Intel® Remote Management Module 4 and Integrated BMC Web Console User Guide

Revision 2.7

July 2013

Enterprise Platforms and Services Division

Revision History

Date	Revision Number	Modifications
February 2011	1.0	After second review. Screen captures updated.
December 2011	2.0	Renamed document and added EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families.
December 2011	2.1	Update for new speed POR.
January 2012	2.2	• Added AXXRMM4R. • Added description of Mouse Mode "Other". • Added description of KVM mouse mode selection capability.
March 2012	2.3	• Added S2400GP, S2400LP, S2600IP, S2600WP, W2600CR boards and systems. • Updated S1200BTL System Debug Log Page information. • Added notes for USB Key not attaching. • Added EMI bracket cover information. • Multiple corrections to the documentation.
May 2012	2.4	• Updated multi node SKU information. • Added S2400EP board and system. • Updated EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families System Debug Log section.
August 2012	2.5	• Changed references to multi node products. • Added note for About button. • Added note for F5 and page refresh not being supported. • Added clarifications on Remote Console page. • Added S1400FP, S1400SP, and S4600LH2/S4600LT2 boards and systems.
December 2012	2.6	Added S1600JP.
July 2013	2.7	• Added S1200V3RP. • Updated Remote Sessions page. • Updated Remote Alerts page. • Updated Server Power Control page. • Corrected R1000SP entry in Table 3. • Updated screen captures.

Disclaimers

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.

Table of Contents

1. Introduction 1
1.1 Target Audience 1
1.2 Terminology 1
1.3 Safety Information 2
1.4 Support Information 6
1.5 Warranty Information 6
2. Intel® Remote Management Module 4 Overview 7
2.1 Intel® RMM4 Lite and Intel® Dedicated Server Management NIC 7
2.2 Intel® RMM4 Features 8
2.3 Supported Operating Systems and Internet Browsers 8
2.3.1 Server System 9
2.3.2 Client System 9
3. Hardware Installations and Initial Configuration 10
3.1 Before You Begin 10
3.2 Tools and Supplies Needed 10
3.3 Installation 10
3.3.1 Installation of the Intel® RMM4 Lite on Intel® Server Boards 11
3.3.2 Installation of the Intel® Dedicated Server Management NIC on an Intel® Rack Server System 12
3.3.3 Installation of the Intel® Dedicated Server Management NIC on an Intel® Multi Node Server System 20
3.3.4 Installation of the Intel® Dedicated Server Management NIC on an Intel® Rack Optimized Server System 20
3.3.5 Installation of the Intel® Dedicated Server Management NIC on an Intel® Pedestal Server System 20
3.3.6 Installation of the Intel® Dedicated Server Management NIC on a Third-party Pedestal Chassis 25
4. Configuring the Integrated BMC Web Console and Intel® RMM4 28
4.1 Configuring the Server Management NIC using BIOS Setup on S1200BTL 29
4.2 Configuring the Server Management NIC using BIOS Setup on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 and S1200V3RP Product Families 30
4.3 Configuring the Server Management NIC using the Intel® Deployment Assistant (IDA) 32
4.4 Configuring the Server Management NIC using the Intel® System Configuration Utility (SysConfig) 41
4.4.1 Configuring the User 41
4.4.2 Configuring the IP Address 41
4.4.3 Configuring the Serial Over LAN 41
5. Getting Started with Intel® RMM4 Operation 42

5.1 Before You Begin 42
5.1.1 Client Browsers 42
5.2 Logging In 43
5.3 Navigation 44
5.4 Online Help 46
5.5 Logging Out 47
6. Remote Console (KVM) Operation 48
6.1 Launching the Redirection Console 48
6.2 Main Window 49
6.3 Remote Console Control Bar 50
6.3.1 Remote Console Video Menu 51
6.3.2 Remote Console Keyboard Menu 51
6.3.3 Remote Console Mouse Menu 54
6.3.4 Remote Console Options Menu 56
6.3.5 Remote Console Device Menu 57
6.4 Remote Console Status Line 58
7. Intel® Integrated BMC Web Console Options 59
7.1 System Information Tab 59
7.1.1 System Information Page 59
7.1.2 Field Replaceable Unit (FRU) Information Page 63
7.1.3 System Debug Log Page 64
7.1.4 DIMM Information Page 68
7.1.5 CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 69
7.1.6 Current Users Page on S1200V3RP Product Family 70
7.2 Server Health Tab 71
7.2.1 Sensor Readings Page 71
7.2.2 Event Log Page 73
7.2.3 Power Statistics Page 76
7.3 Configuration Tab 78
7.3.1 Network or IPv4 Network Page 78
7.3.2 IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 81
7.3.3 Users Page 83
7.3.4 Login Security Settings Page 85
7.3.5 LDAP Settings Page 87
7.3.6 VLAN Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 88
7.3.7 SSL Upload Page 90
7.3.8 Remote Session Page 91
7.3.9 Mouse Mode Page 96

7.3.10 Keyboard Macros Page 99
7.3.11 Alerts Page 101
7.3.12 Alert Email Page 103
7.3.13 Node Manager Power Polices Page on EPSD Platforms Based on Intel® Xeon® Processor E5−4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 104
7.4 Remote Control Tab 107
7.4.1 Console Redirection Page 107
7.4.2 Server Power Control Page 108
7.4.3 Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5−4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 112

List of Figures

Figure 1: Intel® RMM4 Lite 7
Figure 2: Intel® Dedicated Server Management NIC 8
Figure 3: Installing the Intel® RMM4 Lite on Intel® Server Boards 12
Figure 4: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module 13
Figure 5: Attaching the Cable to the Intel® Dedicated Server Management NIC Module 14
Figure 6: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000BTL and R1000RP Families 15
Figure 7: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000IP Family 15
Figure 8: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000LH2/R200LT2 16
Figure 9: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000BB and R2000BB Families, R1000SP Family, or R1000GZ/GL and R2000GZ/GL Families17
Figure 10: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000EP Family 18
Figure 11: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module 19
Figure 12: Installing the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000FP Family or R2000SC Family 19
Figure 13: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module 21
Figure 14: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000BTL and P4000RP Families 22
Figure 15: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000CP Family, P4000FP Family, P4000GP Family, P4000SC Family, or P4000M Chassis .. 23
Figure 16: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000CR Family or P4000IP Family 23
Figure 17. Installation of P4000S and P4000M Chassis EMI Bracket Cover 24
Figure 18. Installation of P4000L Chassis EMI Bracket Cover 25
Figure 19: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module 25
Figure 20: Mounting the Intel® Dedicated Server Management NIC Module to the PCI Slot Bracket 26
Figure 21: Adding the Intel® Dedicated Server Management NIC Module on a Third-party Chassis 26
Figure 22: Server Management – BMC LAN Configuration on S1200BTL 29
Figure 23: Server Management – BMC LAN Configuration on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 and S1200V3RP Product Families 31
Figure 24: IDA Configure Server: Communication Options Window 32
Figure 25: IDA Configure Server: Communication Options Window No Intel® Dedicated Server Management NIC Installed 33
Figure 26: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) IP Address from a DHCP Server Window 34
Figure 27: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) Static IP Address Window 35
Figure 28: IDA Configure Server: Set Up Users Window 36
Figure 29: IDA Configure Server: Edit User Information Window 37

Figure 30: IDA Configure Server: Apply Configuration Window 38
Figure 31: IDA Configure Server: Applying Configuration Progress Window 39
Figure 32: IDA Configure Server: Restart Server 40
Figure 33: Internet Explorer 8* Displaying Encryption Key Length 42
Figure 34: Intel® Integrated BMC Web Console Login Page 43
Figure 35: Integrated BMC Web Console Home Page 44
Figure 36: Launching the Online Help 46
Figure 37: Logging Out of Integrated BMC Web Console – Step 1 47
Figure 38: Logging Out of Integrated BMC Web Console – Step 2 47
Figure 39: Remote Control Console Redirection Page 48
Figure 40: Remote Console 49
Figure 41: Remote Console Main Window 50
Figure 42: Remote Console Control Bar 51
Figure 43: Remote Console Video Menu 51
Figure 44: Remote Console Keyboard Menu 52
Figure 45: Remote Console Keyboard Language Sub Menu 52
Figure 46: Remote Console Keyboard Soft Keyboard Sub Menu 54
Figure 47: Remote KVM Soft Keyboard 54
Figure 48: Remote Console Mouse Menu 55
Figure 49: Remote Console Mouse Menu on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 55
Figure 50: Remote Console Mouse Menu – Mode Selection on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 55
Figure 51: Remote Console Options Menu 56
Figure 52: Remote Console Device Menu 57
Figure 53: Status Line 58
Figure 54: Busy Indicator Bar 59
Figure 55: System Information Page on S1200BTL Platforms 60
Figure 56: System Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 61
Figure 57: System Information Page on S1200V3RP Product Family 62
Figure 58: System Information FRU Information Page 63
Figure 59: System Information System Debug Log Page on S1200BTL Platforms 64
Figure 60: System Information System Debug Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 66
Figure 61: System Information DIMM Information Page 68
Figure 62: System Information CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 69
Figure 63: Current Users Page on S1200V3RP Product Family 70
Figure 64: Server Health Sensor Readings Page (Thresholds not Displayed) 71
Figure 65: Server Health Sensor Readings Page (Thresholds Displayed) 72
Figure 66: Server Health Event Log Page on S1200BTL Platforms 73
Figure 67: Server Health Event Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 74

Figure 68: Server Health Event Log Page on S1200V3RP Product Family 75
Figure 69: Server Health Power Statistics Page on S1200BTL Platforms and S1200V3RP Product Family..... 76
Figure 70: Server Health Power Statistic Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 77
Figure 71: Configuration Network Settings Page on S1200BTL Platforms..... 78
Figure 72: Configuration IPv4 Network Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family . 79
Figure 73: Configuration IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family..... 81
Figure 74: Configuration User List Page 83
Figure 75: Configuration Users Add User Page 84
Figure 76: Configuration Users Modify User Page 84
Figure 77: Configuration Login Security Settings Page on S1200BTL Platforms 85
Figure 78: Configuration Login Security Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family . 86
Figure 79: Configuration LDAP Settings Page 87
Figure 80: Configuration VLAN Settings on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family..... 88
Figure 81: Configuration SSL Upload Page 90
Figure 82: Configuration Remote Session Page on S1200BTL Platforms 91
Figure 83: Configuration Remote Session Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 92
Figure 84: Configuration Remote Session Page on S1200V3RP Product Family..... 94
Figure 85: Configuration Mouse Mode Setting Page on S1200BTL Platforms..... 96
Figure 86: Configuration Mouse Mode Setting Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family . 97
Figure 87: KVM Window with Mouse Other Mode Selected on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family..... 98
Figure 88: Configuration Keyboard Macros Page 99
Figure 89: Configuration Alerts Page on S1200BTL Platforms..... 101
Figure 90: Configuration Alerts Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family..... 102
Figure 91: Configuration Alert Email Page 103
Figure 92: Configuration Node Manager Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 104
Figure 93: Configuration Node Manager Page with Use Policy Suspend Period Selected 106
Figure 94: Remote Control Console Redirection Page 107
Figure 95: Remote Control Server Power Control Page on S1200BTL Platforms..... 108
Figure 96: Remote Control Server Power Control Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 109
Figure 97: Remote Control Server Power Control Page on S1200V3RP Product Family 110
Figure 98: Remote Control Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family 112

List of Tables

Table 1: Terminology 1
Table 2: Intel® Server Boards RMM4 Lite Connector Locations 11
Table 3: Intel® Rack Server Systems – Intel® Dedicated Server Management NIC Connector Locations 12
Table 4: Intel® Multi Node Server Systems 20
Table 5: Intel® Rack Optimized Server Systems 20
Table 6: Intel® Pedestal Server Systems – Chassis Mounted Intel® Dedicated Server Management NIC Connector Locations 21
Table 7: Intel® Pedestal Server Systems with Chassis Mounted Intel® Dedicated Server Management NIC – Installation of EMI Bracket Cover 24
Table 8: Intel® Server Boards RMM4 NIC Connectors 27
Table 9: Integrated BMC Web Console Home Page Tabs 44
Table 10: Horizontal Toolbar Buttons 45
Table 11: System Information Details 60
Table 12: Server Health Sensor Readings Options 72
Table 13: Server Health Event Log Options on S1200BTL Platforms 73
Table 14: Configuration IPv4 Network Settings Options 79
Table 15: Configuration IPv6 Network Settings Options 82
Table 16: Configuration LDAP Settings Options 87
Table 17: Configuration VLAN Settings Options 88
Table 18: Configuration Remote Session Options 91
Table 19: Configuration Remote Session Options 93
Table 20: Configuration Remote Session Options on S1200V3RP Product Family 94
Table 21: Macro Non-printable Key Names 100
Table 22: Configuration Alerts Options 101
Table 23: Configuration Alert Email Options 103
Table 24: Configuration Node Manager Options 104
Table 25: Remote Control Power Control Options on S1200BTL Platforms 108
Table 26: Remote Control Power Control Options on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families 109
Table 27: Remote Control Power Control Options on S1200V3RP Product Family 110
Table 28: Remote Control Virtual Front Panel Options 112

<This page is intentionally left blank.>

1. Introduction

This User Guide describes how to use the Intel® Remote Management Module 4 (hereinafter referred to as Intel® RMM4) and the Integrated BMC Web Console. It provides an overview of the features of the Web Console and the RMM4 module along with instructions on how to set up and operate the Intel® RMM4.

The Intel® Integrated BMC Web Console provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, you can use the Intel® Integrated BMC Web Console to gain location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

Designed to work with the Baseboard Management Controller (BMC), the Intel® RMM4 is a small form-factor mezzanine card that enables remote KVM (Keyboard, Video, and Mouse) and media redirection on your server system, from the built-in Web Console, from anywhere, at any time.

1.1 Target Audience

This User Guide is intended for system technicians who are responsible for monitoring their server systems with the Intel® Integrated BMC Web Console. As a system administrator, you can use the Intel® Integrated BMC Web Console to gain location-independent remote access to respond to critical incidents. You can use the Intel® RMM4 to install, update, and monitor your operating system.

1.2 Terminology

The following table lists the terminology used in this document and the description.

Table 1: Terminology

Word/Acronym	Definition
ARP	Address Resolution Protocol
BMC	Baseboard Management Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ICMP	Internet Control Message Protocol
Intel® ASMI	Intel® Advanced Server Management Interface
Intel® RMM4	Intel® Remote Management Module 4
IPMI	Intelligent Platform Management Interface
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Controller
MII	Media Independent Interface
NIC	Network Interface Controller

Word/Acronym	Definition
OOB	Out Of Band – No operating system interaction on Server
SDR	Sensor Data Record
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol

1.3 Safety Information

WARNING

Before working with your Intel® RMM4 server product – whether you are using this guide or any other resource as a reference – pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described regulated components specified in this guide. Use of other products/components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in the region(s) in which the product is sold.

