism/bin/lra.cfg* file to `TRUE` and reboot the server.

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

[31] Paging is not supported in the SE7210TP1-E server platform.

Configuring Third-Party Event Actions

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

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

To configure event actions for third-party indications:

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

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

Controller	Choices
Adaptec SCSI*	**Storage Device Events Group** Storage Device - Status OK (Informational Event) Storage Device - Status Changed to Non-Critical (SMART Event or Recovered) Storage Device - Status Changed to Critical **Storage Controller Events Group** Storage Controller - Status OK (Informational Event) Storage Controller - Status Changed to Non-Critical Storage Controller - Status Changed to Critical **Enclosure Events Group** Storage Enclosure - Informational Event
LSI Logic SCSI*	**Storage Devices Events Group** Device Error (not responding) Device Warning (predicted failure(S.M.A.R.T.)) **Storage Controller Events Group** Controller Error (not responding) **Mass Storage Association Events** New Storage controller detected New device detected Existing controller changed Existing device changed

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

Continued

Controller	Choices
QLogic SCSI	**Storage Devices Events** New or Recovered Storage Device Error Storage Device Not Responding Device Warning (predicted failure (S.M.A.R.T.)) **Storage Controller Events** Informational SCSI Controller Event Non-Critical SCSI Controller Error Critical SCSI Adapter Event
Promise IDE	**Mass Store Logical Drive Events** IDE RAID Array OK Non-Critical IDE RAID Array Event IDE RAID Array Off-line **Disk Events** IDE Disk Status OK IDE Disk Status Critical
Intel LAN Adapter (These events are available only for Windows 2000 servers)	**NIC Health Contributor** Cable unplugged/No LAN activity Adapter line up Adapter initialization failure **NIC Teaming Events** Primary Adapter is switching over and the Secondary Adapter took over Primary Adapter became active Secondary Adapter is deactivated from the team Initialization Failure The last Adapter has lost link. Network connection has been lost Preferred Primary Adapter has been detected The team has only one active adapter Secondary Adapter has re-joined the team Preferred Primary Adapter has taken over Network Connection restored

Setting Up an ICMB Connection

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

⇒ NOTE

The SE7210T1-E server system does not support the ICMB.

- You must 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 that you wish to manage or monitor through ICMB must be physically connected through their respective ICMB interface ports. For example, the Management Point Server is connected to a server, while that server is connected to another server all using ICMB connections.

For more details (if applicable) on connecting a specific server platform for ICMB management, refer to the server's product guide.

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:

Windows 2000 and Windows 2003 systems

1. Go to the Services control panel.
2. Start the Intel EIF Agent service[32].

NetWare[33] systems

1. Open the `ISC_ON.NCF` file for editing.
2. Remove "rem" from the following line:

   ```
   rem load eif
   ```

   Making this change causes the EIF service to be started each time the ISM services are started on the Management Point Server.

Unixware systems

Enter the following command at the console prompt on the Management Point Server:

```
/etc/init.d/ism start-icmb
```

You can stop the service by entering the following command:

```
/etc/init.d/ism stop-icmb
```

Setting Up ICMB

The Intelligent Chassis Management Bus (ICMB) feature allows you to interconnect and share management information among multiple remote devices even when these devices do not have Intel's server management software installed. For example, your managed server could be configured to be an ICMB Management Point[34] Server and report management information on ICMB devices connected to it through ICMB cabling. Using the ICMB feature, PIC can manage the power state of remote ICMB devices and view FRU information about those devices. The amount of FRU information available depends on the type of ICMB device you are trying to manage.

---

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

[33] The NetWare operating system is not supported on the SE7210TP1-E server system.

[34] 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.

NOTE

The SE7210T1-E server system does not support the ICMB.

In order to use the ICMB feature, you must be sure that you have chosen one server to be a Management Point Server and started the EIF service on that system[35].

Discovering Remote ICMB Systems

Before you use the ICMB feature to look at connected servers, you must configure the Management Point Server and let it discover all the servers that are connected to it through the ICMB cabling.

Follow these steps to configure the Management Point Server:

1. Using PIC, view the Management Point Server. There will be a folder named "ICMB" in the navigation pane.
2. Open the ICMB folder to display ICMB Configuration dialog to the right of the navigation pane.
3. Check the box labeled "Enable as Management Point" in the "Local ICMB Server Configuration" area of the dialog box.
4. Check the box labeled "Enable Full Sensor View" in the same area of the dialog box.
5. Wait for the Management Point Server to discover all ICMB devices. As servers are discovered through the polling process, they appear in the "Remote ICMB Chassis Configuration" area of the dialog box.
6. Configure each remote ICMB server in the "Remote ICMB Chassis Configuration" area as follows:
   - Select the server in the pull-down field.
   - Choose whether to manage the chassis.
   - Choose whether to enable full-sensor view.
   - Define an event-polling period for that device.

ICMB Devices

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

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

---

[35] 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 in an Itanium-based server.

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

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

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

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

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

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

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

Configuring ICMB on the Primary (Managing) Server

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

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

Configuring the Watchdog Timer Value

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

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

To configure the watchdog timer value, do the following:

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

Paging

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

NOTE

The SE7210T1-E server system does not support the paging feature.

Initiating a Page

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

NOTE

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

Paging Configuration

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

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

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

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

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

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

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

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

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

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

Customizing PIC Administrator Options

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

To configure the refresh interval or temperature display format:

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

⟹ NOTE

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

Default Values and Restoring Default Values

PIC installs with the following default values:

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

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

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

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

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

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

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

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

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

PIC Event Messages

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

Messages Displayed at the Server

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

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

For example, the message:

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

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

Broadcast Messages

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

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

Broadcast Messages

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

Email Messages

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

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

Configuring Email Alerts

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

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

NOTE

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

Email Settings

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

Specify these settings on the Email Alert Configuration screen:

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

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

SMTP Server: Specify the name of the mail server.

Test Email

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

NOTE

The subject and message that you enter in a test email are not the same subject and message that will be sent in an actual email alert. The PI software automatically determines the content of the alert message (see page 65).

Discovering Email Errors

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

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

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

You can view the Operating System Event Log errors as follows:

- On a Windows system use the Event Viewer or Event Properties from the Control Panel > Administrative Tools.
- On Novell NetWare see error messages in the file named SYS$LOG.ERR which is typically in the SYS:SYSTEM folder.
- On Linux the errors are written to the /var/log/messages file.
- On OpenUnix the errors are written to one or both of the /var/adm/syslog file or the /var/adm/log/osmlog file.

Configuring System ID LED Alerts

Use the Alert Actions tab for the individual sensors to set an ID LED Alert notification for that sensor. Setting an ID LED Alert causes the system's ID LED to be turned on or off when an event occurs, depending on which check box (LED On or LED Off, respectively) you select in the Alert Actions tab.

Intel® Server Maintenance and Reference Training (SMaRT) Tool Interface

The Intel® SMaRT Tool is a separate software product that provides support information specific to your server. It will assist you with the maintenance and repair of your hardware. Intel SMaRT Tool includes:

- Visual, step-by-step instructions on how to replace Field Replaceable Units (FRUs)
- A complete FRU database containing part numbers and images
- Product spares lists
- Worldwide Intel support information

The PIC has an interface to launch the Intel SMaRT Tool, consisting of a toolbar button and a "Launch SMaRT Tool" menu item. The Intel SMaRT Tool parts information and repair procedures correspond to the specific server hardware that you reference from PIC. When Intel SMaRT Tool launches, it opens on the level of the server hardware you are viewing from the PIC interface:

- If you have highlighted a server name or a Health branch of a server in the PIC, Intel SMaRT Tool opens on a home page for the related server type.
- If you have highlighted a particular sensor or Field Replaceable Unit (FRU) in the PIC, Intel SMaRT Tool opens to either the specific parts information for the highlighted FRU, or to step-by-step procedures necessary for replacing the particular FRU. (In the Intel SMaRT Tool interface labeled "About SMaRT Tool, you can specify which section will open from PIC.)

If possible, PIC attempts to launch the Intel SMaRT Tool in the same language you are using to view ISM on the console system. If that language is not available, Intel SMaRT Tool launches in English.

The Intel SMaRT Tool must be available (previously installed) on the hard disk or over the network when invoked. Otherwise you will receive an error message asking you to provide the location of the Intel SMaRT Tool executable (smart.exe). To locate the Intel SMaRT Tool, use the PIC menu item SMaRT Tool > Locate SMaRT Tool.

To obtain the Intel SMaRT Tool software and installation instructions, please refer to the Resource CD shipped with the Intel Server Board you purchased or order it online at:

http://www.intel.com/go/smartgo/smart

NOTE

PIC will only launch Intel SMaRT Tool version 4.0 or higher.

5. Direct Platform Control (DPC) Details

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

DPC uses a redirected text-based console that runs over a serial connection[36] or the LAN. Since DPC does not communicate with the server OS, it can manage the server even if the OS and primary processors are not working. Because the server's emergency management hardware works on 5 V standby power, DPC can communicate with and control a powered-down server, assuming the AC power is connected.

You can use DPC to:

- Restart a server that is powered on
- Power on a server that is powered off
- Power off a server that is powered on
- View the System Event Log (SEL) for information about recent server activity
- View Sensor Data Records (SDRs) for information about sensor characteristics
- Review Field Replaceable Unit (FRU) inventories
- View current Remote Sensor Access (RSA) information[37]
- Reset a remote server to either EMP mode[38] or Re-direct Mode
- Maintain a Phonebook for remote server connection management
- Reboot to the service partition[39] to run service partition-based utilities on the server such as running a command shell. You can also upload or download files to the service partition, run a remote program, or remote diagnostics if available

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

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

[36] Serial connections between a managing console and the SE7210TP1-E server platform are not supported.

[37] Remote Sensor Access (RSA) is not supported on the SE7210TP1-E server platform.

[38] EMP mode is not supported on the SE7210TP1-E server platform.

[39] The Service Partition is not supported on the SE7210TP1-E server platform.

Server Connections

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

Use the Server Configuration Wizard (page 13) to configure the server's serial and LAN connections. For ISM-supported servers, BIOS Setup is not required for console redirection to allow DPC communications over the COM2 serial port (EMP).

NOTE

Serial (modem or direct connect) connections are not supported when managing SE7210TP1-E servers.

Starting the DPC Console

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

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

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

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

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

NOTE

Command-line options `/modem` and `/direct` are not supported when connecting to SE7210TP1-E servers.

DPC Features

Use the DPC menus or click a toolbar button to access DPC features. The menu items and toolbar change according to what features are available on the server. Features not available appear grayed out in the DPC console. When one of the DPC managers is active its menu is added to the DPC Console.

SEL Manager

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

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

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

SDR Manager

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

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

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

FRU Manager

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

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

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

RSA Manager

The Remote Sensor Access (RSA) Manager[40] lets you view server baseboard FRU and SDR information.

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

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

Console Redirection Window

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

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

NOTE

You cannot use the CSSU to connect to or configure SE7210TP1-E servers. Additionally, service partition operations are not supported on these servers.

Phonebook

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

Rebooting to the Service Partition

You can use DPC to reboot the server to its service partition[41].

The service partition is a special partition on the hard disk that you establish when initially setting up the server (see page 131). The service partition contains utilities, diagnostics, and other software required for remote management. The service partition is not marked as an active partition and the server only boots from it by a special request. It is not normally visible to the server user.

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

[40] The RSA manager is not supported on the SE7210TP1-E server platform.

[41] The Service Partition is not supported on the SE7210TP1-E server platform.

To boot to the service partition:

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

NOTE

SE7210TP1-E servers do not support service partitions. Consequently, you cannot reboot to a service partition on these platforms.

Displaying Configuration Status

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

Supported Viewers: Status on the FRU, SEL, SDR, and RSA[42] viewers.