WARNINGS

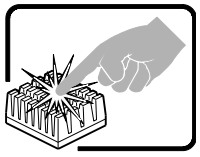
- **System power on/off**: The server power button DOES NOT turn off the system power or Intel® RMM4 power. To remove power from the Intel® RMM4 you must unplug the server AC power cord from the wall outlet. Make sure the AC power cord is unplugged before you open the chassis to add or remove the Intel® RMM4.
- **Hazardous conditions, devices and cables:** Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it. Otherwise, personal injury or equipment damage can result.
- **Electrostatic discharge (ESD) and ESD protection:** ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground—any unpainted metal surface—on your server when handling parts.
- **ESD and handling boards:** Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.
- **Installing or removing jumpers:** A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle nosed pliers. If your jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tools you use to remove a jumper, or you may bend or break the pins on the board.

⚠ Safety Cautions

Read all caution and safety statements in this document before performing any of the instructions. See also *Intel® Server Boards and Server Chassis Safety Information* at http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

SAFETY STEPS: Whenever you remove the chassis covers to access the inside of the system, follow these steps:

1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.
6. Do not operate the system with the chassis covers removed.



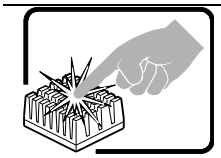
A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

⚠ Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warn- und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die Sicherheitshinweise zu Intel®-Serverplatinen und -Servergehäusen auf der Ressourcen-CD oder unter http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

SICHERHEISMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten:

1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.
2. Schalten Sie das System mit dem Hauptschalter aus.
3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.
4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab.
5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden.
6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.



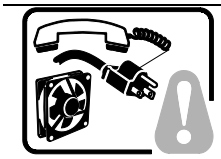
Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

⚠ 重要安全指导

在执行任何指令之前，请阅读本文档中的所有注意事项及安全声明。参见 Resource CD（资源光盘） 和/或 http://www.intel.com/support/motherboards/server/sb/cs-010770.htm 上的 *Intel® Server Boards and Server Chassis Safety Information*（《Intel® 服务器主板与服务器机箱安全信息》）。

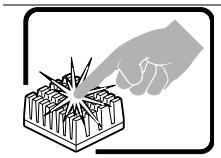
⚠ Consignes de sécurité

Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction. Consultez *Intel® Server Boards and Server Chassis Safety Information* sur le CD Resource CD ou bien rendez-vous sur le site http://www.intel.com/support/motherboards/server/sb/cs-010770.htm



CONSIGNES DE SÉCURITÉ -Lorsque vous ouvrez le boîtier pour accéder à l'intérieur du système, suivez les consignes suivantes:

1. Mettez hors tension tous les périphériques connectés au système.
2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).
3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.
4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système.
5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez une bande antistatique pour poignet et reliez-la à la masse du système (toute surface métallique non peinte du boîtier).
6. Ne faites pas fonctionner le système tandis que le boîtier est ouvert.



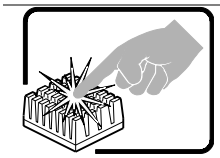
Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.

⚠ Instrucciones de seguridad importantes

Lea todas las declaraciones de seguridad y precaución de este documento antes de realizar cualquiera de las instrucciones. Vea *Intel® Server Boards and Server Chassis Safety Information* en el CD Resource y/o en http://www.intel.com/support/motherboards/server/sb/cs-010770.htm.

INSTRUCCIONES DE SEGURIDAD: Cuando extraiga la tapa del chasis para acceder al interior del sistema, siga las siguientes instrucciones:

1. Apague todos los dispositivos periféricos conectados al sistema.
2. Apague el sistema presionando el interruptor encendido/apagado.
3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna.
4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema.
5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujetada a la toma de tierra del chasis — o a cualquier tipo de superficie de metal sin pintar.
6. No ponga en marcha el sistema si se han extraído las tapas del chasis.

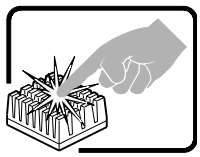


Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

⚠ AVVERTENZA: Italiano

PASSI DI SICUREZZA: Qualora si rimuovano le coperture del telaio per accedere all'interno del sistema, seguire i seguenti passi:

1. Spegnere tutti i dispositivi periferici collegati al sistema.
2. Spegnere il sistema, usando il pulsante spento/acceso dell'interruttore del sistema.
3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche.
4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema.
5. Qualora si tocchino i componenti, proteggersi dallo scarico elettrostatico (SES), portando un cinghia anti-statica da polso che è attaccata alla presa a terra del telaio del sistema – qualsiasi superficie non dipinta – .
6. Non far operare il sistema quando il telaio è senza le coperture.



Se il sistema è stato a lungo in funzione, il microprocessore e il dissipatore di calore potrebbero essere surriscaldati. Fare attenzione alla presenza di piedini appuntiti e parti taglienti sulle schede e sul telaio. È consigliabile l'uso di guanti di protezione.

1.4 Support Information

If you encounter an issue with your Intel® RMM4, follow these steps to obtain support:

1. Visit the following Intel Support website at http://www.intel.com/p/en_US/support. This web page provides 24x7 support when you need to get the latest and most complete technical support information on all Intel® Enterprise Server and Storage Platforms. Information available at the support site includes:

   - Latest BIOS, firmware, drivers, and utilities.
   - Product documentation, installation and *Quick Start Guides*.
   - Full product specifications, technical advisories, and errata.
   - Compatibility documentation for memory, hardware add-in cards, chassis support matrix, and operating systems.
   - Server and chassis accessory parts list for ordering upgrades or spare parts.
   - A searchable knowledgebase to search for product information throughout the support site.
2. If you are still unable to obtain a solution for your issue, you can contact Intel customer support at the following website: http://www.intel.com/support/feedback.htm.

1.5 Warranty Information

To obtain warranty information, visit the following Intel website:
http://www.intel.com/support/motherboards/server/sb/CS-010807.htm.

2. Intel® Remote Management Module 4 Overview

This section gives you an overview of the Intel® RMM4 and highlights significant benefits of its features.

2.1 Intel® RMM4 Lite and Intel® Dedicated Server Management NIC

The Intel® RMM4 is comprised of up to two boards – Intel® RMM4 Lite and the optional Intel® Dedicated Server Management NIC (DMN).

The Intel® RMM4 Lite is a small board that unlocks advanced management features on the RGMII interface when installed on Intel® Server Boards. It provides an increased level of manageability over the basic server management available to the server board. It works as an integrated solution on your server system.

After the Intel® RMM4 Lite has been installed, the advanced management features are available through both the optional Intel® Dedicated Server Management NIC, if installed, and all of the on-board Integrated BMC-shared NIC ports.

If the optional Intel® Dedicated Server Management NIC is installed, the NIC is dedicated to the Intel® RMM4 advanced management features traffic along with all other standard server management traffic. The host system is unaware of this NIC.

If the optional Intel® Dedicated Server Management NIC is not used, the traffic can go through any of the on-board Integrated BMC-shared NIC ports and will share network bandwidth with the host system.

Figure 1: Intel® RMM4 Lite

Figure 2: Intel® Dedicated Server Management NIC

2.2 Intel® RMM4 Features

The Intel® RMM4 add-on offers convenient, remote KVM access and control through LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs in the Integrated Baseboard Management Controller, utilizing expanded capabilities enabled by the Intel® RMM4 hardware.

Key features of the Intel® RMM4 add-on card are:

- KVM redirection from either the RMM4 NIC or the baseboard NIC used for management traffic; up to two simultaneous KVM sessions.
- Media redirection – The media redirection feature is intended to allow system administrators or users to mount a remote IDE or USB CD-ROM, floppy drive, or a USB flash disk as a remote device to the server. After mounted, the remote device appears just like a local device to the server, allowing system administrators or users to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device.
- KVM – Automatically senses video resolution for best possible screen capture, high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup.

2.3 Supported Operating Systems and Internet Browsers

The Intel® RMM4 enabled features run independently of the host operating system on the server where it is installed except during Remote Console (KVM) connections. During Remote Console connections the keyboard, video, and mouse of the console system operate just as if you were at the server where the Intel® RMM4 is connected. During Remote Console connections, the interaction with the host operating system limits the support to operating systems that have been validated. Those operating systems are listed in the following sub sections.

2.3.1 Server System

The following operating systems are supported on the managed server:

- Microsoft Windows Server 2008* R2 SP1
- Microsoft Windows Server 2008* SP2
- Red Hat* Enterprise Linux 6.2
- SUSE* Enterprise Linux 11 SP2
- Microsoft Windows 7* SP1
- Red Hat* Enterprise Linux 5 Update 7

2.3.2 Client System

The following client Internet browsers have been tested:

- Microsoft Internet Explorer 8.0*
- Microsoft Internet Explorer 9.0*
- Microsoft Internet Explorer 10.0*
- Mozilla Firefox* 3.0
- Mozilla Firefox* 3.5
- Mozilla Firefox* 3.6
- Mozilla Firefox* 10 (on Microsoft Windows* operating systems)

3. Hardware Installations and Initial Configuration

This section guides you on the hardware installations and initial configuration.

3.1 Before You Begin

Carefully read the Safety Information provided at the beginning of this manual before working with your server product.

3.2 Tools and Supplies Needed

Following are the tools and supplies needed:

- Phillips (cross head) screwdriver (#1 bit and #2 bit)
- Needle nosed pliers
- Antistatic wrist strap and conductive foam pad (recommended)

3.3 Installation

The Intel® RMM4 has multiple packages:

- RMM4 Lite edition (AXXRMM4Lite), which contains the following components:
  - Intel® Remote Management Module 4 Lite module
- RMM4 full edition (AXXRMM4), which contains the following components:
  - Intel® Remote Management Module 4 Lite module
  - Intel® Dedicated Server Management Network Interface Card (NIC) module
  - Bag containing screws, metal fastening bracket, PCI slot brackets, and cablings
  - EMI bracket covers and thumb screws
- RMM4 full edition 2 (AXXRMM4R) for Intel® Server Boards S2600GZ, S2600GL, S2400BB, S2400EP, and S1400SP, which contains the following components:
  - Intel® Remote Management Module 4 Lite module
  - Intel® Dedicated Server Management Network Interface Card (NIC) module 2
  - Bag containing screws
- RMM4 Multi Node editions (**Note**: For advanced management features functionality, these also require the AXXRMM4LITE to be added)
  - AXXRMM4IOM (Intel® HNS2600JF and Intel® HNS2400LP Compute Module Family) for Intel® Server Boards S2600JF and S2400LP
  - AXXRMM4IOMW (Intel® HNS2600WP Compute Module Family) for Intel® Server Boards S2600WP
  - Each of these contains the following components:
    - A PCI Express* rIOM riser
    - A rIOM carrier board to provide a Dedicated RMM4 NIC port and a connector supporting the Intel® I/O modules
    - Associated mounting hardware (screws, standoff, and brackets)
- RMM4 Rack Optimized edition (A1UJPRMM4IOM) for Intel® Server Boards S1600JP which contains the following components (**Note**: For advanced management features functionality, this also requires the AXXRMM4LITE to be added):
  - A PCI Express* rIOM riser
  - A rIOM carrier board to provide a Dedicated RMM4 NIC port and a connector supporting the Intel® I/O modules

- Associated mounting hardware (screws, standoff, and brackets)

The installation will vary between the chassis configurations. The following sections provide installation instructions.

Caution: Intel® RMM4 Lite and RMM4 DMN are NOT hot-swappable. Before removing or replacing them, you must follow these steps:

1. First take the server out of service.
2. Turn off the system by pressing the power button.
3. Unplug the AC power cord from the system or wall outlet.
4. Wait for at least 10 seconds before installing the module.

3.3.1 Installation of the Intel® RMM4 Lite on Intel® Server Boards

The following are steps for installing the Intel® RMM4 Lite on Intel® Server Boards and apply to all system types:

1. Ensure that AC power has been removed from the system and that you have waited at least 10 seconds after removing power.
2. Find the RMM4 Lite connector as specified in Table 2 for your specific server board. See your *Intel® Server Boards Technical Product Specification (TPS)* for details.
3. Carefully pick up the RMM4 Lite module. Verify the location of the RMM4 Lite connector key pin before inserting the RMM4 Lite into the mating connector on the Intel® Server Board.

Note: For more details see your specific *Intel® Server Systems Technical Product Specification* and *Intel® Server Systems Service Guide*.

Table 2: Intel® Server Boards RMM4 Lite Connector Locations

Intel® Server Board	RMM4 Lite Connector Reference Designator
S1200BTL	J4B1
S1200V3RPL S1200V3RPO S1200V3RPM	J4B1
S2400BB	J3A2
S1400FP	J3D1
S1400SP	J4D2
S1600JP2/S1600JP4	J6A2
S2400EP	J1E1
S2400GP	J2B3
S2400LP	J7F2
S2400SC	J3D1
S2600CO	J1B1
S2600CP	J1B2
S2600GZ/S2600GL	J3B2

Intel® Server Board	RMM4 Lite Connector Reference Designator
S2600IP	J2B1
S2600JF	J1A2
S2600WP	J1A2
S4600LH2/S4600LT2	J44
W2600CR	J2B1

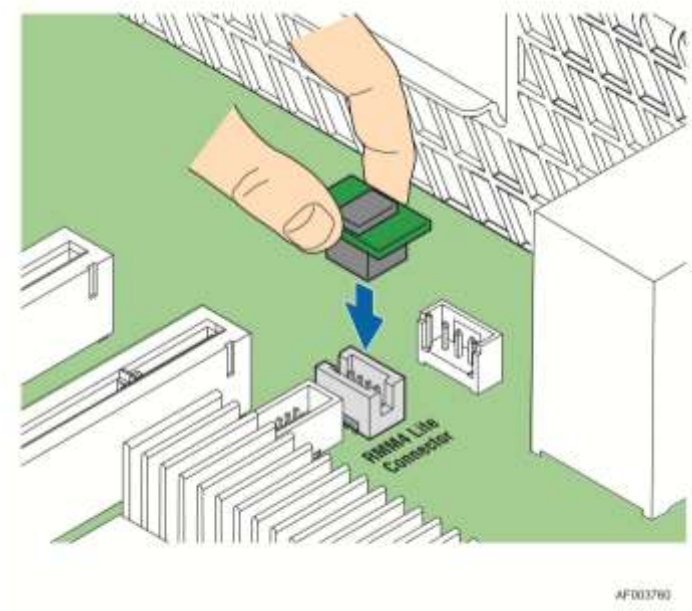


Figure 3: Installing the Intel® RMM4 Lite on Intel® Server Boards

3.3.2 Installation of the Intel® Dedicated Server Management NIC on an Intel® Rack Server System

Most Intel® Rack Server Systems allow the Intel® Dedicated Server Management NIC module to be mounted to the chassis. Table 3 lists all Intel® Rack Server Systems that support a chassis mounted Intel® Dedicated Server Management NIC module. Use the following steps when installing the Intel® Dedicated Server Management NIC module on those server systems:

Note: For the next steps see your specific *Intel® Server Systems Technical Product Specification* and *Intel® Server Systems Service Guide* for more details. Table 3 lists the section and figure describing the installation for that specific system.

Table 3: Intel® Rack Server Systems – Intel® Dedicated Server Management NIC Connector Locations

Intel® Server System	RMM4 NIC Connector Reference Designator	Cable and Bracket Required?	Section	Figure
R1000BTL Family	J5C1	Yes	3.3.2.1	Figure 6
R1000BB Family R2000BB Family	J3B2	No	3.3.2.2	Figure 9

Intel® Server System	RMM4 NIC Connector Reference Designator	Cable and Bracket Required?	Section	Figure
R1000EP Family	J2B1	No	3.3.2.3	Figure 10
R1000RP Family	J5C1	Yes	3.3.2.1	Figure 6
R1000SP Family	J3B2	No	3.3.2.2	Figure 9
R2000FP Family	J1D2	Yes (PCI slot bracket)	3.3.2.4	Figure 12
R2000IP Family	J3A1	Yes	3.3.2.1	Figure 7
R2000LH2/R200LT2	J53	No	3.3.2.1	Figure 8
R2000SC Family	J1C7	Yes (PCI slot bracket)	3.3.2.4	Figure 12
R1000GZ/GL Family R2000GZ/GL Family	J2A1	No	3.3.2.2	Figure 9

3.3.2.1 Installing the Dedicated NIC on Intel® Server System R1000BTL Family, R1000RP Family, R2000IP Family, or R2000LH2/R2000LT2

1. Ensure that AC power has been removed from the system and that you have waited at least 30 seconds after removing power.
2. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.

Caution: Carefully remove the metal cover with pliers; directly removing it with fingers has a potential risk.

3. Attach the metal fastening bracket to the Intel® Dedicated Server Management NIC module as shown in Figure 4.

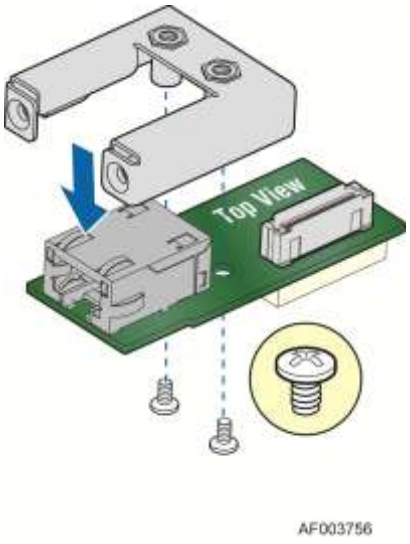


Figure 4: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module

4. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module as shown in Figure 5.

Caution: Take care when attaching or removing this cable. Mishandling the cable could cause damage.

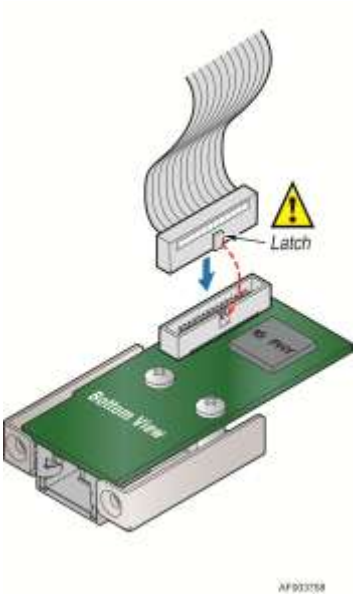


Figure 5: Attaching the Cable to the Intel® Dedicated Server Management NIC Module

5. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module. Mount the NIC module to the back of the chassis and secure the metal fastening bracket with two screws. This will align the RJ-45 with the opening in the chassis. Attach the cable to the RMM4 NIC connector, as specified in Table 3, on the server board.

Caution: Take care when attaching or removing this cable. Mishandling the cable could cause damage.

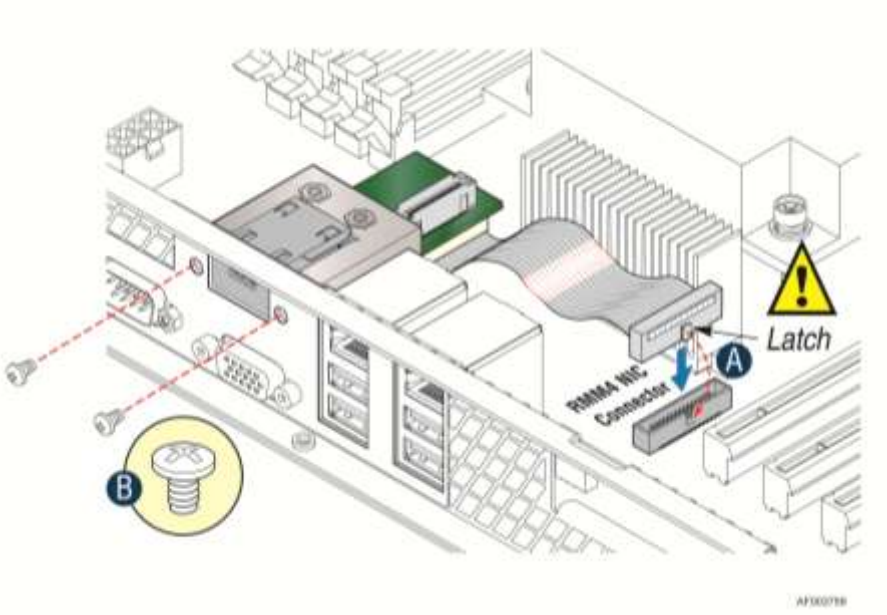


Figure 6: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000BTL and R1000RP Families

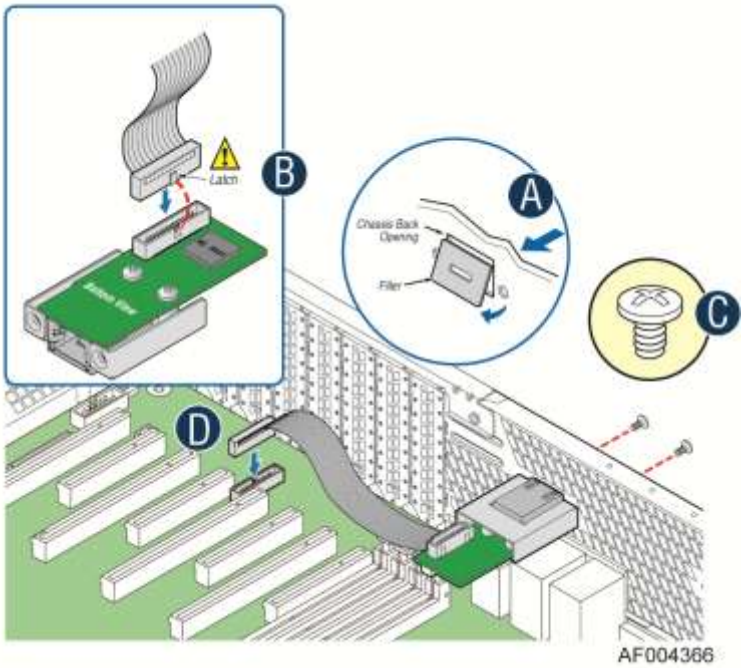


Figure 7: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000IP Family

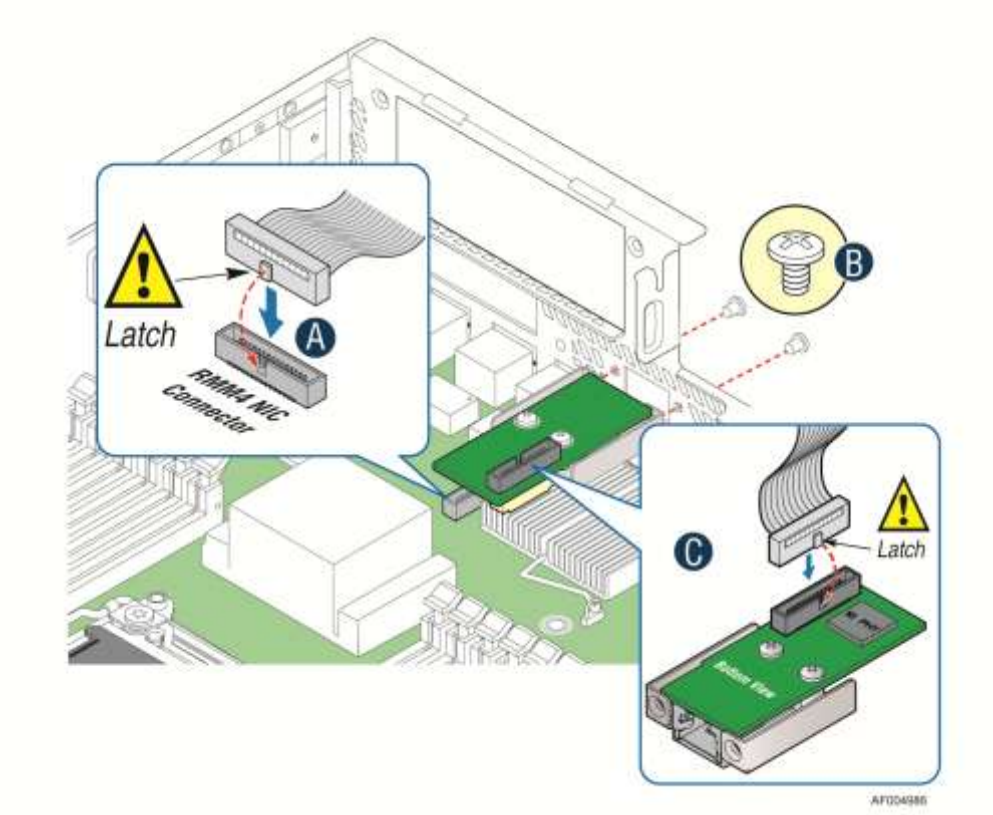


Figure 8: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000LH2/R200LT2

3.3.2.2 Installing the Dedicated NIC on Intel® Server System R1000BB and R2000BB Families, R1000SP Family, or R1000GZ/GL and R2000GZ/GL Families

1. Ensure that AC power has been removed from the system and that you have waited at least 30 seconds after removing power.
2. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.

Caution: Carefully remove the metal cover with pliers; directly removing it with fingers has a potential risk.

3. Mount the NIC module to the Intel® Server System board and secure it to the standoffs with two screws.

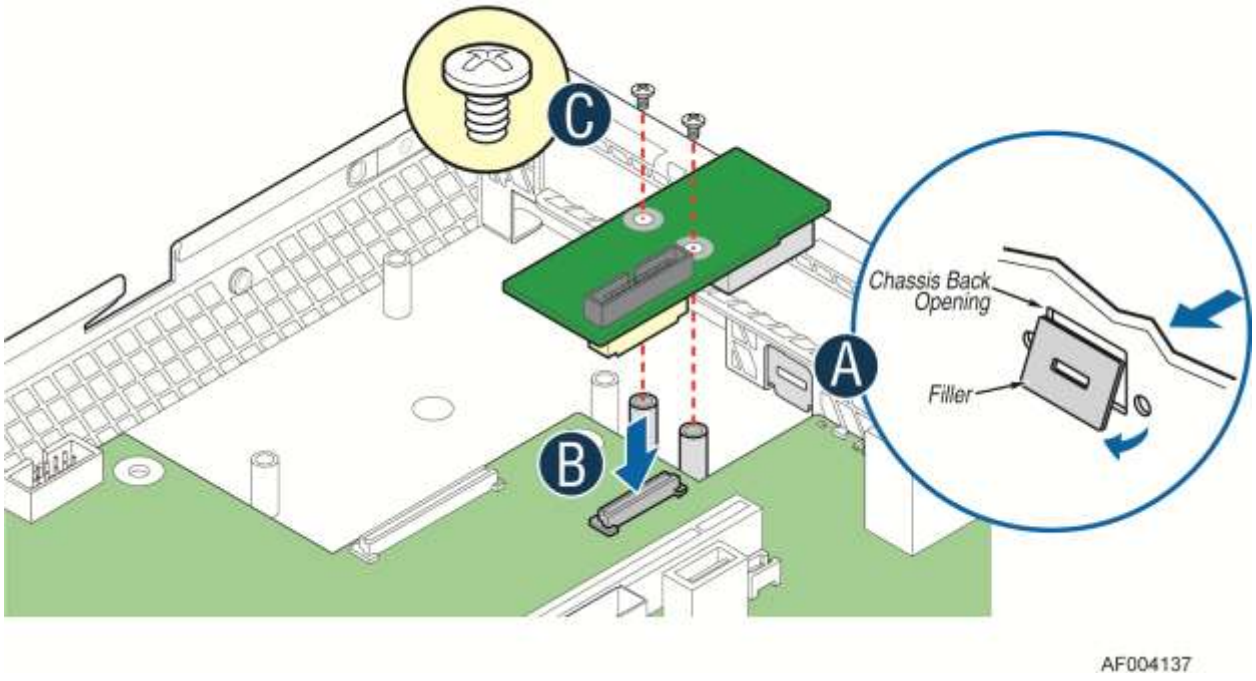


Figure 9: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000BB and R2000BB Families, R1000SP Family, or R1000GZ/GL and R2000GZ/GL Families

4. Replace the chassis cover, attach the AC power, and connect a network cable to the Intel® Dedicated Server Management NIC module.

3.3.2.3 Installing the Dedicated NIC on Intel® Server System R1000EP Family

1. Ensure that AC power has been removed from the system and that you have waited at least 30 seconds after removing power.
2. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.

Caution: Carefully remove the metal cover with pliers; directly removing it with fingers has a potential risk.

3. Insert and fit the metal adapter into the position as shown in Figure 10. Secure the adapter with two screws as shown (see letter **B**).
4. Position the module over the server board, fit the front of the module into the back panel slot, and then attach the module to the server board connector. Secure the module with the one screw as shown (see letter **C**).