Security: Displays the following settings:

- Authentication level: Indicates User or Administrator level. Administrator level exists if you are logged in with administrative rights. User level applies to these situations:
  - EMP (serial) connection[43] when EMP mode is set to "restricted"
  - LAN connection over the onboard NIC where a secure session is not available (*e.g.*, someone else is already connected)
  - Restricted LAN access mode
- Activation Mode: Indicates whether the server is always active or just during pre-boot.
- Chassis Intrusion: Indicates whether intrusion protection is set or not set.

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

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

NOTE

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

[42] The RSA Viewer is not supported on the SE7210TP1-E server platform.

[43] EMP serial connections are not supported on the SE7210TP1-E server platform.

6. Client SSU (CSSU) Details

The Client SSU (CSSU) allows you to remotely run the System Setup Utility (SSU) software or other utilities on the server.

NOTE

The CSSU is not available for use when managing SE7210TP1-E servers. To configure the SE7210TP1-E server you must use SSU locally from the server. To execute any server-resident utilities you must execute them locally from the server.

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

Use CSSU to:

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

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

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

CSSU Operation

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

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

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

Console Redirection Window

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

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

Phonebook

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

CSSU Managers

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

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

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

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

Multiboot Manager

The Multiboot Manager lets you:

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

Password Manager

The Password Manager lets you:

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

System Event Log Manager

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

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

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

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

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

Sensor Data Records Manager

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

Using the SDR Manager, you can:

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

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

Field Replaceable Unit Manager

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

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

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

System Update Manager

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

- Determines the current revision of system BIOS and firmware on server controllers.
- Updates BIOS and/or firmware.
  - — Updates the system BIOS and BIOS boot block with a .CIT file, if the .CIT file is shown as available. The .CIT file is included on the BIOS update disk for platforms that require the BIOS boot block to be updated when the BIOS is updated. See your platform documentation for further information on your platform's BIOS update requirements.
  - — Updates the system BIOS with a BIOS file (.BIO file). For use on platforms that do not require the BIOS boot block to be updated when the BIOS is updated. See your platform documentation for further information on your platform's BIOS update requirements.
  - — Updates operational code for controllers using files composed of Hex Format code (.HEX file).
  - — Updates the BIOS and/or firmware using a user-specified Update Information File (.UIF file). The .UIF file lists all the controllers to be updated, the type of update to be done, and the .CIT, .BIO and .HEX files to be used for the update.
- For controller firmware, verifies the code currently loaded against an external hex file, of either .HEX or .UIF format.

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

Platform Event Manager

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

Configuration Save/Restore Manager

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

7. Command Line Interface

When managing server systems other than the Intel® Server Compute Blade SBX44, ISM gives you the alternative of managing servers using a command line interface from a Windows or Linux console. You can enter commands directly from the command line or you can set up a script file of commands to be run. This feature is called Command Line Interface, or CLI.

NOTE

The Command Line Interface (CLI) cannot be used to connect to or manage Intel® Server Compute Blade SBX44 servers. Information in this section is provided for those who will be using ISM 5.8 Console to manage other Intel® server platforms in addition to Intel® Server Compute Blade SBX44 servers.

CLI Overview

The CLI has two modes: Platform Control mode and Serial over LAN[44] (SOL) Console Redirection mode. When CLI is in Platform Control mode, you can issue CLI commands to the remote system. When CLI is in SOL Console Redirection mode, you can perform, over a LAN connection, any activity you could at the remote system's console, including viewing the remote system's console output (SOL allows data from the server serial port to be redirected over the LAN). When in Platform Control mode, the CLI displays a unique prompt (dpccli>). When in SOL mode, the CLI does not display a prompt and all information displayed comes directly from the SOL character stream. See page 86 for information about switching between these two modes.

NOTE

The SE7210TP1-E server platform does not support the Serial over LAN (SOL) Console Redirection mode.

The CLI uses a network proxy (dpcproxy) that runs on the managing client system or on a central network proxy. The network proxy is automatically installed as part of the Intel Server Management installation process. Rebooting the server on which the proxy runs automatically starts the network proxy. (See page 104 for details on the network proxy.)

[44] The Serial Over LAN feature is not supported on the SE7210TP1-E server platform.

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. Both methods are described in detail later in this section.

NOTES

In order to switch CLI to SOL mode, you must be using a telnet connection to the remote server. You cannot switch to SOL mode (or use CLI commands or options that start the remote server in SOL mode) if you are simply running dpccli to issue CLI commands to the remote server.

Note that Windows Hyperterminal is no longer supported for CLI or SOL.

CLI's console interface, called *dpccli*, runs on the management console and enables communication between the management console and the network proxy, which in turn communicates to the managed server. Like the network proxy, the dpccli interface is automatically installed as part of the ISM installation process. (See page 87 for details on dpccli.).

When using telnet to connect to the remote server (to issue CLI commands and to operate in SOL mode), you must connect the telnet session to the dpcproxy by specifying (in the telnet command line) the port on which dpcproxy is listening (see page 86 for required telnet syntax).

A CLI session over dpccli requires a server name (or address) and login (user and password), which can be supplied as arguments to the dpccli command.

Once the CLI session over dpccli is running and the connection to the intended server is established, you can begin issuing CLI commands to that server at the dpccli prompt. If connecting via telnet, the same dpccli prompt is displayed when in Platform Control mode (default), and you can issue CLI commands at the dpccli prompt over telnet.

CLI Features and Benefits

The ISM Command Line Interface (CLI) lets you control a server from the command line rather than from a graphical user interface. You can enter CLI commands at a command prompt or from a script file to do the following (note that this is not an exhaustive list; see page 91 for a complete list of CLI commands):

- Remotely power on or off a server
- Remotely reset the server
- Request machine identifiers
- Read sensor values
- Display the network configuration of the BMC

You can also execute Perl scripts to issue commands to multiple remote servers. You can use any of the following consoles to launch dpccli or telnet and issue CLI commands:

- The Window's command-line environment: Command Prompt
- A Linux command shell

CLI's Serial over LAN (SOL) Mode

The Serial over LAN Console Redirection mode[45] of CLI lets servers transparently redirect the serial character stream from the baseboard UART to and from the managing client system over the LAN. Serial over LAN has the following benefits compared to a serial interface:

- Eliminates the need for a serial concentrator
- Reduces the amount of cabling
- Allows remote management of servers without video, mouse, or keyboard (headless servers)

NOTE

The dpccli interface does not support formatted output. When using CLI in SOL Console Redirection mode, special characters may not appear properly formatted as they would at the server console. In order to view SOL data, a connection via telnet must be established.

Enabling Serial over LAN on the Server

You can enable the feature locally (on the managed server) through the System Setup Utility (SSU) or enable it remotely (from the managing client) through the Client System Setup Utility (CSSU). Both methods involve the same steps once you have started the utility.

Follow these steps to enable Serial over LAN[44] (see the CSSU online help for detailed information about completing these steps):

1. Either start the SSU locally on the server, or start CSSU from the managing client.
2. From the first screen, select the Platform Event Manager Task to reveal the BMC LAN Configuration Screen.
3. Make sure the LAN Channel is configured for use. For example, make sure that you don't have LAN Access Mode set to "disabled." Also, set the IP Addresses properly.
4. In the Options menu select Configure Serial Over LAN.
5. Specify the SOL Access Mode as either Always Available or Restricted.
6. Set the baud rate parameter.
7. Save your changes.
8. Press the <ESC> key repeatedly until you are back to the command prompt.
9. Reboot the system.

[45] The Serial Over LAN Console Redirection feature is not supported on the SE7210TP1-E server platform.

Using the Command Line Interface (CLI)

As stated previously, there are two basic methods for issuing CLI commands to a remote server: through dpccli, or through telnet. Both methods are described below.

If you want to use CLI in SOL mode[46], you must connect to the remote server through telnet (SOL mode is not supported through dpccli). However, the dpccli command line options, which affect the behavior of the connection, cannot be used when connecting through telnet (because you are not using the dpccli command if you use telnet). So, you will need to decide which method to use, depending on what you want to do on the server. See page 87 for details on the dpccli command and its options.

NOTE

When using the Command Line Interface (CLI) with Serial over LAN Console Redirection from a management console running a supported version of Linux, the backspace key [Backspace] does not work. You must use [Control]-[Backspace] instead when using Command Line Interface (CLI) with Serial over LAN Console Redirection from a management console running a supported version of Linux. Other utilities (SPU and PCU) do not experience this issue.

NOTE

Both Platform Control mode and SOL mode use the network proxy to communicate to the remote managed server. This is because the telnet command described in this manual (see page 86) specifies using port 623 for telnet, which is the port on which the network proxy, dpcproxy, listens.

NOTE

Using dpccli or telnet on a server platform that uses a full BMC, ***only four concurrent connections can be made to one server****. This is because the dpcproxy connects directly to the BMC of the remote server, and the BMC only supports four concurrent connections. For systems that use the mini BMC, such as the SE7210TP1-E server platform, only one connection can be made to the server.*

Upon attempting the fifth connection, the following is displayed approximately 15-20 seconds after entering the password:

Invalid Password
Connection Failed

followed by the operating system prompt. Note that any Out-of-Band connections to that server from other ISM applications count toward the total of four connections to that server's BMC.

[46] Serial Over LAN mode is not available on the SE7210TP1-E server.

Using CLI Commands with dpccli (Platform Control Mode Only)

NOTE

To start a CLI session with dpccli, the network proxy dpcproxy must be running, either on the managing console or a central network proxy system. However, by default you should not have to do anything for the network proxy to be running, because the ISM installation installs the network proxy and sets it up for automatic start upon reboot. See page 104 for details on the network proxy.

Using Windows Command Prompt

To connect to the server in Platform Control Mode and use CLI commands:

1. Enter the dpccli command and provide any command-line options (see page 89).
2. At the "Server:" prompt provide the IP Address or DNS Name of the server to which you want to connect.
3. At the username prompt, press Return to specify a null IPMI user (default).
4. At the password prompt, press Return to specify a null IPMI user password (default; if you have configured a password for the default IPMI user, enter that password).
5. After authentication is performed, you will see a login successful message and the `dpccli>` prompt. You can now enter CLI commands.

Using Linux Shells

To connect to the server in Platform Control Mode and use CLI commands from your Linux command line shell:

1. Enter the following command and provide any command-line options (see page 89).
   `/usr/local/cli/dpccli`
2. At the "Server:" prompt provide the IP Address or DNS Name of the server to which you want to connect.
3. At the username prompt, press Return to specify a null IPMI user (default).
4. At the password prompt, press Return to specify a null IPMI user password (default; if you have configured a password for the default IPMI user, enter that password).
5. After authentication is performed, you will see a login successful message and the `dpccli>` prompt. You can now enter CLI commands.

Using telnet for both Platform Control and SOL Modes

NOTE

When using the Serial over LAN Console Redirection mode of Command Line Interface (CLI) from a management console running a supported version of Linux, the backspace key [Backspace] does not work. You must use [Control]-[Backspace] instead when using Command Line Interface (CLI) with Serial over LAN Console Redirection from a management console running a supported version of Linux. Other utilities (SPU and PCU) do not experience this issue.

Serial over LAN mode[47] requires a telnet session from the managing console to the managed server, regardless of which operating system (Windows or Linux) you are running on either system. Start the telnet session to the remote server as described below.

1. At the operating system command prompt, type "telnet xxx.xxx.xxx.xxx 623 <Enter>". The xxx represent the IP address of the system running the Network Proxy. This may be a central network server with the Proxy installed. If you are connecting to the local system, use "localhost" instead of the system's IP Address. The 623 represents the default Port address required for CLI connections. If this port address has been changed while executing the dpcproxy command use that port address. Eg: telnet 10.7.162.58 623 or telnet localhost 623
2. At the "Server:" prompt provide the IP Address or DNS Name of the server to which you want to connect.
3. At the username prompt, press Return to specify a null IPMI user (default).
4. At the password prompt, press Return to specify a null IPMI user password (default; if you have configured a password for the default IPMI user, enter that password).