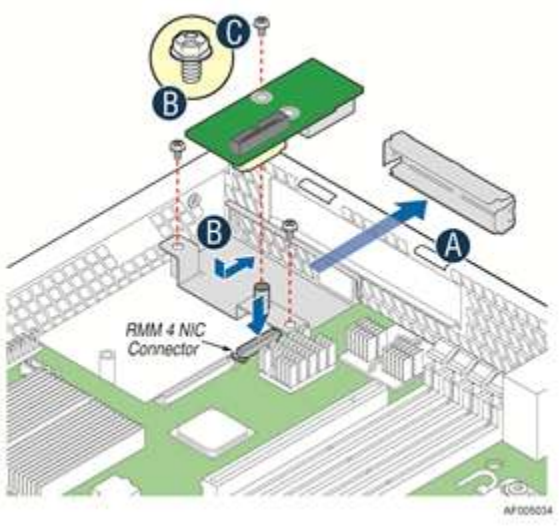


Figure 10: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System R1000EP Family

3.3.2.4 Installing the Dedicated NIC on Intel® Server System R2000FP Family or R2000SC Family

1. Ensure that AC power has been removed from the system and that you have waited at least 30 seconds after removing power.
2. Attach the metal fastening bracket to the Intel® Dedicated Server Management NIC module.

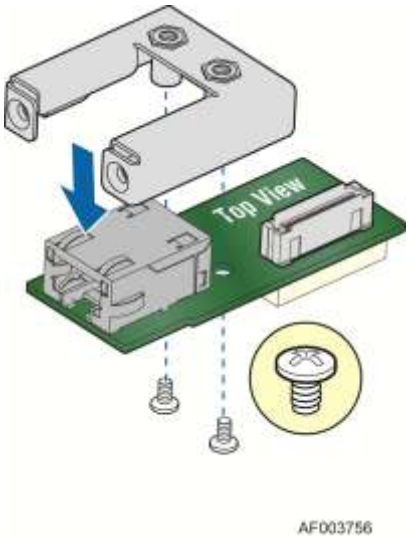


Figure 11: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module

3. Remove the Filler Panel and Retention Device. See **A** in Figure 12.
4. Secure the metal fastening bracket with the NIC module to the PCI slot bracket with two screws as shown in **B** of Figure 12. This will align the RJ-45 with the opening in the PCI slot bracket.
5. Fasten the bracket with one screw as shown in **C** of Figure 12.

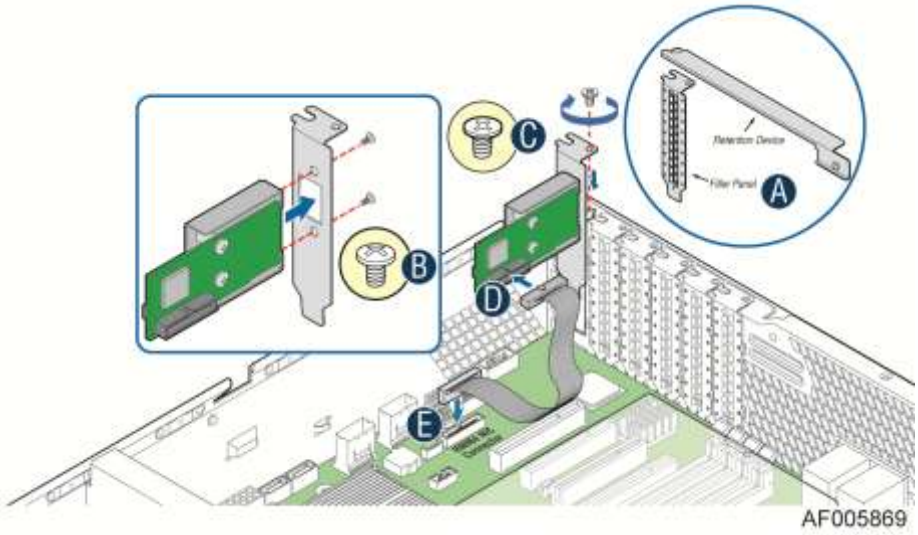


Figure 12: Installing the Intel® Dedicated Server Management NIC Module in the Intel® Server System R2000FP Family or R2000SC Family

6. Connect one end of the cable to the connector on the Intel® Dedicated Server Management NIC module as shown in **D** of Figure 12.
7. Connect the opposite end of the cable to the Intel® Dedicated Server Management NIC connector on the Server board as shown in **E** of Figure 12.

3.3.3 Installation of the Intel® Dedicated Server Management NIC on an Intel® Multi Node Server System

The Intel® Multi Node Server Systems have unique Intel® Dedicated Server Management NIC solutions. The NIC is located on the rIOM carrier modules. See your specific *Intel® Server System Technical Product Specification (TPS)* and *Server Guides* for details. These Intel® Multi Node Systems are listed in Table 4.

Table 4: Intel® Multi Node Server Systems

Intel® Server System
H2000JF
H2000LP
H2000WP

3.3.4 Installation of the Intel® Dedicated Server Management NIC on an Intel® Rack Optimized Server System

The Intel® Rack Optimized Server Systems have unique Intel® Dedicated Server Management NIC solutions. The NIC is located on the rIOM carrier modules. See your specific *Intel® Server System Technical Product Specification (TPS)* and *Server Guides* for details. These Intel® Rack Optimized Server Systems are listed in Table 5.

Table 5: Intel® Rack Optimized Server Systems

Intel® Server System
R1000JP

3.3.5 Installation of the Intel® Dedicated Server Management NIC on an Intel® Pedestal Server System

Most Intel® Pedestal Server Systems allow the Intel® Dedicated Server Management NIC module to be mounted to the chassis. Table 6 lists all Intel® Pedestal Server Systems that support a chassis mounted Intel® Dedicated Server Management NIC module. Use the following steps when installing the Intel® Dedicated Server Management NIC module on those server systems:

1. Ensure that AC power has been removed from the system and that you have waited at least 10 seconds after removing power.
2. Attach the metal fastening bracket to the Intel® Dedicated Server Management NIC module.

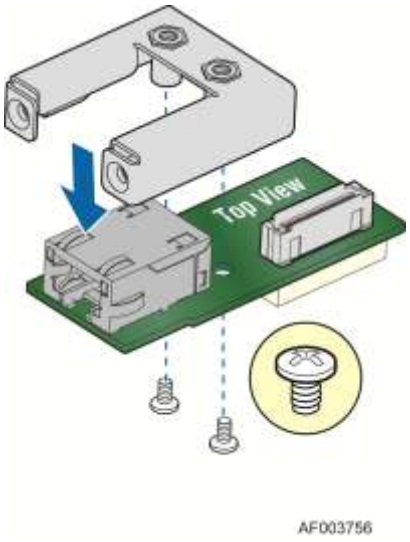


Figure 13: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module

Note: For the next two steps see your specific *Intel® Server Systems Technical Product Specification* and *Intel® Server Systems Service Guide* for more details. Table 6 lists the figure showing the installation for that specific system.

3. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.

Caution: Carefully remove the metal cover with pliers; directly removing it with fingers has a potential risk.

4. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module. Mount the NIC module to the back of the chassis and secure the metal fastening bracket with two screws. This will align the RJ-45 with the opening in the chassis. Attach the cable to the RMM4 NIC connector, as specified in Table 6, on the server board.

Caution: Take care when attaching or removing this cable. Mishandling the cable could cause damage.

Table 6: Intel® Pedestal Server Systems – Chassis Mounted Intel® Dedicated Server Management NIC Connector Locations

Intel® Server System	RMM4 NIC Connector Reference Designator	Figure
P4000BTL Family	J5C1	Figure 14
P4000CR Family	J3A1	Figure 16
P4000CP Family	J1C7	Figure 15
P4000FP Family	J1D2	Figure 15
P4000GP Family	J1B2	Figure 15
P4000IP Family	J3A1	Figure 16
P4000RP Family	J5C1	Figure 14

Intel® Server System	RMM4 NIC Connector Reference Designator	Figure
P4000SC Family	J1C7	Figure 15
S2400GP/P4000M Chassis	J1B2	Figure 15
S2400SC/P4000M Chassis	J1C7	Figure 14
S2600CO/P4000M Chassis	J1B3	Figure 15
S2600CP/P4000M Chassis	J1C1	Figure 15

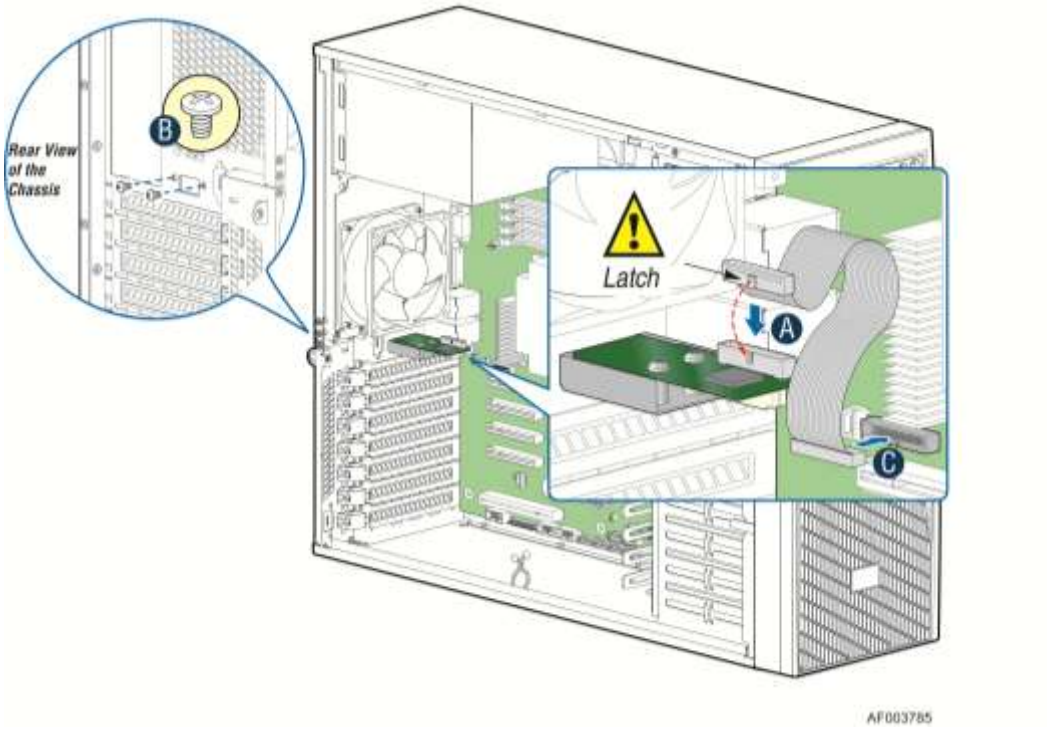


Figure 14: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000BTL and P4000RP Families

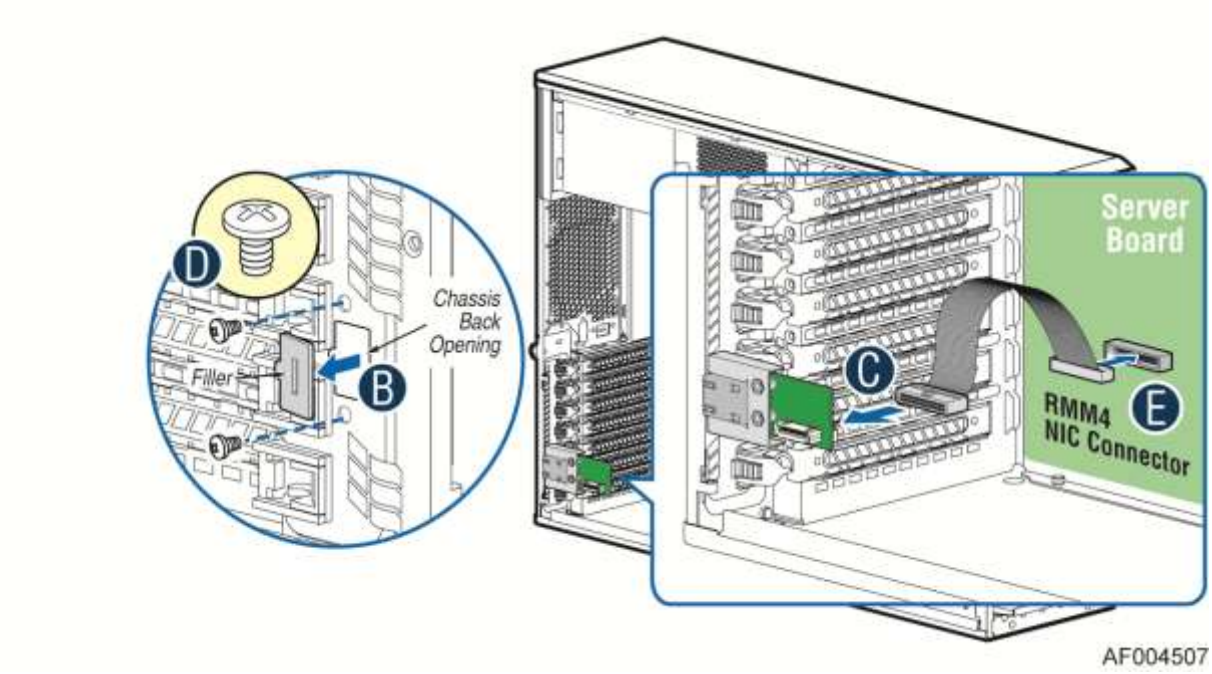


Figure 15: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000CP Family, P4000FP Family, P4000GP Family, P4000SC Family, or P4000M Chassis

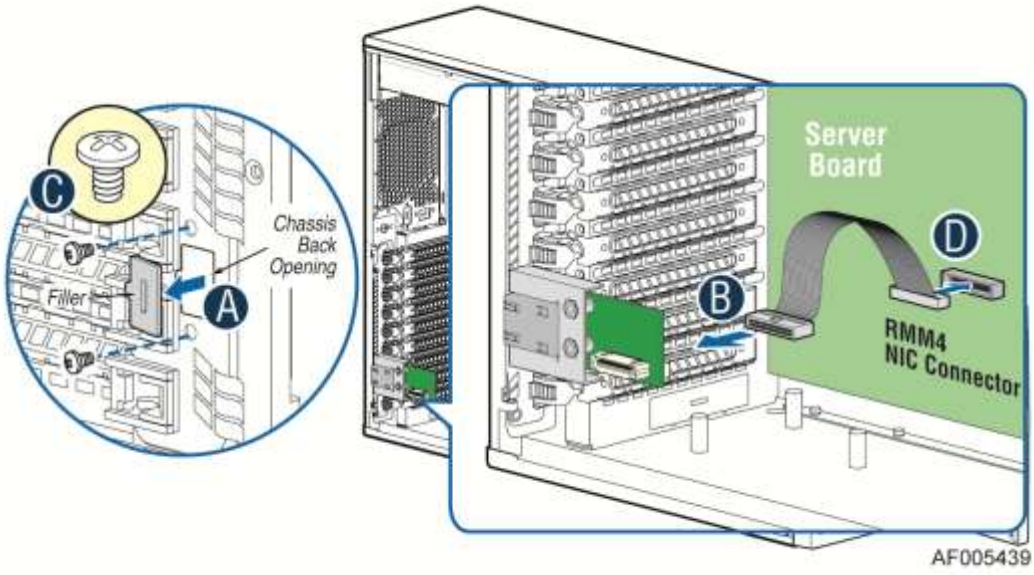


Figure 16: Adding the Intel® Dedicated Server Management NIC Module in the Intel® Server System P4000CR Family or P4000IP Family

5. Add the EMI bracket cover using the two thumb screws as shown in Figure 17 or Figure 18 per Table 7.

Table 7: Intel® Pedestal Server Systems with Chassis Mounted Intel® Dedicated Server Management NIC – Installation of EMI Bracket Cover

Intel® Server System	Figure
P4000BTL Family	Figure 17
P4000CR Family	Figure 18
P4000CP Family	Figure 17
P4000FP Family	Figure 17
P4000GP Family	Figure 17
P4000IP Family	Figure 18
P4000SC Family	Figure 17
P4000M Chassis	Figure 17
P4000S Chassis	Figure 17

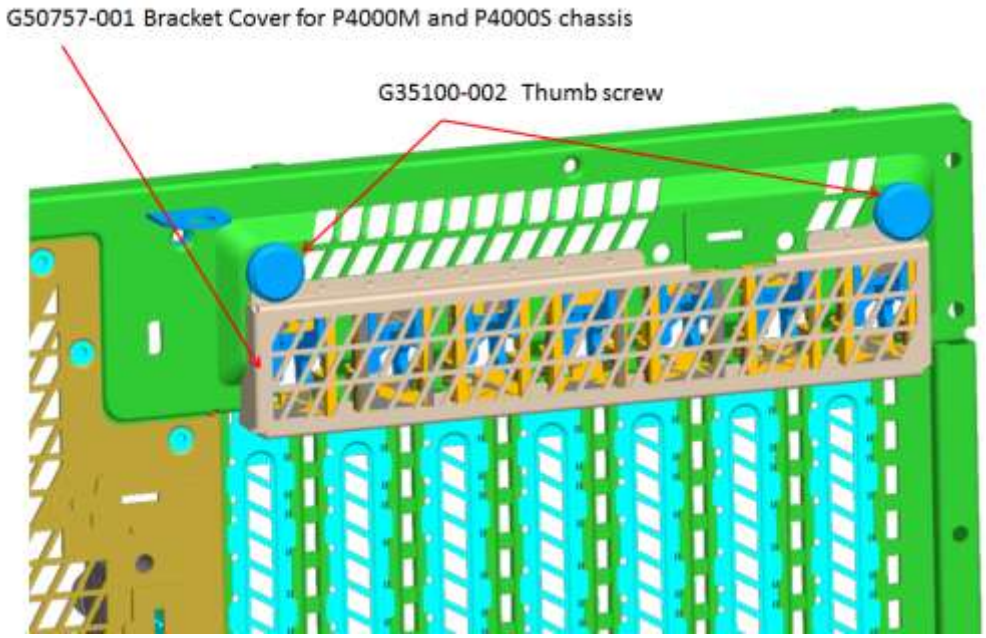


Figure 17. Installation of P4000S and P4000M Chassis EMI Bracket Cover

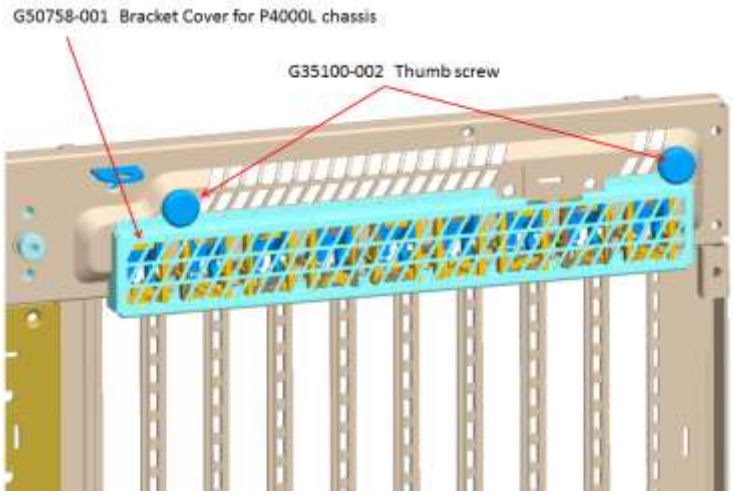


Figure 18. Installation of P4000L Chassis EMI Bracket Cover

6. Replace the chassis cover, attach the AC power, and connect a network cable to the Intel® Dedicated Server Management NIC module.

3.3.6 Installation of the Intel® Dedicated Server Management NIC on a Third-party Pedestal Chassis

Use the following steps when installing the Intel® Dedicated Server Management NIC module on a Third-party pedestal chassis:

1. Ensure that AC power has been removed from the system and that you have waited at least 10 seconds after removing power.
2. Attach the metal fastening bracket to the Intel® Dedicated Server Management NIC module.

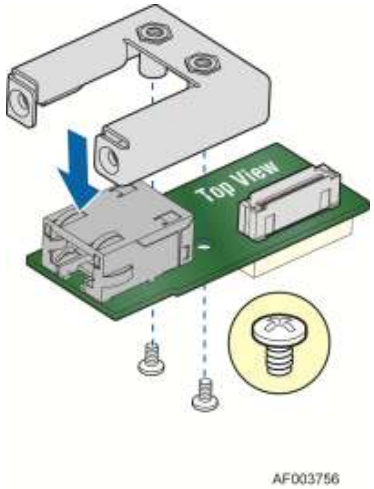


Figure 19: Attaching the Bracket to the Intel® Dedicated Server Management NIC Module

3. Secure the metal fastening bracket with the NIC module to the PCI slot bracket with two screws as shown in Figure 20. This will align the RJ-45 with the opening in the PCI slot

bracket.

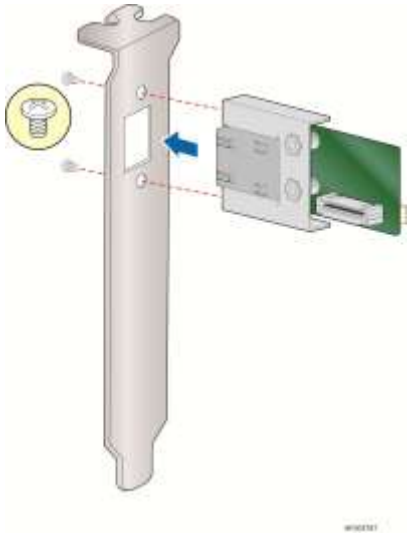


Figure 20: Mounting the Intel® Dedicated Server Management NIC Module to the PCI Slot Bracket

4. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module as shown in Figure 21 (**A**).
5. Mount the PCI slot bracket with the NIC module to the third-party chassis and secure the PCI slot bracket with the screw as shown in Figure 15 (**B**).
6. Attach the cable to the RMM4 NIC connector (J5C1) on the server board as shown in Figure 21 (**C**).

Caution: Take care when attaching or removing this cable. Mishandling the cable could cause damage.

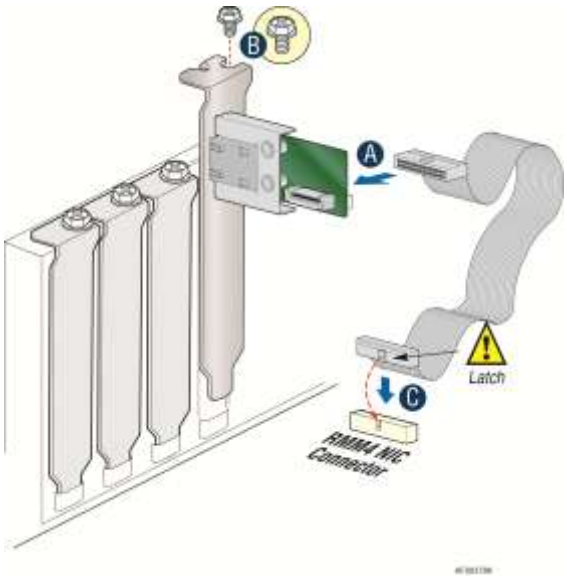


Figure 21: Adding the Intel® Dedicated Server Management NIC Module on a Third-party Chassis

Table 8: Intel® Server Boards RMM4 NIC Connectors

Intel® Server Board	RMM4 NIC Connector Reference Designator
S1200BTL	J5C1
S2400BB	J3B2
S1400FP	J1D2
S1400SP	J3B2
S2400EP	J2B1
S2400GP	J1B2
S2400SC	J1C7
S2600CO	J1B3
S2600CP	J1C1
S2600GZ/S2600GL	J2A1
S2600IP	J3A1
S4600LH2/S4600LT2	J53
W2600CR	J3A1

7. Replace the chassis cover.
8. Attach the AC power.
9. Connect a network cable to the Intel® Dedicated Server Management NIC module.

4. Configuring the Integrated BMC Web Console and Intel® RMM4

This section discusses using the Server Utilities to enable your system to use the Integrated BMC Web Console or the Intel® RMM4 from a new unconfigured state to an operational one.

When first powered on, by default, the Server Management BMC LAN and the Intel® RMM4 have a static IP address of 0.0.0.0.

The Server Management BMC LAN and the Intel® RMM4 can be configured in multiple ways:

- Using BIOS setup
- Using the Intel® Deployment Assistant (IDA)
- Using Sysconfig (SYSCFG)
- Using IPMI commands

Note: You can download the IDA and SYSCFG software from the following links:

- IDA – http://www.intel.com/p/en_US/support/highlights/server/ida – This is also available on the resource disk that is shipped with the server board.
- SYSCFG – http://downloadcenter.intel.com/default.aspx > relevant server platforms page

Two steps are necessary before Server Management BMC LAN or the Intel® RMM4 can be used:

1. One or both LAN channels must be configured as either DHCP or static addresses.
2. At least one user must be enabled to use the LAN channels.

4.1 Configuring the Server Management NIC using BIOS Setup on S1200BTL

1. During POST, press <F2> to go to BIOS setup.
2. Navigate to the **Server Management** tab and then scroll down to **BMC LAN Configuration**. Press <Enter>.
3. If configuring your Server Management BMC LAN, scroll to **IP source** > **IP source** and then select either Static or Dynamic.
4. If configuring your Intel® RMM4, scroll down to **Intel(R) RMM4 LAN configuration** > **IP source** and then select either Static or Dynamic.
5. If Static is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as required.
6. Scroll down to **User ID.** Select the user that you want to use.
7. Scroll down to **User status**. Select Enabled.
8. Scroll down to **User name**. Change the name as needed. Note that you cannot change anonymous or root.
9. Scroll down to **User password**. Change the password. Note that you need to enter the password twice.
10. When you finish configuring the LAN addresses and user information for the server, press <F10> and select save and exit. Your server will reboot with the new LAN settings.

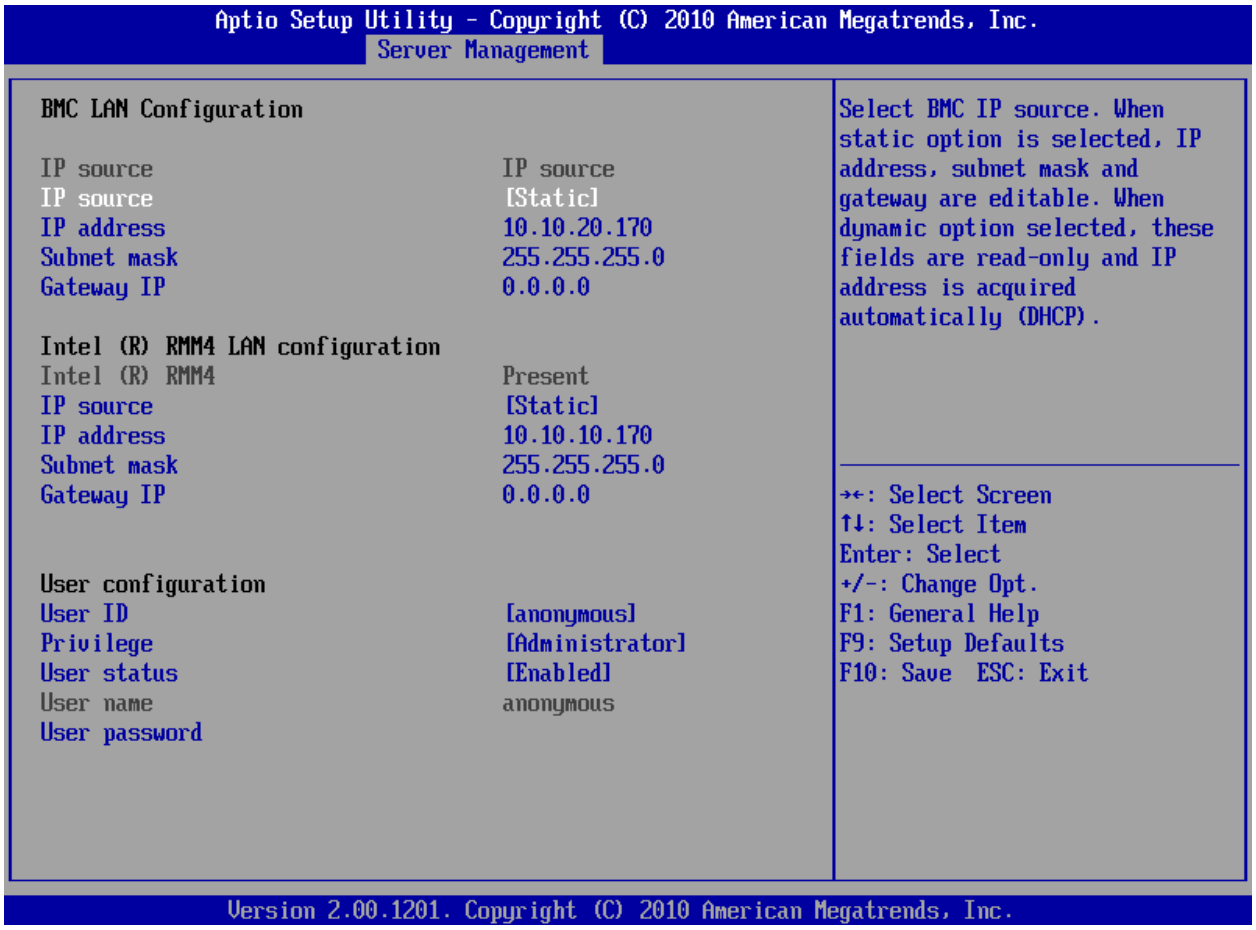


Figure 22: Server Management – BMC LAN Configuration on S1200BTL

4.2 Configuring the Server Management NIC using BIOS Setup on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 and S1200V3RP Product Families

1. During POST, press <F2> to go to BIOS setup.
2. Navigate to the **Server Management** tab and then scroll down to **BMC LAN Configuration**. Press <Enter>.
3. If you will be using an IPv4 network:
   a. If configuring your Server Management BMC LAN, scroll to **Baseboard LAN configuration** > **IP source** and then select either Static or Dynamic.
   b. If configuring your Intel® RMM4, scroll down to **Intel(R) RMM4 IPV4 LAN configuration** > **IP source** and then select either Static or Dynamic.
   c. If Static is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
4. If you will be using an IPv6 network:
   a. If configuring your Server Management BMC LAN, scroll to **Baseboard LAN IPv6 configuration** > **IP source** and then select Enabled.
      1. Scroll to **IPV6 source** and select either Static or Dynamic.
   b. If configuring your Intel® RMM4, scroll down to **Intel(R) RMM4 IPv6 LAN configuration** > **IP source** and then select either Static or Dynamic.
   c. If Static is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
5. Scroll down to **User ID.** Select the user that you want to use.
6. Scroll down to **User status**. Select Enabled.
7. Scroll down to **User name**. Change the name as needed. Note that you cannot change anonymous or root.
8. Scroll down to **User password**. Change the password. Note that you need to enter the password twice.
9. When you finish configuring the LAN addresses and user information for the server, press <F10> and select save and exit. Your server will reboot with the new LAN settings.