After authentication is performed, you will see a login successful message and the `dpccli>` prompt (even over telnet, CLI starts in Platform Control mode by default). You can now enter CLI commands (see page 91 for list of commands) or switch to SOL Console Redirection mode, as described below.

NOTE

When using the BIOS setup utility on a remote server through an SOL connection, be aware that upon exiting the BIOS setup utility (by pressing F10), the SOL connection to the remote server will be lost and you will need to re-establish the SOL connection to the server.

Switching Between Platform Control Mode and SOL Console Redirection Mode

When you use telnet as described above to connect to the remote server through the network proxy (due to the use of the port on which dpcproxy is listening), the CLI session starts in Platform Control Mode, in which CLI commands can be executed on the remote system. To switch to SOL Console Redirection mode, issue the CLI command "console" (see page 96). To exit SOL Console Redirection mode and return to Platform Control Mode, enter the tilde-period key sequence (~.). This switches the console back to Platform Control Mode.

[47] Serial Over LAN mode is not available on the SE7210TP1-E server platform.

The Console Interface (dpccli)

As stated above, for a command prompt console such as a Linux shell, you must start dpccli before you can access the CLI commands. The dpccli executable file acts as an interface between the console and the network proxy. Once the interface is started, you can then connect to a server and enter commands.

The console interface is particularly useful in scripting environments that use standard console input and output. It is also useful as a simple interactive interface when formatted output is not required.

dpccli Return Codes

When it exits, dpccli will return a status code to the environment. Normal exits are performed by using the CLI commands exit or quit (see page 97) during a dpccli session. However, if the -e option is used when invoking the network proxy (dpcproxy), dpccli will exit abnormally whenever an error condition is encountered. If the -e option is not used, only the very last return code can be viewed (that is, if multiple errors occurred during the session, and you exit normally, you will only see the return code of the last error).

If you would like to set the -e option for the network proxy, see page 104 for information on setting persistent arguments (arguments that will be read whenever the network proxy is restarted upon reboot).

To view the return code upon exiting dpccli (either by using the exit or quit command, or because of an error), type one of the following commands at the command prompt, depending on your operating system:

- Linux: `echo $?`
- Windows: `echo %errorlevel%`

The following are the status codes dpccli will return (non-zero values for the return code indicate an error condition was encountered):

Code	Meaning	Suggested Action
0	Success	No action necessary.
1	Connection lost to proxy	Restart dpccli session or telnet session, depending on which you were using.
2	Login failed	Retry login.
3	Unrecognized command	Retype command (this error will be displayed if command is mistyped).
4	Command failed	Retype command. May need to restart the network proxy and try the command again.
5	Invalid Arguments	Retype command and arguments (this error will be displayed if argument is mistyped).
6	Unknown error	Contact system administrator.

The .dpcclirc Configuration File

In situations where you regularly start the dpccli console interface, you can set up a configuration file of common command-line options. Thus you avoid having to enter the options each time at the command line. For example, you could put in this file the network address of a centralized network proxy using the `-P` option. Each time you start dpccli it reads the configuration file, and it would get the network proxy from the file.

NOTE

The .dpcclirc file is only referenced when the dpccli command is launched from an operating system command prompt. If you use telnet to connect to the managed server, as described on page 86, the .dpcclirc file will not be referenced.

By default dpccli looks for a file named *.dpcclirc*, first in the directory specified in the **HOME** environment variable (see below) and then in the current working directory. You can explicitly specify the file name and its path on the command line with the `-r` option.

NOTE

Options specified on the dpccli command line (see page 89) always take precedence over options specified in the configuration file. ***Not all dpccli options are supported from*** **.dpcclirc**. *The supported options are:*

`a, c`[48]`, I, v, i, o, p, P, s,` *and* `u`.

Command text is not processed through the configuration file. Any option not understood or supported is silently ignored. Thus, you can insert blank lines or comments that start with a non-option letter, for example, # in the file.

When creating the configuration file, enter each option on a separate line. Each line must begin with an option letter optionally preceded by the hyphen character. Follow the option with any argument that applies (note that there must be a space between the option and its argument; for example, `-s server_name`). See the options listed on page 89.

Setting the HOME environment variable

NOTE

The HOME environment variable may already be in use by other applications. Verify that HOME is not being used before changing this setting.

In Linux

As stated above, by default dpccli looks for a file named *.dpcclirc*, first in the directory specified in the **HOME** environment variable and then in the current working directory.

[48] This option is not supported on the SE7210TP1-E server platform.

To set the HOME environment variable, do one of the following:

- To temporarily set the HOME variable (until next reboot), type the following command: `export HOME=<path>`
- To permanently set the HOME variable, edit the `/etc/profile` script and add the line `export HOME=<path>`.

In Windows

Access the System Properties dialog by right-clicking the My Computer icon on the desktop and selecting Properties. Click the Advanced tab, then select Environment Variables. From there add the variable HOME, and define the path as desired.

The dpccli Command Syntax

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]...}
```

NOTE

The -c option is not supported when managing SE7210TP1-E server platforms.

NOTE

The first text encountered on the command line that is not associated with a command-line option (i.e., the [text] option referenced above) is interpreted as the start of text to be sent to the network proxy. Therefore you must place this text last on the command line.

NOTE

It is recommended that the [-o outputFile] option be used with the [-i inputFile] option. If you do not use[-i] when using [-o], CLI may appear to hang (even though it is working properly) because all output is being directed to the file specified in the -o option instead of to the console.

The dpccli Command-line Options

Option	Description
`-?` or `-h`	Displays command usage. Any other options specified with this option are ignored.
`-s server`	Specifies the IP Address or DNS hostname associated with the Network Interface Card (NIC) used by the Baseboard Management Controller (BMC). For *server*, specify either an IP Address or DNS hostname. If you do not specify this option, you will be prompted for the information.
`-u user`	Specifies the Intelligent Platform Management Interface (IPMI) username associated with this session. For *user*, specify a valid username associated with the managed server. If you do not specify this option, you will be prompted for the information. Note that if you are using a null user and password, supply "" for the user name (e.g., dpccli -s server_name -u "" -p "").

continued

Option	Description
`-p` *`password`*	Specifies the IPMI password associated with this session and user. For *password*, specify the password associated with the username. If you do not use this option, you will be prompted for the information. Note that if you are using a null user and password, supply "" for the password (e.g., dpccli -s server_name -u "" -p "").
`-i` *`inputFile`*	Specifies an input file to be read as standard input. For *inputFile*, specify any text file. When the end of file is reached, the dpccli session ends unless you have also used the `-I` command-line option. If you do not use the -i option, you must interactively supply input from the command line. Note that you may not supply dpccli command line options specified in this table (-u, -s, -p, etc.) in the contents of the input file. However, those options may be specified in the same command string in which the [-i inputFile] option is used. For example, dpccli -u user_name -p password -s server_name -i input_file_name
`-o` *`outputFile`*	Specifies an output file in which to capture standard output. For *outputFile*, specify any text file. If you do not use this option, all standard output arrives at the console. It is recommended that the [-o outputFile] option be used with the [-i inputFile] option. If you do not use[-i] when using [-o], CLI may appear to hang (even though it is working properly) because all output is being directed to the file specified in the -o option instead of to the console.
`-c`	Forces the BMC session into Serial over LAN mode. In Serial over LAN mode, data is passed unaltered from the managed server to the console. If you do not use this command-line option, Platform Control Mode is the default mode. **NOTE:** This option is not supported when managing SE7210TP1-E server platforms.
`-I`	Causes the dpccli session to continue as an interactive session after all characters in the input file (specified with the `-i` command-line option) have been processed. The interactive mode continues after processing all characters read from an input file and/or any text specified at the command line. This is the default mode if an input file and/or text is not specified on the command line.
`-v`	Causes session progress messages to be sent to standard error (i.e. verbose output). Additionally, any non-zero exit condition prints an associated error message. This behavior is also the default behavior during any interactive session.
`-P` *`networkProxy`*	Specifies the IP Address or DNS hostname of the system running the network proxy (dpcproxy). The system whose IP Address or hostname you supply for *networkProxy* is the system that the client (your console system) will contact to look for the network proxy service. By default, the IP Address is the local host (127.0.0.1). Note that unless the -a flag is also used (to specify a particular port to use), the console system will attempt to communicate to the remote proxy through the default dpcproxy port of 623.
`-a` *`alternatePort`*	Specifies an alternate network proxy port number. By default, the port number is 623. If you have changed the port on which dpcproxy is listening (by using the dpcproxy command with the -p option; see page 107), you must supply the -a option with the new port number in your dpccli command.
`-r` *`rcFile`*	Specifies an alternate dpccli configuration file. By default, dpccli first looks for a file named *.dpcclirc* in the directory specified by the environment variable **HOME** (see page 88) and then in the current working directory. This option specifies the path including filename, which can be different than *.dpcclirc*. For information on dpccli configuration files, see page 88.

Running dpccli Commands from a Script

In order to scan multiple servers for information or to monitor their health, dpccli can be executed as part of a user created script. The following is an example of how input and output files could be used to query a server and save the information to a file which could then be parsed for data.

Sample input file:

```
111.112.113.20
     (null user name. carriage return only, no spaces or tabs)
     (null password. carriage return only, no spaces or tabs)
sensors –v
network
```

Script command to execute.

```
./dpccli –i inputfilename –o outputfilename
```

Output file created based on the sample input file above.

```
Server: 111.112.113.20
user name:
Password:
Login successful
dpccli> sensors -v
04/08/02 | 06:56:18 | Baseboard 1.25V   | ok  |    1.24 | Volts
04/08/02 | 06:56:18 | Baseboard 2.5V    | ok  |    2.47 | Volts
04/08/02 | 06:56:18 | Baseboard 3.3V    | ok  |    3.29 | Volts
04/08/02 | 06:56:18 | Baseboard 3.3VSB  | ok  |    3.28 | Volts
04/08/02 | 06:56:18 | Baseboard 5.0V    | ok  |    4.97 | Volts
04/08/02 | 06:56:18 | Baseboard 12V     | ok  |   11.97 | Volts
04/08/02 | 06:56:18 | Baseboard -12V    | ok  |  -11.97 | Volts
04/08/02 | 06:56:19 | Baseboard VBAT    | ok  |    3.07 | Volts
04/08/02 | 06:56:19 | Processor VRM     | ok  |    1.45 | Volts
04/08/02 | 06:56:19 | Baseboard Temp    | ok  |   30.00 | Celsius
04/08/02 | 06:56:19 | FntPnl Amb Temp   | ok  |   28.00 | Celsius
04/08/02 | 06:56:19 | Processor1 Temp   | ok  |   37.00 | Celsius
04/08/02 | 06:56:19 | Processor2 Temp   | ok  |   36.00 | Celsius
04/08/02 | 06:56:19 | PwrDstBd Temp     | ok  |   27.00 | Celsius
04/08/02 | 06:56:19 | PwrDstBrd Fan     | ok  | 7320.00 | RPM
04/08/02 | 06:56:19 | System Fan 3      | ok  | 3872.00 | RPM
04/08/02 | 06:56:19 | System Fan 1      | ok  | 5852.00 | RPM
dpccli> network
```

```
IP Address:         111.112.113.20
IP Address Source: static
MAC Address:        00:03:47:A4:FC:7D
Subnet Mask:        255.255.255.0
Gateway:            111.112.113.20
dpccli> exit
```

CLI Commands

The table below lists the CLI commands. Each command is described in the following sections.

CLI Commands

Command	Description
alarm[49]	Queries, sets, or clears alarms established at a system. This command is valid only when used against a system configured specifically with hardware for telephone company (telco) alarm capabilities.
boot	Sets the IPMI boot options
console[49]	Starts Serial over LAN mode
diagint	Causes the BMC to generate an IPMI diagnostic interrupt
exit	Ends the CLI session
quit	Ends the CLI session
help	Displays command usage
id	Displays the Globally Unique ID (GUID) of the managed server
identify[49]	Causes the server to signal its location
network	Displays the network configuration of the BMC
power on	Initiates a power up sequence on the managed server.
power off	Initiates a power down sequence on the managed server
power	Displays the current power state of the managed server
reset	Performs a reset operation on the managed server
sel	Displays the System Event Log (SEL) records
sensors	Displays the current status of the server's sensors
service[49]	Lets you interact with the Remote Service Agent (RSA)
set	Defines the CLI command mode prompt and response prefix
shutdown	Shuts down or resets the managed system
version	Displays the version of the active dpcproxy

[49] This command is not supported on the SE7210TP1-E server platform.

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 SE7210TP1-E server platforms. Issuing this command causes an "error COMMAND IS INVALID" message to be returned.

Syntax:

`alarm -s -a id -l severity`

Description:

The –s option designates this command as the "set alarm" command. This command adds a single Telco alarm record to the Telco alarm database. The generator ID for CLI will always be 41h. The following is an example of an alarm command to add a new alarm:

```
alarm –s –a 25 –l MJR
```

Options (all required):

-s Specifies "set alarm" command.

-a Sets alarm ID.

-l Sets alarm severity. Possible severities are MJR (major), MNR (minor), and CRT (critical).

After every set alarm command, you should see one of the following five messages.