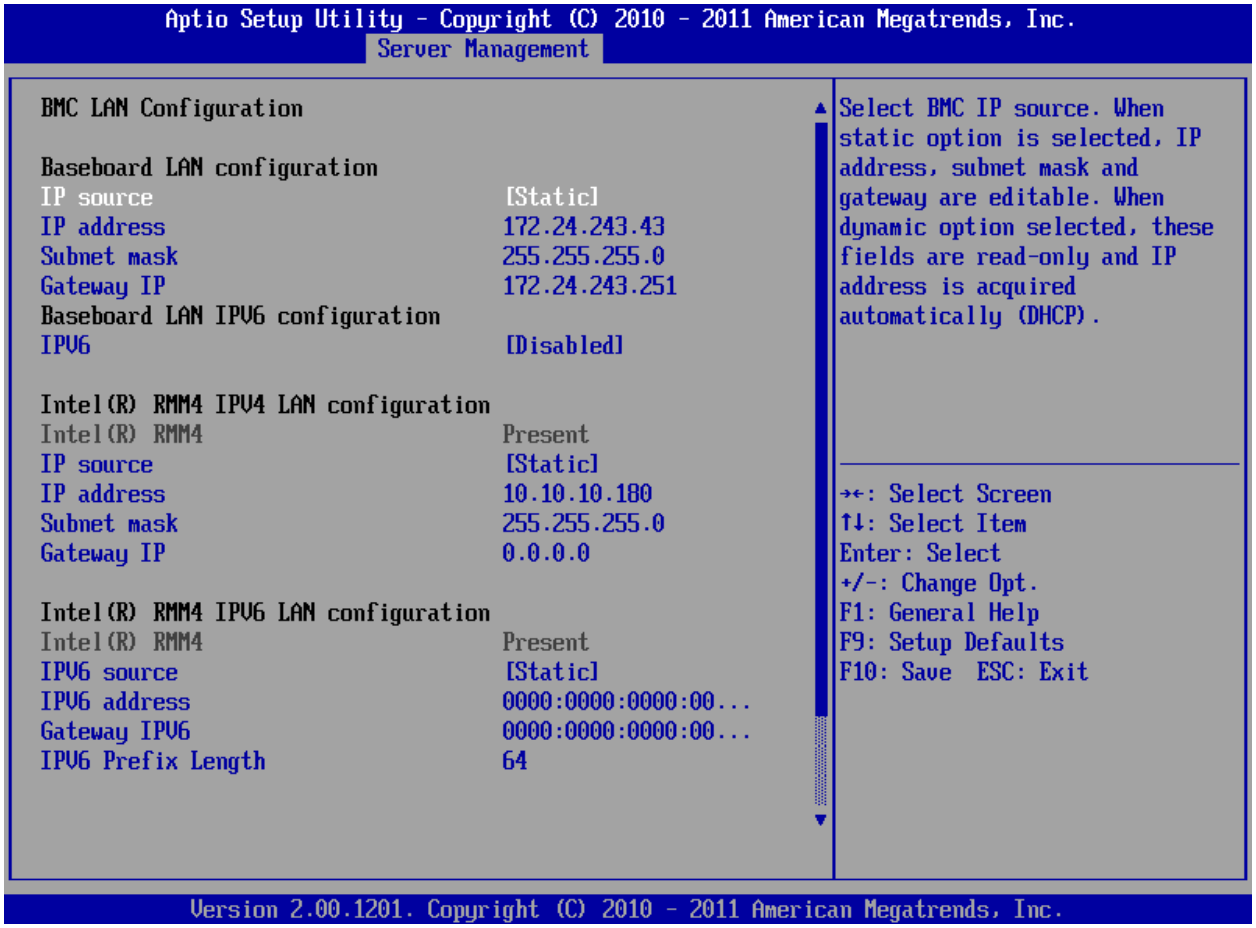


Figure 23: Server Management – BMC LAN Configuration on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 and S1200V3RP Product Families

4.3 Configuring the Server Management NIC using the Intel® Deployment Assistant (IDA)

The following section explains how to use the IDA to configure the on-board NIC1 and/or the RMM4 NIC for use with the Integrated BMC Web Console and the Intel® RMM4. The example shows how to configure LAN Channel 3 (Intel® RMM4 NIC).

⚠ WARNING

If you need to configure both LAN Channel 1 and LAN channel 3 (Intel® Dedicated Server Management NIC), ensure that they are configured with different subnets.

Note: When the Intel® Dedicated Server Management NIC is not installed, because the RMM4 Lite has no dedicated NIC, the LAN Channel 3 is not displayed. The user can access the RMM4 Lite advance features from LAN channel 1 (on-board NIC1). See Figure 25.

1. Select the channel to be configured.

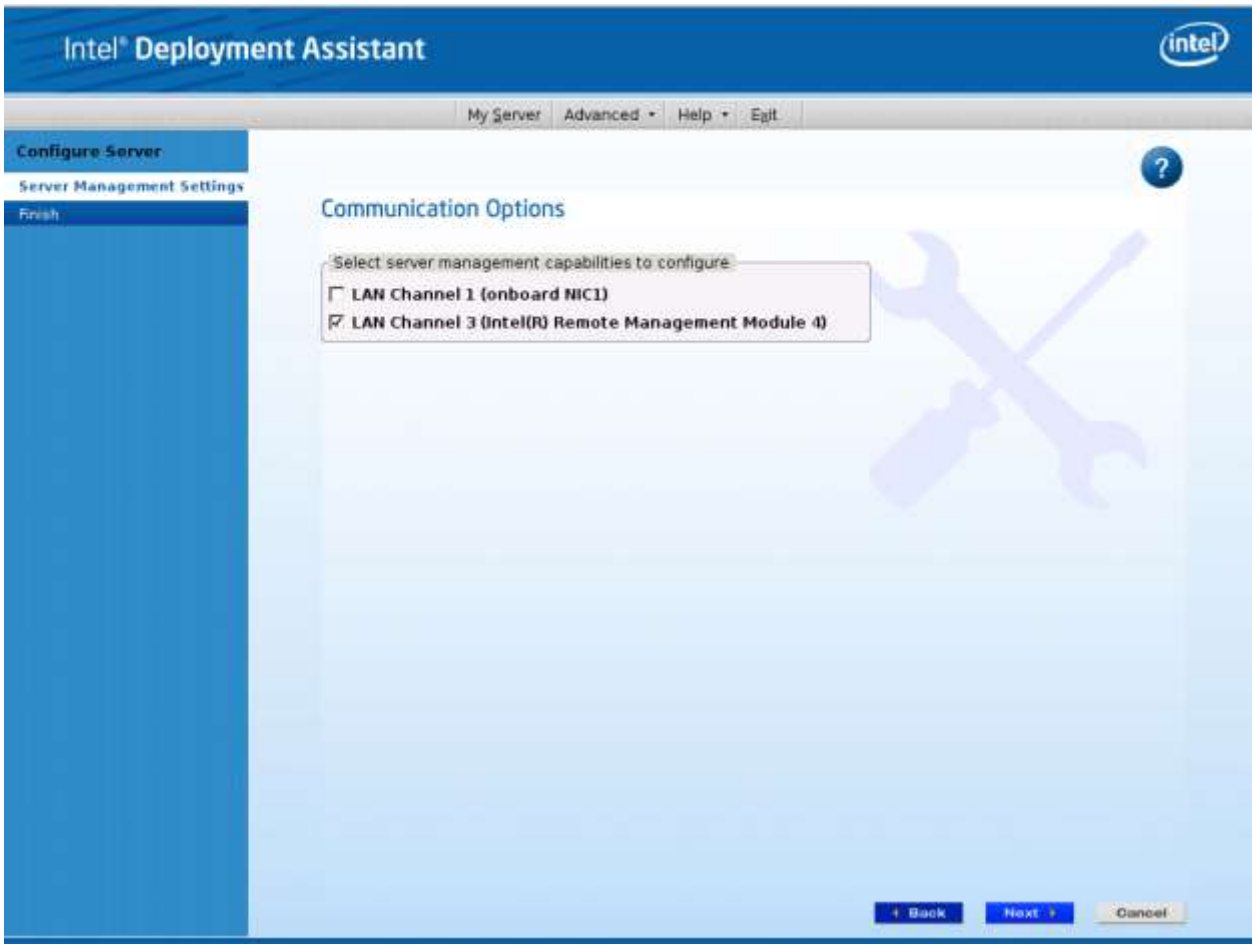


Figure 24: IDA Configure Server: Communication Options Window

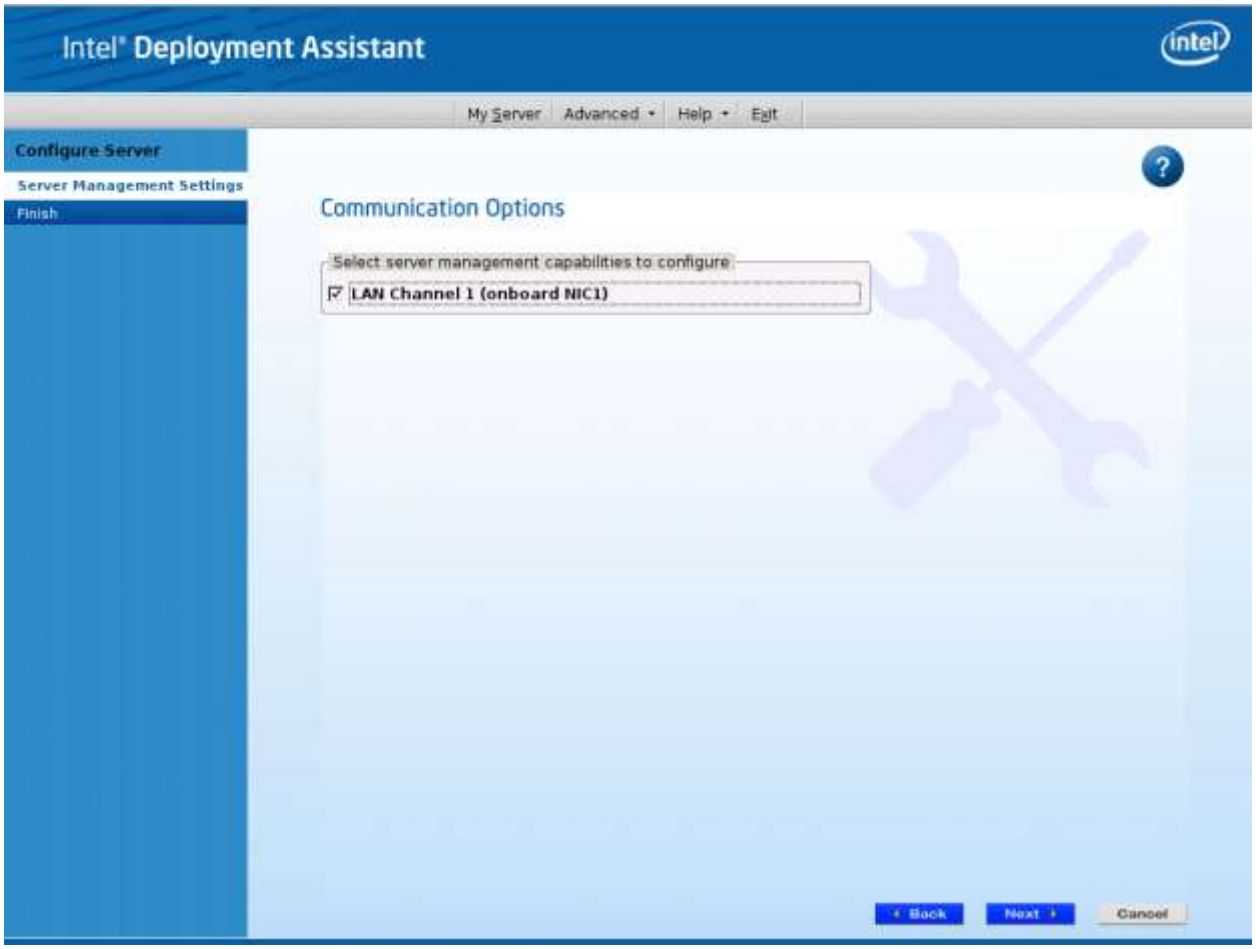


Figure 25: IDA Configure Server: Communication Options Window
No Intel® Dedicated Server Management NIC Installed

2. Select **IP Address from a DHCP server** or **Static IP Address**:
   a. If **IP Address from a DHCP server** is selected, configure the **DHCP Host Name** as shown in Figure 26.
   b. If **Static IP Address** is selected, configure the **IP address**, **Subnet Mask**, and **Gateway** as shown in Figure 27.
3. You can also select **Enable Serial Over LAN** and **Configure Alert** on these screens.

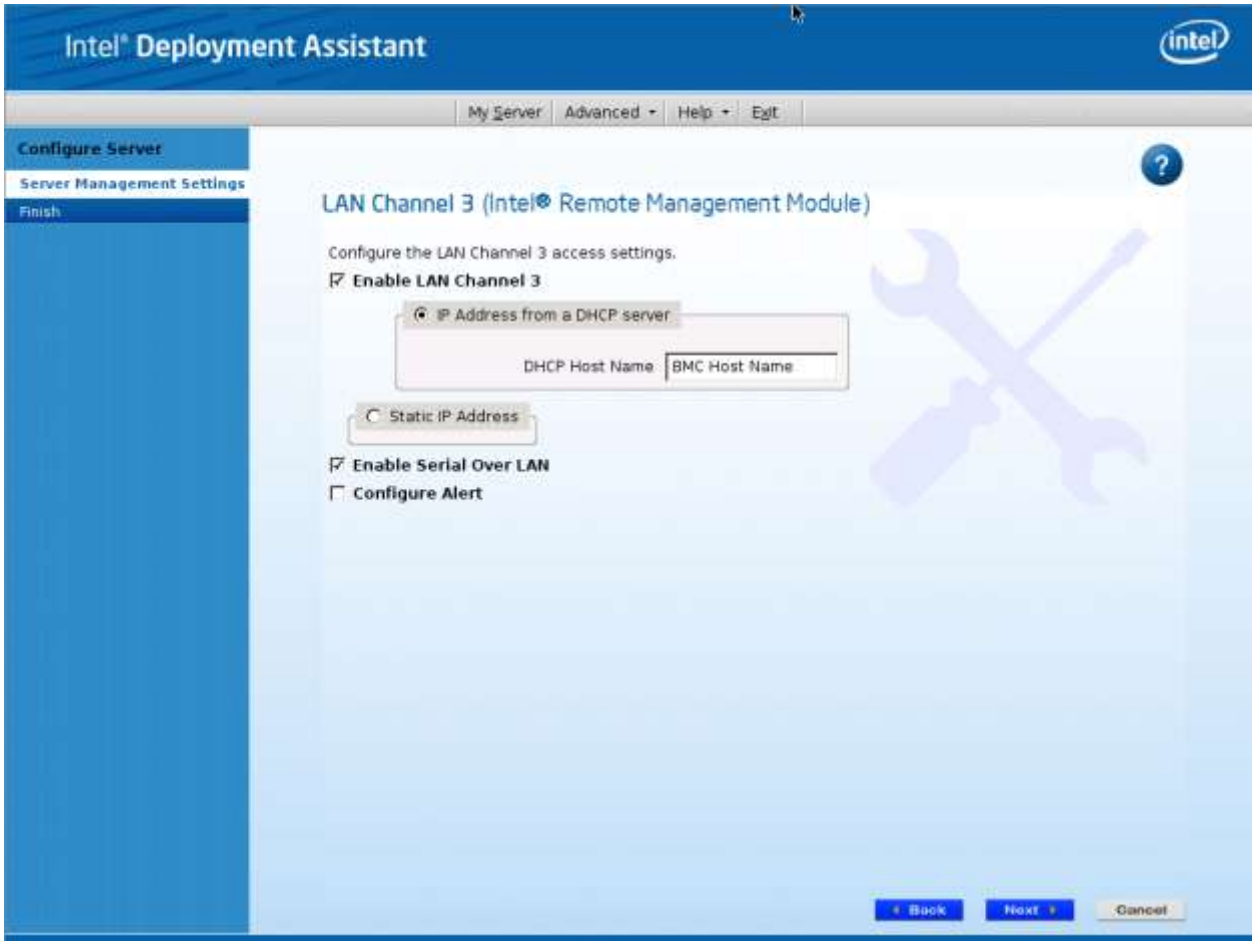


Figure 26: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) IP Address from a DHCP Server Window

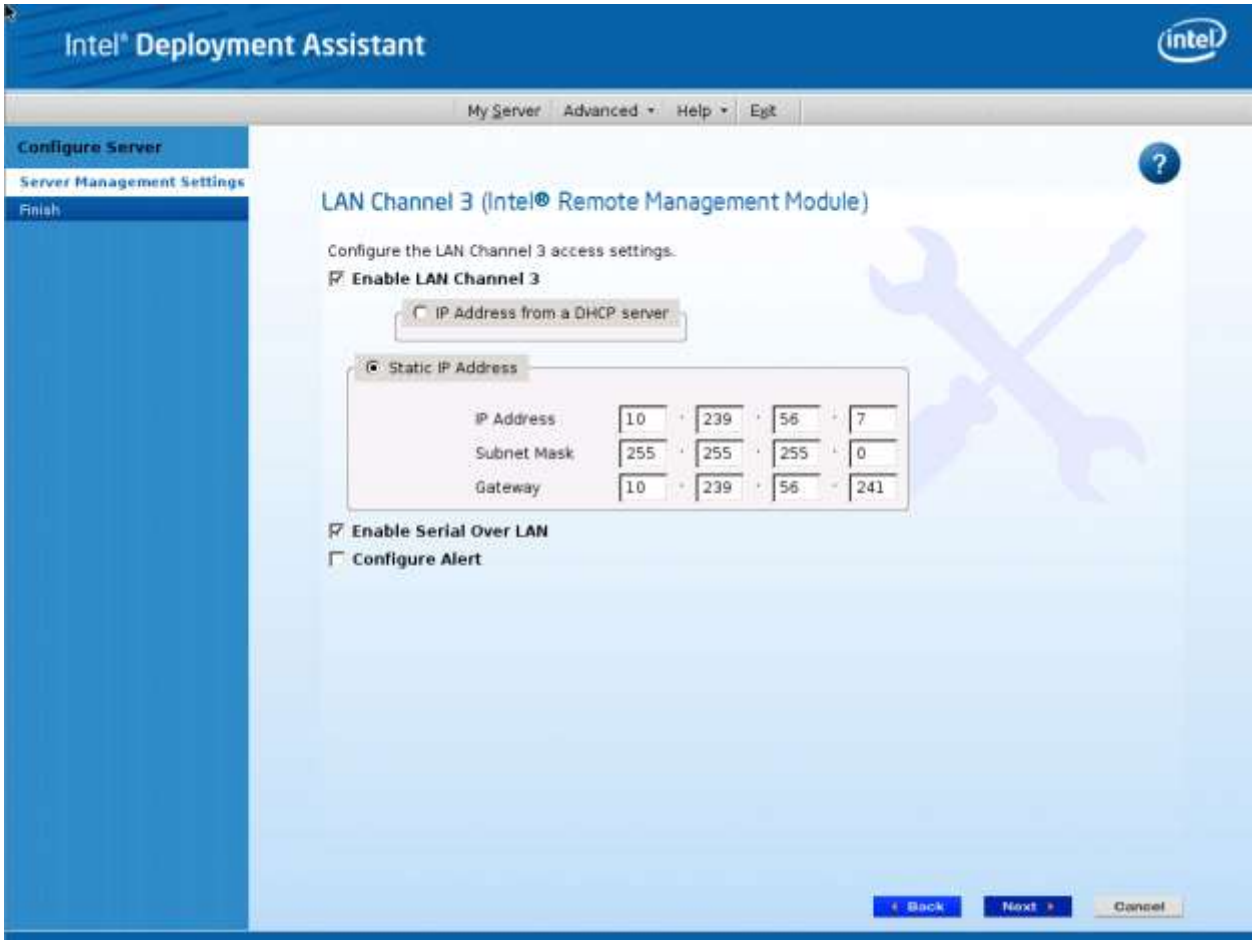


Figure 27: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) Static IP Address Window

4. (Optional) Set up the users by selecting the **User Name** and then clicking **Edit**.
   The Edit User Data window is displayed.

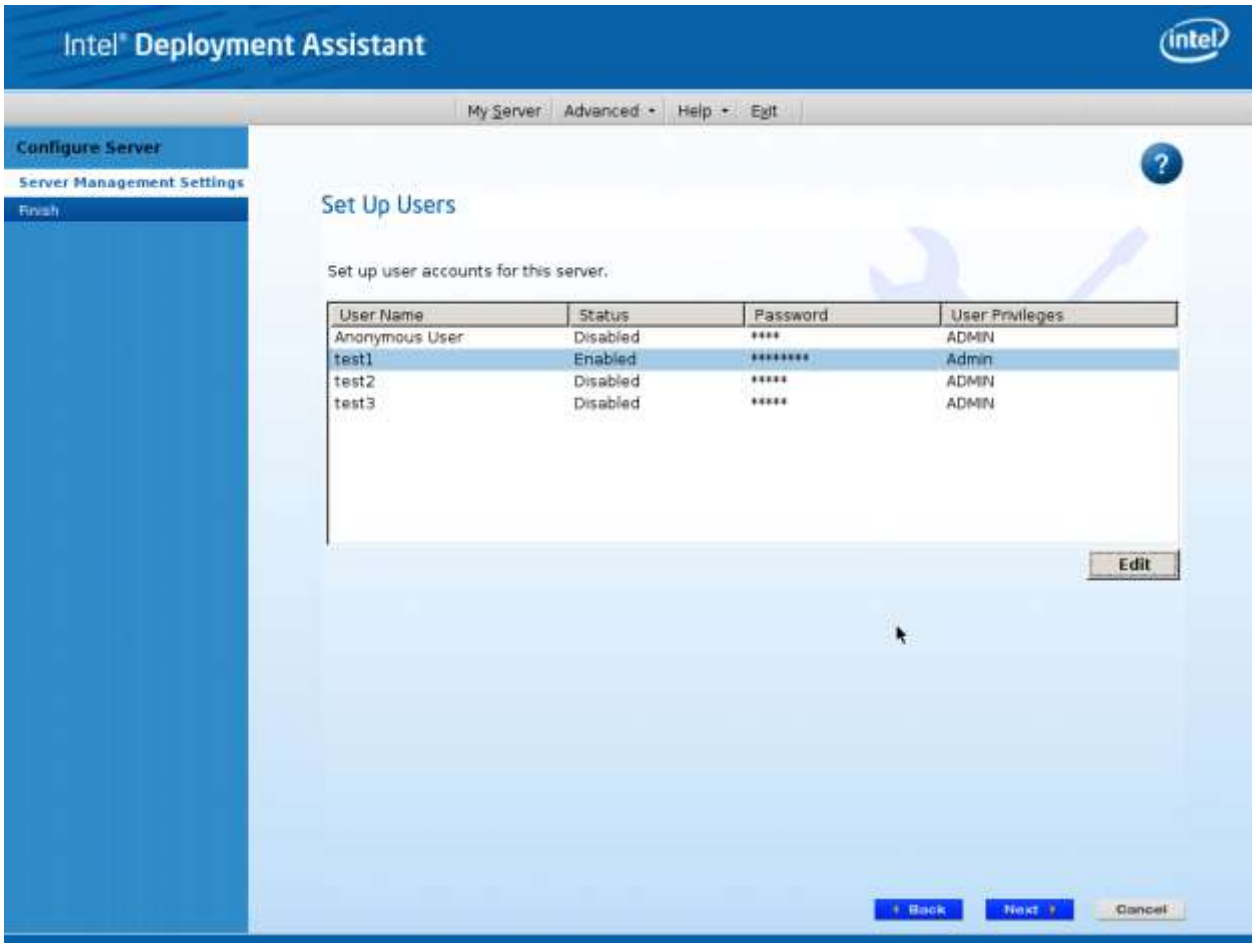


Figure 28: IDA Configure Server: Set Up Users Window

Notes:

- You cannot login to the Integrated BMC Web Console or RMM4 Remote Console as an Anonymous User. You must modify the existing users.
- Enable and edit the username/passwords; set the privilege for the users as shown below.