```
New alarm added to BMC TAM alarm database.
Request alarm matches existing BMC TAM alarm database record.
Request alarm updated an existing BMC TAM alarm database record.
BMC TAM alarm database is full.  Request alarm record bumped
because of lower priority.
BMC TAM alarm database is full.  Request alarm record bumped
existing record.
```

alarm -q

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 SE7210TP1-E server platforms. Issuing this command causes the error message "There are no records in the BMC TAM alarm database to be displayed" to appear.

Syntax:

`alarm -q [-g id [ -o id ] [-a id ]] | [-p] | [ -l severity]`

Description:

The –q option designates this command as the "query alarm" command. This command queries Telco alarm records in the alarm database based on the options entered by the user. Other than –q, no options are required and all of the other options can be specified.

Options:

[-q]	Specifies "query alarm" command.
[-g]	Query against the generator ID specified.
[-o]	Query against the software originator ID specified.
[-a]	Query against the alarm ID specified.
[-p]	Query only alarms that are related to power.
[-l]	Query against the severity specified. Severities are MJR (major), MNR (minor), and CRT (critical).

This command will display all records that match the query criteria. The following is an example of an input and output sequence.

```
alarm –q –l MJR

AlarmGenID=4  AlarmSW=Y  AlarmSWID=5  AlarmID=1  AlarmSev=MJR  AlarmPWR=N
AlarmGenID=3  AlarmSW=N AlarmSWID=NA  AlarmID=2  AlarmSev=MJR  AlarmPWR=N
AlarmGenID=2  AlarmSW=N  AlarmSWID=NA  AlarmID=3  AlarmSev=MJR AlarmPWR=Y
```

alarm -c

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 SE7210TP1-E server platforms. Issuing this command causes the error message "There are no records in the BMC TAM alarm database to be displayed" to appear.

Syntax:

`alarm -c [-g id [-o id] [-a id ]] | [-l severity] | all`

Description:

The –c option designates this command as the "clear alarm" command. This command clears all Telco records in the Telco alarm database based on the options entered by the user. Other than –c, no options are required. If the –a option is specified, then the –g and –o options must also be specified.

Options:

[-c] Specifies "clear alarm" command.

[-g] Clears alarm for the generator ID specified.

[-o] Clears alarm for the software originator ID specified.

[-a] Clears alarm for the alarm ID specified. If the –a option is specified, then the –g and –o options must also be specified.

[-l] Clears alarm for the severity specified. Severities are MJR (major), MNR (minor), and CRT (critical).

This command will display the alarm id of every record it removes. The following is an example input and output sequence.

```
alarm –c –g 4 –o 5 –a 1
Alarm ID 1 cleared (Generator ID 4)
```

boot

Syntax:

```
boot  {normal | service} [-f] [-c]
```

Description:

Sets the IPMI boot options and then resets the system. By default, the boot command attempts a graceful shutdown[50] of the operating system before executing the IPMI reset command. If the specified boot option is unavailable, the server will boot using the boot order set in its BIOS.

Options:

[-f] Forces a boot without a graceful shutdown.

[-c] **This command-option combination can only be used over a telnet session to the remote server** (see page 86). Switches the session to Serial over LAN mode after successfully executing the IPMI reset command. You will see the BIOS output and other boot messages as if sitting at the managed server. If you specify a `service` option along with the -c option, the CLI opens a connection with the Remote Service Agent (RSA) running on the service partition instead of establishing a Serial over LAN session. Then you can interact with RSA using the `service` command (see page 102).

NOTE

This option is not supported when managing SE7210TP1-E server platforms.

`normal` Boots the server from the hard drive.

`service` Boots the server from the Service Partition.

console

Syntax:

```
console
```

Description:

This command-option combination can only be used over a telnet session to the remote server (see page 86). Switches the CLI from Platform Control mode to Serial over LAN Console Redirection mode.

NOTE

This command is not supported when managing SE7210TP1-E server platforms.

In Serial over LAN Console Redirection mode, the character stream is passed unaltered allowing you to view directly the output of the console serial port of the server. Switching into this mode causes any output data that was received and buffered while CLI was in command mode to be displayed.

[50] The SE7210TP1-E server platform does not support a graceful shutdown of the operating system.

You can switch from Serial over LAN Console Redirection mode back to CLI command mode by typing a tilde followed by a period (~.) To escape the tilde and send it to the console, type a second tilde.

diagint

Syntax:
`diagint [-c]`

Description:
Forces the Baseboard Management Controller (BMC) to generate an IPMI diagnostic interrupt.

Options:
`[-c]` **This command-option combination can only be used over a telnet session to the remote server** (see page 86). Switches the session to Serial over LAN mode after successfully executing the IPMI diagnostic interrupt command.

> **NOTE**
>
> *This option is not supported when managing SE7210TP1-E server platforms.*

exit or quit

Syntax:
`exit`
`quit`

Description:
Terminates the CLI session. Either command closes all IPMI sessions associated with the user of the network proxy as well as closing the network proxy socket.

help

Syntax:
`help [CLIcommand]`

Description:
Displays how to use the specified CLI command. If you do not specify a CLI command, abbreviated usage information is displayed for all CLI commands.

Options:
`[CLIcommand]` Any valid CLI command.

id

Syntax:
`id`

Description:
Displays the 16-byte system Globally Unique Identifier (GUID) of the managed server in the conventional GUID format; for example, `422e7704-23f5-4706-a943-a7859c073aed`.

identify

Syntax:
`identify [-on [seconds]] [-off] [-s]`

Description:
Causes the server to signal its physical location with a blinking LED or beep. Use this command to locate a server in a rack of servers.

NOTE

This command is not supported when managing SE7210TP1-E server platforms.

Options:

`[-on [seconds]]`	Specifies the number of seconds to blink the LED or sound the beep. If you do not provide a value for *seconds*, the default is 15 seconds. If you provide the value 0 for *seconds*, the server will identify itself indefinitely. The maximum value for seconds is 255. Not all servers support specifying the number of seconds.
`[-off]`	Turns off the blinking LED or beep. This option has no effect if the specified server is not currently identifying itself.

identify -s

Syntax:
`identify -s`

Description:
Displays the current LED state as ON (Application), ON (Button), or OFF.

NOTE

This command is not supported when managing SE7210TP1-E server platforms.

Options:

[-s] Displays the current LED state as ON (Application), ON (Button), or OFF.

network

Syntax:
`network [mac] [ip] [subnet] [gateway]`

Description:
Displays the network configuration of the Baseboard Management Controller (BMC). The display includes the MAC address, IP address and source (static, DHCP, BIOS), subnet mask, and gateway IP address. If you do not supply an option, all information is displayed.

Options:

`[mac]`	Displays only the MAC address.
`[ip]`	Displays only the IP Address.
`[subnet]`	Displays only the subnet mask.
`[gateway]`	Displays only the gateway IP Address.

power

Syntax:
`power {on [-c]} | {off [-f]}`

Description:

Initiates a power up or power down sequence on the managed server. By default, this command attempts a graceful shutdown[51] of the operating system before executing the IPMI power-off command. To perform a graceful shutdown, the Platform Instrumentation (PI) software must be installed on the server.

Options:

`[-c]` **This command-option combination can only be used over a telnet session to the remote server** (see page 86). Switches the session to Serial over LAN mode after successfully executing the IPMI power-on command.

> **NOTE**
>
> *This option is not supported when managing SE7210TP1-E server platforms.*

`[-f]` Forces a power off without attempting a graceful shutdown.

power -s

Syntax:
`power -s`

Description:

Displays the current power state of the managed server.

[51] The SE7210TP1-E server platform does not support a graceful shutdown of the operating system.

reset

Syntax:
`reset [-f] [-c]`

Description:
Performs a platform reset. By default, this command attempts a graceful shutdown[52] of the operating system before executing the IPMI reset command. To perform a graceful shutdown, the Platform Instrumentation (PI) software must be installed on the server.

Options:

`[-c]` **This command-option combination can only be used over a telnet session to the remote server** (see page 86). Switches the session to Serial over LAN mode after successfully executing the IPMI reset command.

> **NOTE**
>
> *This option is not supported when managing SE7210TP1-E server platforms.*

`[-f]` Forces a reset without attempting a graceful shutdown.

sel

Syntax:
`sel [-c] [-num] [-f filename] [-h filename]`

Description:
Displays System Event Log (SEL) records. Each record displays on a single line and uses the following format:

```
Record # | Date Time | Sensor | Event description
```

Options:

`[-c]` Displays the record in a comma-separated value format using a single comma to separate each field, as in the following example:

```
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
```

`[-num]` Specifies the number of events displayed. If you do not use this option, all SEL records are displayed.

`[-f filename]` Writes decoded output of the System Event Log to the specified text file.

`[-h filename]` Writes the hexedecimal codes of the System Event Log to the specified file.

[52] The SE7210TP1-E server platform does not support a graceful shutdown of the operating system.

NOTE

When saving SEL files using the "sel -f" or "sel -h" commands, the file will be saved to the system where the dpcproxy is running. Example: If connected to a remote DPCProxy the saved SEL files will be placed on the remote system (where the dpcproxy is running) rather than the local system.

Any path specified must exist on the system on which the proxy is running.

sel -clear

Syntax:
`sel [-clear]`

Description:

Clears the System Event Log.

sensors

Syntax:
`sensors [-v] [-c] [-f threshold] [sensor]`

Description:
Displays the current status of platform sensors using this general format:

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

Options:

`[-v]` Displays all information fields (date, time, sensor type, etc.) if they are available, as in the following example:

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

`[-c]` Displays the record using a comma-separated format. In this format, fields are separated by a single comma, as in the following example:

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

`[-f threshold]` Filters the display based on *threshold*. All sensors that are at the threshold and above will be displayed. For example, setting the threshold to CR displays all sensors with critical, non-recoverable, and unspecified conditions. Specify one of the following for *threshold:*

- `ok` Operating in normal ranges.
- `nc` Non-critical condition caused by a sensor outside of its normal ranges.
- `cr` Critical condition that is potentially fatal to the system caused by a sensor exceeding its specified ratings.
- `nr` Non-recoverable condition that has potential to damage hardware.
- `us` Unspecified status indicating a fault whose severity is unknown.

`[sensor]` Specifies the sensor group to display. If you do not specify a sensor group, the command displays all groups for which there is information. Specify one of the following for *sensor:*

```
volt
temp
power
fan
```

service

Syntax:

```
service {console | exit | ftp {start | stop}}
```

Description:

This command-option combination can only be used over a telnet session to the remote server (see page 86). After booting from the Service Partition (see the `boot` command with the `service` option) , this command lets you interact with the Remote Service Agent (RSA) that is running from the managed server's Service Partition.

NOTE

This command is not supported when managing SE7210TP1-E server platforms.

Options:

`console` Switches the CLI session to RSA console mode. In this mode the RSA starts and redirects a DOS command window through the Command Line Interpreter parser. In this mode, the character stream is passed unaltered to and from the RSA. You can switch out of RSA console mode and return to CLI command mode by typing a tilde followed by a period (~.) To escape the tilde and have it sent to the console, supply a second tilde. Switching out of RSA console mode does not close the RSA-DOS console connection, which can be established again by issuing another `service console` command.

`exit` Closes the RSA-DOS console connection and returns the CLI session to CLI command mode.

`ftp start` Instructs the RSA to start the FTP server. Once the FTP server is started, standard OS 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 generates an error message from the CLI parser. The default ftp user name is "ftpuser" and the default ftp password is "ftp1234".

`ftp stop` Instructs the RSA to stop the FTP server.

set

Syntax:
`set prompt=`*`text`* `| prefix=`*`text`*

Description:
Defines the CLI command-line prompt and the prefix that is applied to CLI command responses. By default, the command-line prompt is "dpccli", and the default response prefix is an empty string.

Options:

`prompt=`*`text`*	Changes the CLI prompt to *`text`*.
`prefix=`*`text`*	Changes the response prefix to *`text`*.
`text`	The prompt or prefix text. You can supply any literal text characters plus the system variable $system, $time, and $date. These variables resolve to the hostname or IP Address, the system time, and date, respectively. The time and date reflect current time for the system that is hosting the network proxy.

shutdown

Syntax:
`shutdown [-f] [-r]`

Description:
Shuts down or resets the managed system, depending on which option is selected. By default, the software will attempt a graceful shutdown[53]. Performing a graceful O/S shutdown requires a proprietary O/S agent be present. If this agent is not present or unable to respond after 7 seconds, an error message will be displayed for the user and the command will terminate (no reset or power off performed). Graceful shutdown commands will not perform hard resets or power off if O/S shutdown does not complete. This model varies from previous implementations of graceful shutdown requests.

Options:

`[-f]`	Forces a power off without performing a graceful shutdown. A graceful shutdown requires Intel Server Management to be installed on the server.
`[-r]`	Causes the software to attempt a graceful shutdown and then execute the IPMI reset command.

version

Syntax:
`version`

Description:
Displays the version of the active network proxy (dpcproxy).

[53] The SE7210TP1-E server platform does not support a graceful shutdown of the operating system.

About the CLI Network Proxy (dpcproxy)

The ISM installation automatically installs and starts the network proxy that enables Command Line Interface and Serial over LAN[54]. The proxy is named *dpcproxy*. Ordinarily it starts running automatically on reboot and you do not need to do anything to start it. By default, the network proxy starts with no command line arguments supplied. However, you can change the persistent arguments that are read whenever dpcproxy automatically starts (see page 107 for details on dpcproxy's command line arguments). You can also manually start and stop the installed network proxy and check to see if it is running.

In addition, on Windows systems you can manually install the network proxy as a service (for example, on a system on which you have not installed ISM). Linux does not require daemons to be formally installed like Windows services. And, on either operating system, you can start the network proxy in the foreground without installing it, provided dpcproxy is not currently running in the background on the same port as the foreground process.

These actions are all described in the following sections, depending on your operating system.

NOTE

The network proxy installs as a single executable file (dpcproxy.exe on Windows and dpcproxy on Linux) and it can be run from any directory. The default client port of 623 is a privileged port. Unless you change the port by using the `-p` *command-line option (see table on page 107), the proxy will require root/administrative privileges to start. You can install the network proxy locally on each managed server or on a central proxy server.*

Changing the Persistent Arguments for the Network Proxy

By default, the network proxy starts with no command line arguments (see page 107 for details on dpcproxy's command line arguments). However, you can add arguments to the automatic start process for the network proxy, which will be read whenever the system is rebooted (i.e., persist across system boots).

On Windows

To view the current persistent arguments, issue the following command at the command prompt:

```
dpcproxy -viewarg
```

To change the persistent arguments for the network proxy, issue the following command at the command prompt:

```
dpcproxy -argchg arguments
```

For example,

```
dpcproxy -argchg -p 623
```

See page 107 for information on dpcproxy command line syntax and its valid arguments.

[54] The Serial Over LAN Feature is not supported on the SE7210TP1-E server platform.

On Linux

Edit the file `/etc/rc.d/init.d/cliservice` to supply command line arguments to the dpcproxy command in this file. Arguments supplied in the `cliservice` file will be used whenever the network proxy is restarted upon reboot.

To add command line arguments, edit the following line `/usr/local/cli/dpcproxy` in the `/etc/rc.d/init.d/cliservice` file, adding options as desired from the syntax table on page 107. The following is an example of an edited cliservice command file (see page 107 for details on dpcproxy's command line arguments):

```
/usr/local/cli/dpcproxy -p 623 -e
```

Manually Starting the Installed Network Proxy

If the installed dpcproxy service/daemon is currently stopped (either intentionally or because of a problem), and you want to restart it without rebooting the system, use one of the following methods:

On Windows

From Windows, you can start, stop, and check on the network proxy using any of the following methods:

- Use the Service Control Manager to view the status, start, or stop the "ISM DPC Proxy."
- Use the Control Panel to access the Administrative Tools window. From that window double-click on Services. The network proxy appears as "ISM DPC Proxy." From the Services window you can stop, start, and change properties of the service.
- From a command prompt you can use the net start command with no argument to list the services currently running. To start and stop the service use the following commands (note that you cannot supply dpcproxy command line arguments as part of the net start commands below):

  ```
  net start dpcproxy
  net stop dpcproxy
  ```

On Linux

From a Linux console you can start, stop and check on the network proxy as follows:

- Check that the proxy is running with the command
  `/etc/rc.d/init.d/cliservice status`
- If the proxy is not running, you can start it with the command
  `/etc/rc.d/init.d/cliservice start`
- If the proxy is running, you can stop it with the command
  `/etc/rc.d/init.d/cliservice stop`
- If the proxy is currently running, you can restart it with the command
  `/etc/rc.d/init.d/cliservice restart`

Manually Installing the Network Proxy

As stated above, the ISM install automatically installs the network proxy as a service (Windows) or daemon (Linux). However, you can manually install the service/daemon as well. For example, you may want to use the network proxy on a system where you have not installed ISM, or you may need to reinstall the network proxy at a later time.

On Windows

1. If you have not installed ISM on the system, copy the file dpcproxy.exe from the ISM CD to any directory on the system.
2. Change directory to the location of the dpcproxy.exe file on the system (the default ISM install directory is c:\Progam Files\Intel\servermanagement6x\bin).
3. Use the following dpcproxy command (see page 107 for details) to manually install the network proxy as a Windows service.

   ```
   dpcproxy -install
   ```

Once the network proxy is installed as a Windows service, you must then start the service (see page 105).

On Linux

If you have not installed ISM on the system, then from the ISM CD, run the rpm file associated with CLI by typing rpm -i *filename*. The naming convention for the CLI rpm file is as follows (depending on 32-bit or 64-bit platform):

ia32: CLI-<*release*>-1.i386.rpm

ia64: CLI-<*release*>-1.ia64.rpm

Once the rpm command completes, CLI is fully installed (but not started) on the Linux system. If you have already installed ISM on the system, no further installation action is required before starting the network proxy. See page 105 for information on starting the network proxy on Linux.

The dpcproxy Command Syntax

Ordinarily you won't need to enter a dpcproxy command, because the ISM installation starts the proxy as an automatic service or daemon. However, if you need to restart or reinstall the service, or supply persistent arguments to the automatic service/daemon (see page 104), use the command syntax described here.

Command line syntax is as follows, and each option is described in the table below.

```
dpcproxy  { { -? | -h } | { -f [-p port] [-L] [-l language] [-d logfiledir] [–u]
[-nv] [-e] [-la attempts] } | { -argchg arguments | -viewarg } |
{ -install [arguments] | -uninstall } }
```

NOTES

The- install and -uninstall options are only applicable to Windows, as they formally install or uninstall the network proxy as a Windows service. In addition, the -argchg and -viewarg options are also only applicable in Windows (see table below).

If you did not use the ISM install program to install the network proxy (i.e., you performed a manual install of dpcproxy), you must either update your path to include the directory in which the dpcproxy executable resides, or you must make that directory the current working directory before executing the dpcproxy command.

The dpcproxy Command-line Options

Option	Description
`-? or -h`	Displays a usage message and exits. If you specify either of these options, all other options and input text are ignored.
`-f`	Runs the network proxy in the foreground. **Required at the command prompt**, unless using only the -?, -h, -argchg, -viewarg, -install, or -uninstall options. For example, `dpcproxy –f –p 623`. Note that when supplying options in the Windows Service Control Manager or the Linux script cliservice, the -f option **cannot** be used.
`-p port`	Specifies an alternate port at which the network proxy listens for incoming client connections. By default, the network proxy listens on port 623, which is a privileged port in most operating systems.
`-L`	Forces the network proxy to accept connections only from the local host address (127.0.0.1). This option prevents this instance of the network proxy from providing services to systems other than the local system.

Continued

Option	Description
`-l language`	Localizes (displays in a specific language) messages and dates sent to a network proxy client. If you do not use this option, the network proxy detects the language from the Operating System. If a language is not specified on the command line the detected language is not a language supported by CLI, the network proxy defaults to English. Use the following codes to set the language (the first value is for Linux, the second for Windows): en_US or enu - English de_DE or deu - German ko_KR or kor - Korean es_ES or esp - Spanish zh_CN or chs - Chinese
`-d logfiledir`	Keeps a debug log file in the directory *logfiledir*. If you do not use this option, debug information is not logged.
`-u`	Turns off Serial over LAN data encryption for this instance of dpcproxy. With encryption off, all serial data transferred over the LAN is sent without encryption. **NOTE:** The Serial over LAN feature is not supported when managing the SE7210TP1-E server platform.
`-nv`	Sets non-verbose mode. No messages will be returned to the client. Only data from the commands will be returned.
`-e`	Sets "exit after error." If an error is encountered, close the client session.
`-la attempts`	Sets the number of login attempts to allow. If -e is specified as well, the -la argument is ignored and the session is closed on the first failure. <*attempts*> is the number of attempts before failing.
`-argchg arguments`	**Windows Only.** Persistently changes the startup arguments for the dpcproxy service (i.e., the command line options that will be used with the dpcproxy command when it is started upon reboot). Valid *arguments* are -p, -L, -l, -d, -u, -nv, -e, -la from this table.
`-viewarg`	**Windows Only.** Lists the current persistent arguments to be used with the dpcproxy command when the service is started upon reboot.
`-install [arguments]`	**Windows Only.** Installs the proxy as a Windows service. You can use this option only in a Windows environment. You can also specify the other options to be used each time the proxy starts. Enter other options after the `-install` option, if desired. Valid *arguments* are -p, -L, -l, -d, -u, -nv, -e, -la from this table. Once it is installed, the service will be started automatically (with specified options) every time the system starts up. **NOTE:** When using the -install option, the current working directory MUST be the directory in which the dpcproxy.exe file is located (that is, you must run the dpcproxy -install command from the directory where the dpcproxy.exe file is located). The proxy service is installed with an executable path specifying the current working directory. So, if you are in c:\mypath, and the dpcproxy.exe file is c:\different_path, the service will look for the dpcproxy.exe file in c:\mypath, and will not find it.
`-uninstall`	**Windows Only.** Removes the proxy from the Windows service control manager database. You can use this option only in a Windows environment. After removal, the proxy is no longer an installed service. Make sure to stop the service before you uninstall it.

8. Native Command Line

Native Command Line Overview

Native command line is a feature that allows you to directly send text-based commands to the server's Baseboard Management Controller (BMC) using a serial port connection.

NOTE

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

Terminal mode supports standard binary IPMI 1.5 hex-ASCII commands as well as specific text commands. In terminal mode you 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

Setup and Configuration

Connection Mechanism

You can connect to the server in two ways:

- Direct connection, where the local host is connected to the target system directly through each system's serial port. This requires a null modem cable.
- Modem connection, where the local host is connected to the target system via modem. This requires that each system is connected to its own modem using a serial cable.

Server Configuration Using the System Setup Utility (SSU)

To configure native command line on the server, run the System Setup Utility (SSU) as described in your server Product Guide and follow these steps.

1. On the SSU main screen, choose the Platform Event Manager (PEM)
2. On the PEM screen, choose Configure EMP.
3. On the Emergency Management Port (EMP) screen, make the following changes:
   a. Enter a password and verify the password
   b. For Access Mode, select Always Available
   c. In the Connection Mode box, pull down the menu and select Direct Connect Mode or Modem Connection, whichever is correct for your server.

d. Leave the Enable Data Terminal Ready box unselected.
e. Check the box to Enable Terminal Mode
f. Check the box to Enable Line Editing
(this lets you make changes to the input line before submitting it to the BMC for processing)
g. For Delete Control, select Backspace
(the other option is <Del>, and these options are only available if you enable line editing)
h. Check the box to Turn On BMC Echo Of Received Characters
(BMC echoes each character to the console as you enter it; highly recommended when you enable line editing)
i. Check the box to Enable Handshake When BMC ready to receive another message
(the BMC will return the string "SYS <newline sequence>" when it is ready to accept another message from the console)
j. For the Newline output sequence (BMC to console), select "CRLF"
(carriage return/linefeed)
k. For the Newline input sequence (console to BMC), select "CR"
(carriage return)

4. Click "Save" to save your settings and "OK" until you return to the main SSU menu.
5. Reboot the server.

Console Configuration:

1. Boot the console system to run Windows
2. Launch Hyperterminal: Click on the "Start" button in the task bar, select "Programs>Accessories>Communications" and click on Hyperterminal.
3. At the Connection Description window, enter "guest" for the name and click "OK" to proceed.
4. At the Connect To window, select the COM port of the console to which the modem or the null modem cable is connected, for example, COM1.
5. In the COM1 Properties window, select "19200" Bits per second for the Baud rate
6. For Flow Control, select "None"
7. Leave the default settings for the other boxes
8. Click "OK" to accept the settings and enter the Hyperterminal screen.
9. You will see characters being displayed to the Hyperterminal screen. This is the PING message sent by the BMC.
10. Press the <ESC> key followed by the "(" left parenthesis key. This enables Terminal Mode and ends the PING messages. The string "[TMODE OK]" should be displayed.
11. Enter the string "[SYS TMODE]" This is case sensitive and must be in uppercase. The response will be "[OK TMODE]" indicating that Terminal Mode is functioning.
12. To log into the Terminal Mode Session, enter the string "[SYS PWD -N guest]" The "-N" represents the Anonymous User and "guest" is the password. These items are case sensitive.
13. The BMC returns "[SYS]" and "[OK]" to show a successful login.
14. At this point, you can type any supported Terminal mode command (see the following pages).
15. To logout type "[SYS PWD -X]".

Native Command Line Commands

There are two basic formats for Native Command Line commands: text and hex-ASCII. These formats are explained in more detail below.

Input Syntax

Native command line messages follow the general syntax:

```
[<message data>]<newline sequence>
```

Each native command line message must be preceded with the left bracket "start" character and must be ended with a right bracket "stop" character and the configured input newline sequence. No input characters are accepted until the start character has been received.

Native command line text commands are case sensitive, but hex-ASCII commands can use either upper or lower case letters for ASCII representations of hex digits.

Native command line messages are limited to a maximum length of 122 characters. This includes the left and right brackets, but not control characters.

The only characters allowed are standard printable ASCII characters. All other characters are treated as illegal, except the following special characters. If the BMC receives an illegal character it clears the message in progress and goes back to looking for the start character.

Special Characters

<ESC> You can use the <ESC> character to delete an entire message prior to submission to the BMC. If line editing is enabled, and the <ESC> key is followed by an input newline sequence, the BMC responds by outputting an output newline sequence. Otherwise following an <ESC>, the BMC goes back to looking for the start character.

Special Character Handling - character

<Des> or **<Backspace>** Use the <Del> or <Backspace> key to delete the last character entered if the message has not yet been submitted to the BMC.

<Backslash><Newline> Split long IPMI messages across multiple lines by using the line continuation <backslash> character followed immediately by an input newline sequence. Line continuation characters are supported for both text and hex-ASCII commands.

Hex-ASCII Command Format

Binary IPMI commands are sent and received as a series of case insensitive hex-ASCII pairs, where each is optionally separated from the preceding pair by a single <space> character. Following is an example of a binary IPMI request message:

[18 00 22]<newline sequence>

The software ID and LUN for the remote console are fixed and implied by the command. The SWID for messages to the remote console is always 47h, and the Logical Unit Number (LUN) is 00b. Instead, there is a 'bridge' field that is used to identify whether the message should be routed to the BMC's bridged message tracking or not. This data is described in the following tables.

Table 1. Native Command Line Request to BMC

Byte	Explanation
1	[7:2] - Net Function (even) [1:0] - Responder's LUN
2	[7:2] - Requester's Sequence Number [1:0] - Bridge field
3	Command Number
4:N	Data

Table 2. Native Command Line Request from BMC

Byte	Explanation
1	[7:2] - Net Function (odd) [1:0] - Responder's LUN
2	[7:2] - Requester's Sequence Number [1:0] - Bridge field
3	Command Number
4	Completion Code
5:N	Data

Native Command Line IPMI Message Bridging

Native Command Line supports the ability to bridge IPMI messages to another interface when binary hex-ASCII IPMI commands are used. The message bridge is determined by the following: the bridge field, whether the message is a request or a response, the message direction with respect to the BMC and the LUN. Table 30 lists the supported BMC combinations for IPMI message bridging. Any other combinations are unsupported.

Note that IPMI messages to and from the system interface are transferred using the BMC SMS (System Management Software) LUN, 10b, and with the bridge field set to 00b.

Table 3. Supported BMC Combinations for IPMI Message Bridging

Bridge Field	Request/Response	Message Direction (to BMC)	LUN	Message Interpretation
00b	Request	In	00b, 01b, 11b	Remote Console request to BMC functionality Message is a request from the remote console to the BMC.
00b	Response	Out	00b, 01b, 11b	Response to Remote Console from BMC functionality Message is a response to an earlier request from the remote console to the BMC.
00b	Request	In	10b	Remote Console request to SMS Message is a request from the remote console to SMS via the Receive Message Queue.
00b	Response	Out	10b	SMS Response to Remote Console Message is a response to an earlier request from SMS.
01b	Response	Out	Any	Response to earlier Bridged Request from Remote Console Message is the asynchronous response from an earlier bridged request that was encapsulated in a Send Message command issued to the BMC by the remote console.

Text Command Format

Text commands do not support the bridging and sequence number fields used in the hex-ASCII commands. Text commands are case-sensitive, and must be preceded by the prefix string "SYS".

Examples

Hex-ASCII command example (IPMI Reset Watchdog Cmd):

```
[18 00 22]<CR>
[1C 00 22 00]<CR-LF>
```

Text command example:

```
[SYS TMODE]<CR>
[OK TMODE]<CR-LF>
```

Table 4. Native Command Line Text Commands

Command	Switches	Description
SYS PWD	-U USERNAME <password>	Used to activate a terminal mode session. USERNAME corresponds to the ASCII text for the username. <password> represents a printable password (up to 16 characters). If <password> is not provided, then a Null password (all binary 0's) is submitted. Passwords are case sensitive. Either the SYS PWD command (or Activate Session IPMI message) must be successfully executed before any command or IPMI messages are accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
	-N <password>	-N represents a Null username. <password> represents a printable password (up to 16 characters). If <password> is not provided, then a Null password (all binary 0's) is submitted. Passwords are case sensitive. Either the SYS PWD command (or Activate Session IPMI message) must be successfully executed before any command or IPMI messages are accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
	-X	-X immediately 'logs out' any presently active session. Entering an invalid password with -U or -N also has the same effect.
SYS TMODE		Used as a 'no-op' confirm that Terminal Mode is active. BMC returns an OK response followed by "TMODE".
SYS SET BOOT XX YY ZZ AA BB		Sets the boot flags to direct a boot to the specified device following the next IPMI command or action initiated reset or power-on. XX...BB represent five hex-ASCII encoded bytes, which are the boot flags parameter in the Boot Option Parameters. See the Boot Option Parameters Table below for more information. Upon receiving this command, the BMC automatically sets the 'valid bit' in the boot options and sets all the Boot Initiator Acknowledge data bits to 1b.

continued

Table 4. Native Command Line Text Commands (continued)

Command	Switches	Description
SYS SET BOOTOPT XX YY...NN		This is essentially a text version of the IPMI "Set System Boot Options" command. It allows any of the boot option parameters to be set, not just the boot flags. XX YY...NN represent the hex-ASCII encodings for the data bytes that are passed in the Set System Boot Options request. See the Boot Option Parameters Table below for more information. XX - Parameter valid [7] - 1b = Mark parameter invalid / locked 0b = Mark parameter valid / unlocked [6:0] - Boot option parameter selector YY...NN -- Boot Option Parameter Data Per Boot Option Parameters Table below. Passing 0-bytes of parameter data allows the parameter valid bit to be changed without affecting the present parameter setting.
SYS GET BOOTOPT XX YY ZZ		This is essentially a text version of the IPMI "Get System Boot Options" command. It allows any of the boot option parameters to be retrieved. XX YY ZZ represents the hex-ASCII for the data bytes that are passed in the Get System Boot Options request. The BMC returns the data from the command in hex-ASCII format. See the Boot Option Parameters Table below for more information. XX - Parameter selector [7] -Reserved [6:0] - Boot option parameter selector YY - Set Selector [7:0] -Selects a particular block or set of parameters under the given parameter selector Write as 00h if parameter doesn't use a Set Selector. ZZ - Block Selector Selects a particular block within a set of parameters. Write as 00h if parameter doesn't use a Block Selector. Note: As of this writing, there are no IPMI-specified Boot Options parameters that use the block selector. However, this field is provided for consistency with other configuration commands and as a placeholder for future extension of the IPMI specification.

continued

Table 4. Native Command Line Text Commands (continued)

Command	Switches	Description
SYS SET TCFG		Returns the Terminal Mode Configuration bytes where XX and YY represent hex-ASCII encodings for the volatile version of data bytes 1 and 2 as specified in the Terminal Mode Configuration Table below, and AA BB represent hex-ASCII encoding of the non-volatile version. V:XX YY<output termination sequence> N:AA BB<output termination sequence>
	-V XX YY	This command sets the volatile Terminal Mode Configuration. XX and YY represent hex-ASCII encodings for data bytes 1 and 2 as specified in the Terminal Mode Configuration Table below. The BMC returns the same output as for SYS SET TCFG, above.
	-N XX YY	This command sets the non-volatile Terminal Mode Configuration. XX and YY represent hex-ASCII encodings for data bytes 1 and 2 as specified in the Terminal Mode Configuration Table below. The BMC returns the same output as for SYS SET TCFG, above.
SYS RESET		Directs the BMC to perform an immediate system hard reset.
SYS POWER OFF		Directs the BMC to perform an immediate system power off.
SYS POWER ON		Causes the BMC to initiate an immediate system power on.
SYS HEALTH QUERY		Causes the BMC to return a high level version of the system health status in 'terse' format. The BMC returns a string with the following format if the command is accepted. PWR:zzz H:xx T:xx V:xx PS:xx C:xx D:xx S:xx O:xx Where: PWR is system POWER state H is overall Health T is Temperature V is Voltage PS is Power Supply subsystem F is cooling subsystem (Fans) D is Hard Drive / RAID Subsystem S is physical Security O is Other (OEM)

continued

Table 4. Native Command Line Text Commands (continued)

Command	Switches	Description
SYS HEALTH QUERY (cont)		zzz is: "ON", "OFF" (soft-off or mechanical off), "SLP" (sleep - used when can't distinguish sleep level), "S4", "S3", "S2", "S1", "??" (unknown) and xx is: ok, nc, cr, nr, uf, or ?? where: "ok" = OK (monitored parameters within normal operating ranges) "nc" = non-critical ('warning': hardware outside normal operating range) "cr" = critical ('fatal': hardware exceeding specified ratings) "nr" = non-recoverable ('potential damage': system hardware in jeopardy or damaged) "uf" = unspecified fault (fault detected, but severity unspecified) "??" = status not available/unknown (typically because system power is OFF)
SYS 000157 ACTIVATE		Activates the Intel OEM Terminal Mode extensions. This allows Intel OEM text commands to be entered without the 000157 text prefix. To enable the OEM commands this command must be executed every time a session is activated.
SYS ID		Displays the 16-byte system GUID of the managed server. Output formatted similar to what is displayed by the DPCCLI command.
SYS NETWORK	MAC| IP| SUBNET | GATEWAY	Displays the network configuration of the BMC. Using the mac, ip, subnet or gateway parameters only display the requested information. Output formatted similar to what is displayed by the DPCCLI command. This only displays information for the primary OOB NIC.
SYS DIAGINT		Causes the BMC to generate an IPMI diagnostic interrupt (NMI for IA-32 systems).
SYS BOOT	-F NORMAL | SERVICE[1]	The boot command sets the IPMI boot options and resets the system. This command is different then the IPMI "set boot" command. boot: This command attempts a graceful shutdown of the OS before resetting. With no parameters this is the same as "shutdown –r". boot –f: Forces a hard reset (no graceful shutdown). With no additional parameters this is the equivalent of "shutdown –rf". boot (normal | service): This command can also have the –f option. Sets the needed boot flags for use on the next boot. This command only sets the required boot flags. If BIOS does not support the required boot flags it will have no effect on the boot sequence.
SYS SHUTDOWN	-R -F[1]	Shutdown = Graceful O/S shutdown and power off Shutdown –f = Forced system power off Shutdown –r = Graceful O/S shutdown then a system hard reset Shutdown –r -f = Forced system hard reset

continued

Table 4. Native Command Line Text Commands (continued)

Command	Switches	Description
SYS IDENTIFY	-ON [# of SECONDS] -OFF	Instructs the server to signal its location by turning on the LED or beep. IDENTIFY = enables the server to identify itself for 15 seconds. IDENTIFY ON = enables the server to identify itself for 15 seconds. IDENTIFY ON XX = Causes the BMC to signal the system's location for a specific amount of time. XX is a hex-ASCII byte representing the number of seconds the BMC is to cause the system to identify itself. If XX is 00 the BMC will signal the system's location until a request to stop (via the IDENTIFY OFF command, other software commands or the ID Button) is received. IDENTIFY OFF = Causes the BMC to stop signaling the system's location. This has no effect if the system is not currently identifying itself. IDENTIFY –S = Displays the current identify state and source of request. ON (Application) ON (Button) OFF Software execution will make the system ID LED blink. Hardware execution (front panel switch) will make it go on solid. If the software has already turned on the ID LED (the ID LED will be blinking) then the hardware ID LED button will do the following: 0- software turns on the LED to blinking. 1- Pressing the hardware LED button will turn the LED OFF. (preferred) 2- Pressing the hardware LED button a second time will turn the LED on solid.
ALARM -S	-A id -L severity	This command sets or adds a Telco Alarm record to the Telco Alarm database. The generator id will always be 47h and the software originator id will be 0. Parameters: [-A id] - Alarm ID [-L severity] - Alarm Severity Level. Severities are CRT (critical), MJR (major) and MNR (minor). The BMC returns any one of the following response: • New alarm added to BMC TAM alarm database. • Request alarm matches existing BMC TAM alarm database record. • Request alarm updated an existing BMC TAM alarm database record. • BMC TAM alarm database is full. Request alarm record bumped because of lower priority. BMC TAM alarm database is full. Request alarm record bumped existing record.

continued

Table 4. Native Command Line Text Commands (continued)

ALARM –Q	{{-G id {-O id} {-A id}} | {-L severity} {–P} }	This command queries Telco alarm records in the Telco alarm database based on the options entered by the user. Options: [-G id] - Query against the generator ID specified. [-O id] - Query against the software originator ID specified. [-A id] - Query against the alarm ID specified. [-L severity] - Query against the severity specified. Severities are CRT (critical), MJR (major) and MNR (minor). [-P] - Query only alarms that are related to power. The BMC returns the response string in the following format: AlarmGenID=id AlarmSW=[Y|N] AlarmSWID=id AlarmID=id AlarmSev=severity AlarmPWR=[Y|N]
ALARM –C	({{-G id {-O id} {-A id}} | {-L severity}} | ALL)	This command clears all Telco records in the Telco alarm database based on the options entered by the user. Options: [-G id] - Clears alarms that match the generator ID specified. [-O id] - Clears alarms that match the software originator ID specified. [-A id] - Clears alarms that match the alarm ID specified. [-L severity] - Clears alarms that match the severity specified. Severities are CRT (critical), MJR (major) and MNR (minor). ALL - Clears all alarm records. The BMC returns the response string in the following format: (id value represented in decimal) Alarm ID id cleared (Generator ID id)
SYS HELP	COMMAND	Displays the syntax and usage information for the command specified. If a command is not specified the current IPMI revision, FW version numbers and all supported commands are displayed.

1. Execution of graceful OS shutdown has restrictions listed below.

Performing a graceful O/S shutdown requires a proprietary O/S agent be present. If this agent is not present or unable to respond after 7 seconds, an error message will be displayed for the user and the command will terminate (no reset or power off performed). Graceful shutdown commands will not perform hard resets or power off if O/S shutdown does not complete. This model varies from previous implementations of graceful shutdown requests.

Table 5. Boot Option Parameters

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Set In Progress (volatile)	0	Data 1 - This parameter is used to indicate when any of the following parameters are being updated, and when the updates are completed. The bit is primarily provided to alert software that some other software or utility is in the process of making changes to the data. The change shall take effect when the write occurs. [7:2] - Reserved [1:0] - 00b = Set complete. If a system reset or transition to powered down state occurs while 'set in progress' is active, the BMC goes to the 'set complete' state. If rollback is implemented, going directly to 'set complete' without first doing a 'commit write' causes any pending write data to be discarded. 01b = Set in progress. This flag indicates that some utility or other software is presently doing writes to parameter data. It is a notification flag only, it is not a resource lock. The BMC does not provide any interlock mechanism that would prevent other software from writing parameter data while. 10b = Reserved 11b = Reserved
Service partition selector (semi-volatile)[1]	1	Data 1 [7:0] - Service partition selector. This value is used to select the service partition from which that BIOS should boot. This document doesn't specify which value corresponds to a particular service partition. 00h = Unspecified.
Service partition scan (semi-volatile)[1]	2	Data 1 [7:2] - Reserved [1] - 1b = Request BIOS to scan for specified service partition. BIOS clears this bit after the requested scan has been performed. [0] - 1b = Service Partition discovered. The BIOS sets this bit to indicate it has discovered the specified service partition. The BIOS must clear this bit on all system resets and power ups, except when a scan is requested.

continued

Table 5. Boot Option Parameters (continued)

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
BMC boot flag valid bit clearing (semi-volatile)[1]	3	Data 1 - BMC boot flag valid bit clearing. Default = 0000b. [7:5] - Reserved [4] - 1b = Don't clear valid bit on reset/power cycle caused by PEF [3] - 1b = Don't automatically clear boot flag valid bit if IPMI Chassis Control command not received within 60-second timeout (countdown restarts when a IPMI Chassis Control command is received) [2] - 1b = Don't clear valid bit on reset/power cycle caused by watchdog timeout [1] - 1b = Don't clear valid bit on pushbutton reset / soft-reset (e.g. "Ctrl-Alt-Del") [0] - 1b = Don't clear valid bit on power up via power pushbutton or wake event
Boot info acknowledge (semi-volatile)[1]	4	These flags are used to allow individual parties to track whether they've already seen and handled the boot information. Applications that deal with boot information should check the boot info and clear their corresponding bit after consuming the boot options data. Data 1: Write Mask ('write-only'. This field is returned as 00h when read. This is to eliminate the need for the BMC to provide storage for the Write Mask field.) [7] - 1b = enable write to bit 7 of Data field [6] - 1b = enable write to bit 6 of Data field [5] - 1b = enable write to bit 5 of Data field [4] - 1b = enable write to bit 4 of Data field [3] - 1b = enable write to bit 3 of Data field [2] - 1b = enable write to bit 2 of Data field [1] - 1b = enable write to bit 1 of Data field [0] - 1b = enable write to bit 0 of Data field Data 2: Boot Initiator Acknowledge Data The boot initiator should typically write FFh to this parameter prior to initiating the boot. The boot initiator may write 0's if it wants to intentionally direct a given party to ignore the boot info. This field is automatically initialized to 00h when the management controller is first powered up or reset. [7] - reserved. Write as 1b. Ignore on read. [6] - reserved. Write as 1b. Ignore on read. [5] - reserved. Write as 1b. Ignore on read. [4] - 0b = OEM has handled boot info. [3] - 0b = SMS has handled boot info. [2] - 0b = OS / service partition has handled boot info. [1] - 0b = OS Loader has handled boot info. [0] - 0b = BIOS/POST has handled boot info.

continued

Table 5. Boot Option Parameters (continued)

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot flags (semi-volatile)[1]	5	Data 1 [7] - 1b = Boot flags valid. The bit should be set to indicate that valid flag data is present. This bit may be automatically cleared based on the boot flag valid bit clearing parameter, above. [6:0] - Reserved BIOS support for the following flags is optional. If a given flag is supported, it must cause the specified function to occur in order for the implementation to be considered to be conformant with this specification. The following parameters represent temporary overrides of the BIOS default settings. BIOS should only use these parameters for the single boot where these flags were set. If the bit is 0b, BIOS should use its default configuration for the given option. Data 2 [7] - 1b = CMOS clear [6] - 1b = Lock Keyboard [5:2] - Boot device selector 0000b = No override 0001b = Force PXE 0010b = Force boot from default Hard-drive[2] 0011b = Force boot from default Hard-drive, request Safe Mode[2] 0100b = Force boot from default Diagnostic Partition[2] 0101b = Force boot from default CD/DVD[2] 0110b-1110b = Reserved 1111b = Force boot from Floppy/primary removable media [1] - 1b = Screen Blank [0] - 1b = Lock out Reset buttons

continued

Table 5. Boot Option Parameters (continued)

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot flags (semi-volatile)[1] (continued)	5	Data 3 [7] - 1b = Lock out (power off/ sleep request) via Power Button [6:5] - Firmware (BIOS) Verbosity (Directs what appears on POST display) 00b = System default 01b = Request quiet display 10b = Request verbose display 11b = reserved [4] - 1b = Force progress event traps. When set to 1b, the BMC transmits PET traps for BIOS progress events to the LAN or serial/modem destination for the session that set the flag. Since this capability uses PET traps, this bit is ignored if for connection modes that do not support PET such as Basic Mode and Terminal Mode. [3] - 1b = User password bypass. When set to 1b, the managed client's BIOS boots the system and bypasses any user or boot password that might be set in the system. [2] - 1b = Lock Sleep Button. When set to 1b, directs BIOS to disable the sleep button operation for the system, normally until the next boot cycle. [1:0] - 00b = Console redirection occurs per BIOS configuration setting 01b = Suppress (skip) console redirection if enabled 10b = Request console redirection be enabled 11b = Reserved

continued

Table 5. Boot Option Parameters (continued)

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot flags (semi-volatile)[1] (continued)	5	Data 4 [7:4] - Reserved [3] - BIOS Shared Mode Override Can be used to request BIOS to temporarily place the channel into Shared access mode. Per the recommendations in the IPMI specification, 'Shared' access would cause the baseboard serial controller to both remain enabled after POST/start of OS boot, while also allowing the BMC to be accessible. This can be useful when booting to an alternative device such as a Diagnostic Partition since it means the partition can use the serial port but that communication with the BMC can remain available if the partition software fails. 1b = Request BIOS to temporarily set the access mode for the channel specified in parameter #6 to 'Shared'. This is typically accomplished by sending a 'Set Channel Access' command to set the volatile access mode setting in the BMC. 0b = No request to BIOS to change present access mode setting. [2:0] - BIOS Mux Control Override Can be used to request BIOS to force a particular setting of the serial/modem mux at the conclusion of POST / start of OS boot. This override takes precedence over the mux settings for the access mode even if the BIOS Shared Mode Override is set. 000b = BIOS uses recommended setting of the mux at the end of POST (See IPMI specification for more info). 001b = Requests BIOS to force mux to BMC at conclusion of POST/start of OS-boot. If honored, this overrides the recommended setting of the mux at the end of POST (See IPMI specification for more info.) 010b = Requests BIOS to force mux to system at conclusion of POST/start of OS-boot. If honored, this overrides the recommended setting of the mux at the end of POST. (See IPMI specification for more info.) Data 5 - Reserved

continued

Table 5. Boot Option Parameters (continued)

Parameter	#	Parameter Data (non-volatile unless otherwise noted)
Boot initiator info (semi-volatile)[1]	6	Address & Identity information for the party that initiated the boot. The party that initiates the boot writes this parameter and the boot info acknowledge parameter prior to issuing the command that causes the system power up, power cycle, or reset. This data is written by the remote console application, not the BMC. Boot Source Data 1- Channel Number. Channel that delivers the boot command (e.g. chassis control). BIOS and boot software (e.g. service partition or OS loader) can use the Get Channel Sessions to find out information about the party that initiated the boot. [7:4] - Reserved [3:0] - Channel Number Data 2:5 - Session ID. Session ID for session that the boot command will be issued over. This value can be used with the Get Channel Sessions command to find out information about the party that initiated the boot. Data 6:9 - Boot Info Timestamp. This timestamp is used to help software determine whether the boot information is 'stale' or not. A service partition or OS loader may elect to ignore the boot information if it is older than expected. The boot initiator should load this field with the timestamp value from the IPMI Get SEL Time command prior to issuing the command that initiates the boot.
Boot initiator mailbox (semi-volatile)[1][2]	7	This parameter is used as a 'mailbox' for holding information that directs the operation of the OS loader or service partition software. Note: Since this information is retained by the BMC and may be readable by other software entities, care should be taken to avoid using it to carry 'secret' data. Data1: Set Selector = Block selector Selects which 16-byte info block to access. 0-based. Data 2: (17) Block data The first three bytes of block #0 are required to be an IANA Enterprise ID Number (least significant byte first) for the company or organization that has specified the loader. Up to 16-bytes per block of information regarding boot initiator, based on protocol and medium. The BMC supports five blocks of storage for this command. Previous values are overwritten. The BMC does not automatically clear any remaining data bytes if fewer than 16 bytes are written to a given block.
All other parameters	All Others	Reserved

1. The designation 'semi-volatile' means that the parameter will be kept across system power cycles, resets, system power on/off, and sleep state changes, but will not be preserved if the management controller loses standby power or is cold reset. Parameters designated as 'semi-volatile' are initialized to 0's upon controller power up or hard reset, unless otherwise specified.
2. IPMI allows software to use the boot initiator mailbox as a way for a remote application to pass OEM parameters for additional selection of the boot process and direction of the startup of post-boot software. If additional parameters are not included, the system boots the primary/first-scanned device of the type specified.

Table 6. Native Command Line Configuration

Byte	Explanation
1	[7:6] - Reserved [5] - Line Editing 0b = Disable 1b = Enable (Factory default) [4] - Reserved [3:2] - Delete control (only applies when line editing is enabled) 00b = BMC outputs a <DEL> character when <BKSP> or < DEL > is received 01b = BMC outputs a < BKSP >< SP >< BKSP > sequence when < BKSP > or < DEL > is received (Factory default) [1] - Echo control0b = No echo 1b = Echo (BMC echoes characters it receives) (Factory default) [0] - Handshaking - BMC outputs a [SYS]<newline> after receiving each terminal mode IPMI message and is ready to accept the next message. 0b = Disable 1b = Enable (Factory default)
2	[7:4] - Output newline sequence (BMC to console). Selects what characters the BMC uses as the <newline> sequence when the BMC writes a line to the console in Terminal Mode. 0h = no termination sequence 1h = <CR-LF> (Factory default) 2h = <NULL> 3h = <CR> 4h = <LF-CR> 5h = <LF> All other = reserved [3:0] - Input newline sequence (Console to BMC). Selects what characters the console uses as the <newline> sequence when writing to the BMC in Terminal Mode. 0h = reserved 1h = <CR> (Factory default) 2h = <NULL> All other = reserved

9. One-Boot Flash Update Utility

This section describes the process for updating the BIOS and firmware (BMC, FRU, and SDR) on a server while the operating system is running. Once the update process has completed, the next system reset activates the newly updated BIOS and/or firmware.

NOTE

The One-Boot Flash Update Utility is not supported when managing SE7210TP1-E server systems.

For information on installing this utility, see page 27.

The One-Boot Flash Update Utility, the software, which performs the update, runs on Windows 2000 and Red Hat Linux 8.0, and is launched from a command prompt in either operating system. The new versions of BIOS and firmware images are programmed in secondary flash memory and are not used until the next system reset (the utility sets the BIOS and firmware update notification flags when the BIOS and firmware have been successfully updated). After a system reset, the newer versions are validated and activated. If the newer versions fail to be validated or activated after the reset, then the current version will be restored and used instead—in effect canceling the update.

NOTE

In the case of FRU, the update is performed directly on the current version. FRU is not stored in secondary flash memory like the BIOS and other firmware. Therefore, no restoration of the previous FRU version is possible.

The One-Boot Flash Update Utility expects a configuration (CFG) file (default name flashupdt.cfg) to be present in the location specified by the < *URL or path* > argument supplied when the One-Boot Flash Update Utility is started (see Command Line Syntax below). This location must be the same location as the actual files for use in the update. The configuration file is a text file containing information about the update files.

This utility can be executed remotely via a secure network connection using a Telnet Client and Terminal Services in Windows or using a Telnet Client and Remote Shell under Linux.

Command Line Syntax for One-Boot Flash Update Utility

One-Boot Flash Update Utility requires administrative (Windows) or root (Linux) permissions.

Syntax:
`flashupdt [-i] [-u < URL or path >] [-c] [-h|?]`

Description:

Updates the BIOS and/or firmware on the local server with the BIOS and/or firmware specified in the configuration file.

Options:

[-i] Displays the version information for the currently running BIOS and firmware. If the -i option is specified with –u option, the utility displays the version information of the update package files.

[-u] Performs the BIOS and firmware update; <*URL or path*> specifies location where the files required for the update are located, including the configuration file. If no filename is specified in URL or path, the utility expects the default flashupdt.cfg for the configuration file. The value of <*URL or path*> can be a local file system path, an FTP server, or an HTTP server. See examples below:

-u	Specifies the current local directory.
-u http://<IP address or URL>/<path>	Specifies an HTTP server.
-u ftp://<login:password>@<server name or IP address>/<path>	Specifies an FTP server.

[-c] Cancels all pending update operations that were performed using the utility. The utility resets the internal flags in the BIOS, BMC, and SDR to cancel the update operation, whether there is one or not. Note that FRU updates can not be cancelled with this option since the FRU updates are executed immediately.

[-h|?] Displays command line help information.

10. Glossary

The following terms and abbreviations are used in this document:

Term	Description
CA Unicenter TNG	Computer Associates Unicenter The Next Generation
CSSU	Client System Setup Utility lets you run SSU remotely from a client
DMI	Desktop Management Interface
DPC	Direct Platform Control
EMP	Emergency Management Port—the COM2 serial port on a server
ESMC	Enterprise Server Management Console, a non-ISM or third-party management console that can integrate with ISM software
FRU	Field Replaceable Units
GUID	Globally Unique Identifier
ICMB	Intelligent Chassis Management Bus
IPMI	Intelligent Platform Management Interface
ISC	Intel Server Control is the former name of Intel Server Management (ISM)
ISM	Intel Server Management
MBE	Multiple-Bit Error
MIF	Management Information Format, used by DMI for describing component instrumentation
NIC	Network Interface Controller—a network access port
NMI	Non-Maskable Interrupt
PIC	Platform Instrumentation Control, which runs on the client system
PI	Platform Instrumentation, which runs on the managed server system
PXE	Preboot Execution Environment, code that enables booting from a network server
RAID	Redundant Array of Inexpensive Disks
RPC	Remote Procedure Call
SBE	Single-Bit Error
SCSI	A type of bus used to access peripherals such as hard disks
SCW	Server Configuration Wizard – DOS utility to configure the server for server management features
SDR	Sensor Data Records
SEL	System Event Log
SMI	System Management Interrupt
SNMP	Simple Network Management Protocol, a standard network protocol for management information
SSU	System Setup Utility lets you do low-level configuration on a server
SUM	System Update Manager
TCO	Total Cost of Ownership port—a particular network access port on a server

Appendix A. The Service Partition and Utilities

NOTE

The SE7210TP1-E server platforms do not support service partitions. Thus, service partition utilities do not apply to these server platforms.

Service Partition

The service partition is a special hard disk partition on the server system that you install or update with the Server Configuration Wizard. This partition contains utilities such as the System Setup Utility (SSU) and other software required for remote management. The service partition is not marked as an active partition and the server will only boot from it by a special request. Low-level disk utilities may see the partition entry as an EISA partition and recognize its space.

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

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

When you run the Server Configuration Wizard you decide whether to install or upgrade the service partition. If you check this configuration option and the server does not have an existing service partition, the wizard will present you with options where one can be created. If the server has an existing service partition, the wizard will upgrade it with utilities from the CD.

NOTE

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

Locally Booting the Server from the Service Partition

To run the utilities (such as SSU) that are installed on the service partition, boot the server from the service partition. You can reboot a server locally to run the SSU directly and configure the server for management. Later, after ISM software is installed on both console and server systems, you can also boot from the service partition remotely, using DPC, Client SSU, or the Command Line Interface (CLI), as described elsewhere in this manual.

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

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

Utilities

An option in the Server Configuration Wizard allows you to run these Server Configuration Utilities:

- Service Partition Administrator (SPADMIN)
- System Setup Utility (SSU)
- Field Replaceable Units (FRU) and Sensor Data Record (SDR) Loader Utility

Service Partition Administrator (SPADMIN)

SPADMIN is the software utility that lets you create and configure the service partition on the server’s hard disk drive. For information on how to use this utility, refer to the server’s platform documentation.

System Setup Utility

The SSU lets you set and display specific attributes of the server's firmware. You should be very familiar with the configurable aspects of the server before using the SSU to alter any settings.

Not only can you enter the SSU from the Server Configuration Wizard, you can also run SSU in these ways:

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

B. You can remotely run the SSU interface from the client console using the Client SSU (CSSU) component of ISM. To reboot to the service partition and run SSU, Select (Re)Connect from the Server menu in CSSU.

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

FRUSDR Loader Utility

The FRUSDR Load utility lets you load and display system FRUs and SDRs. For information on how to use this utility, refer to the server product guide.