5. Edit the user information and click **OK** to apply configuration.

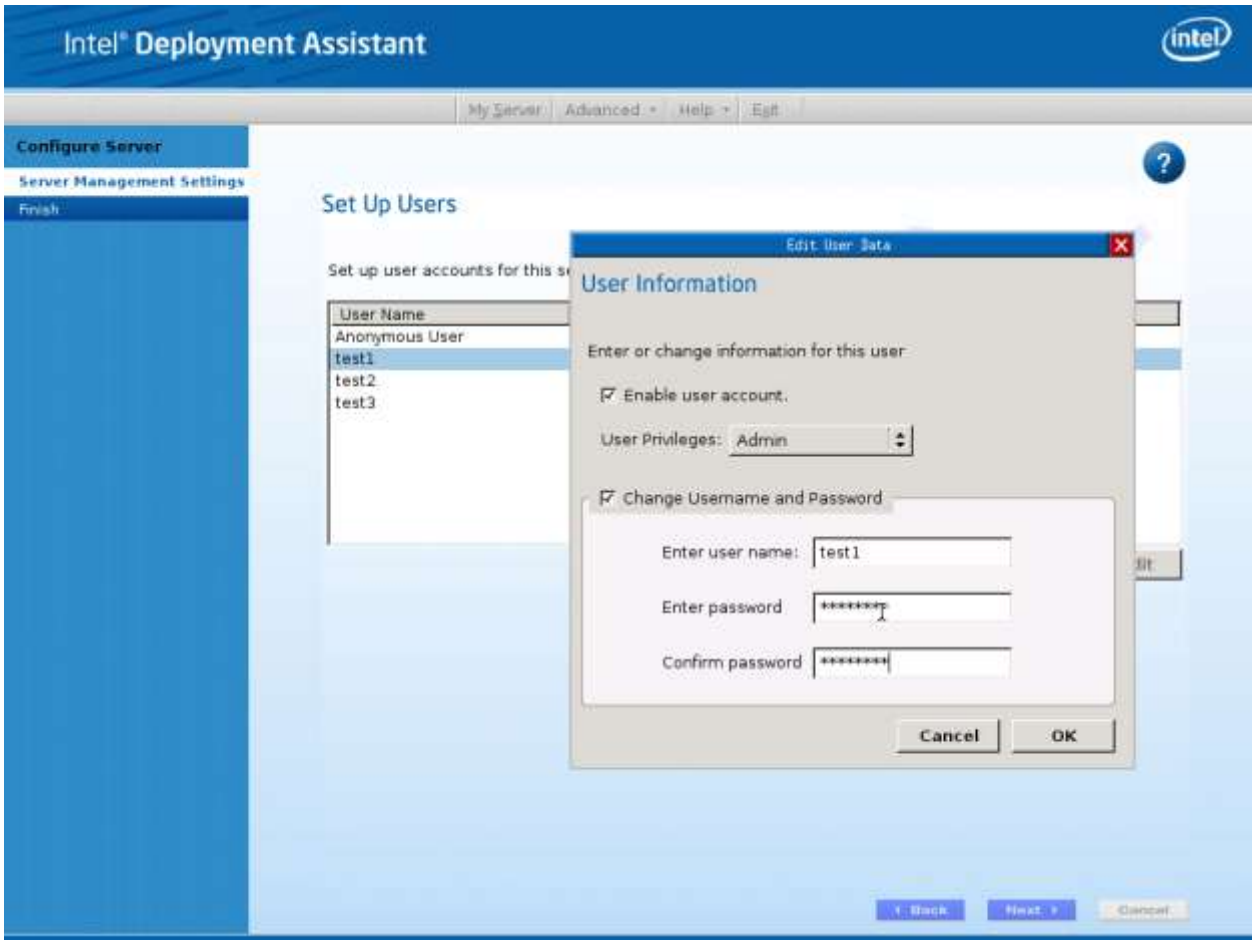


Figure 29: IDA Configure Server: Edit User Information Window

6. Click **Apply** to save your settings.

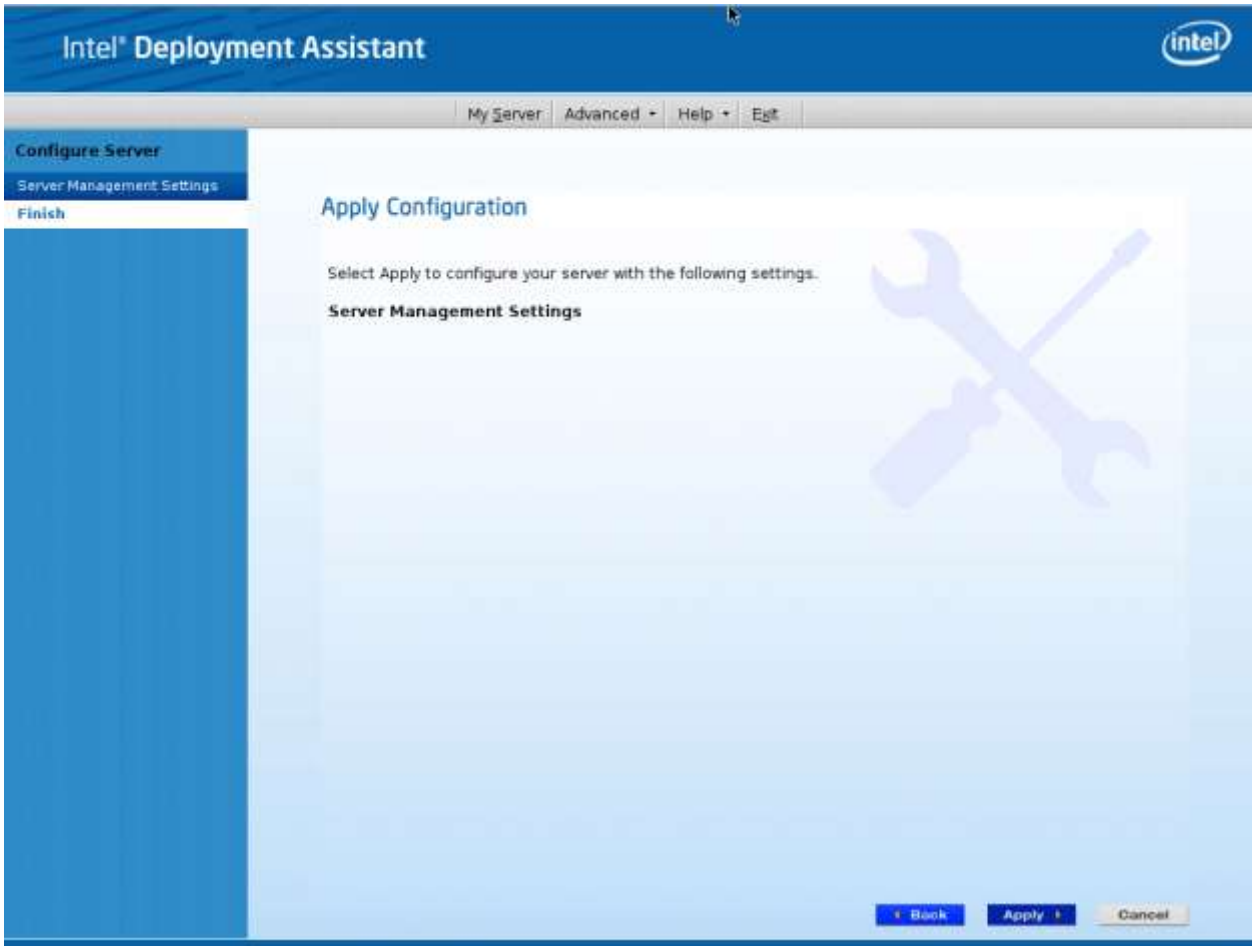


Figure 30: IDA Configure Server: Apply Configuration Window

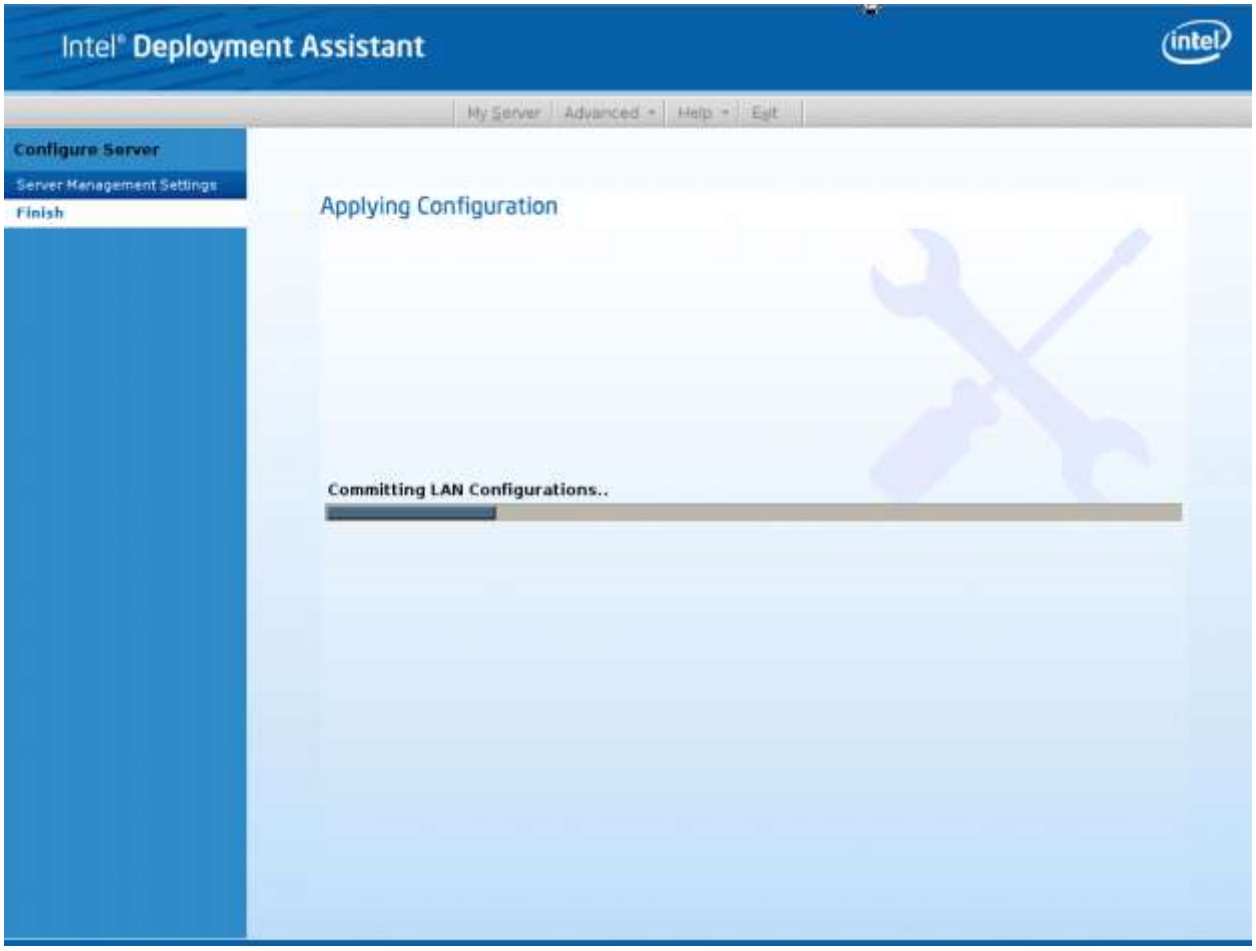


Figure 31: IDA Configure Server: Applying Configuration Progress Window

7. Keep a record of the DHCP Host Name and assigned IP address.
   These will be needed later when you are trying to connect to the Integrated BMC Web Console.
8. In order for the configuration settings to take effect, the server must be restarted. Click the **Restart** button.

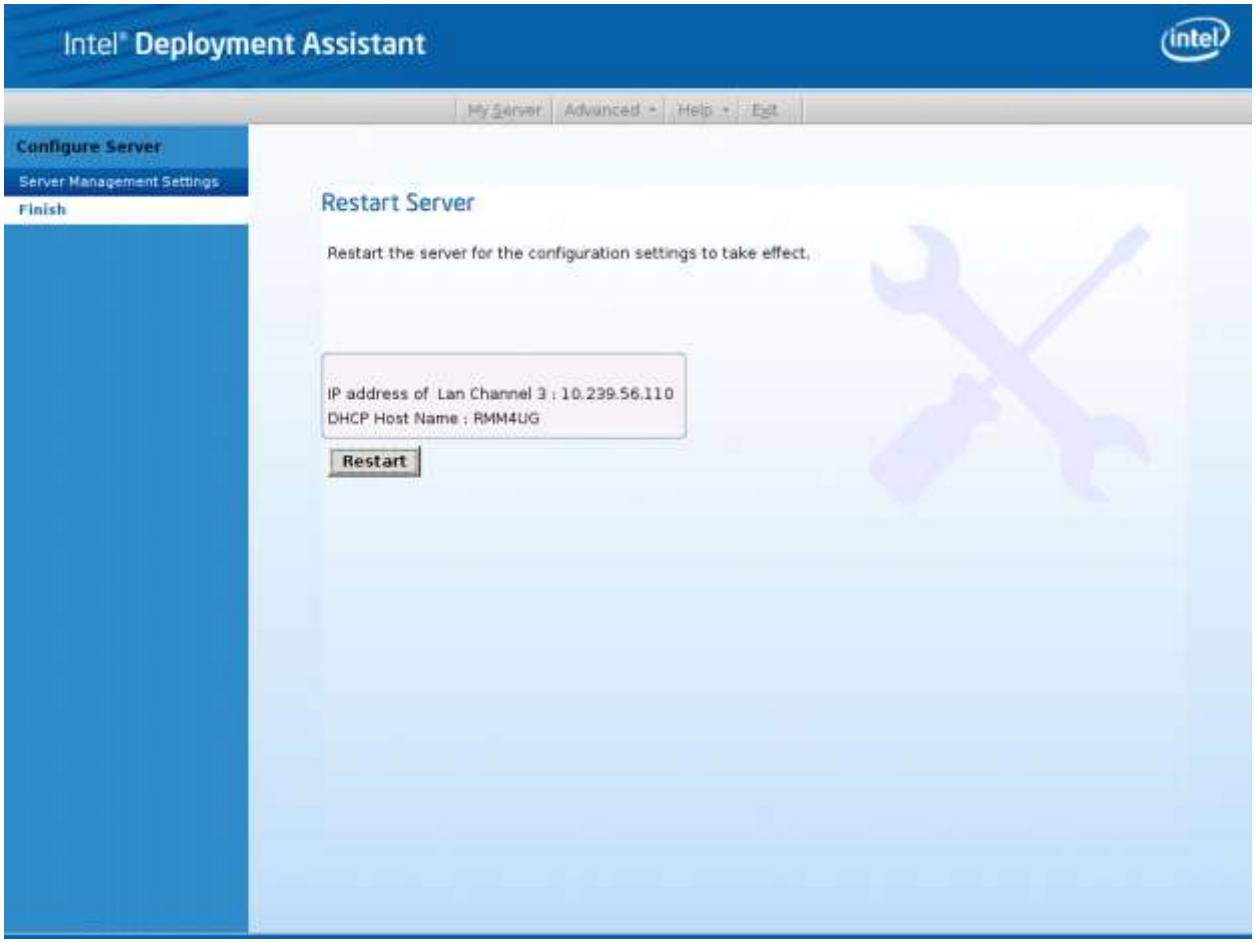


Figure 32: IDA Configure Server: Restart Server

4.4 Configuring the Server Management NIC using the Intel® System Configuration Utility (SysConfig)

This section describes the basic commands needed to configure the RMM4 using *SysConfig* commands. This utility is supported in EFI, Linux*, and Microsoft Windows*. The commands are the same for all versions. At a minimum, you need to configure the following settings:

- Enable one user
- Enable user's privilege level
- Set users and passwords
- IP source (static or DHCP)
- IP Address
- Subnet mask
- Default gateway (only required if you will be connecting from client outside of subnet)
- Enable text-based console redirection (Serial Over LAN – SOL) if needed

Note: The examples in the following sections use the Intel® Dedicated Server Management NIC LAN channel 3. If you are not using the Intel® Dedicated Server Management NIC, substitute the appropriate channel number. For NIC1 it will be channel 1. For NIC2 it will be channel 2.

4.4.1 Configuring the User

Step by step instructions to enable a user for the RMM4:

1. Set the password for BMC user 2 (root) by typing (password is "p@ssw0rd" in this example):
   ```
   syscfg /u 2 "root" "p@ssw0rd"
   ```
2. Enable the BMC user 2 on LAN channel 3 by typing:
   ```
   syscfg /ue 2 enable 3
   ```
3. Enable the "admin" privilege and payload type to "SOL+KVM" for the BMC user 2 on LAN channel 3 by typing:
   ```
   syscfg /up 2 3 admin sol+kvm
   ```

4.4.2 Configuring the IP Address

- Set static IP address and subnet mask on LAN channel 3 by typing:
  ```
  syscfg /le 3 static <STATIC_IP> <SUBNET_MASK>
  ```
- If needed, set the default gateway on LAN channel 3 by typing:
  ```
  syscfg /lc 3 12 <DEFAULT_GATEWAY_IP>
  ```
- Set DHCP IP address source on LAN channel 3 by typing:
  ```
  syscfg /le 3 dhcp
  ```

4.4.3 Configuring the Serial Over LAN

- If needed, enable the Serial Over LAN (SOL) on LAN Channel 3 by typing:
  ```
  syscfg /sole 3 Enable Admin BAUD_RATE RETRY_COUNT
  RETRY_INTERVAL_IN_MILLISECONDS
  ```

5. Getting Started with Intel® RMM4 Operation

The Intel® RMM4 module features remote KVM access and control through LAN or Internet. The Intel® Integrated BMC Web Console is part of the standard BMC firmware / Server Management Software. The Integrated BMC Web Console feature is used to access the remote KVM.

This section describes both the interfaces and how to use them. The interfaces are accessed using TCP/IP protocol.

5.1 Before You Begin

For initial setup information, refer to Chapter 4. Before you log in, you must enable the intended user. The examples in this chapter use user “root’, but other usernames and passwords could be used.

The Intel® RMM4 enabled advanced features may be accessed using a standard Java* enabled web browser. You may use the HTTP protocol or a secure encrypted connection from the HTTPS configurable in the embedded web server.

5.1.1 Client Browsers

In order to access the web console using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a Cipher Strength (encryption) of 128-bit. Some older browsers may not have a strong 128-bit encryption algorithm.

If you are using Microsoft Windows Internet Explorer 7.0* or higher, you can verify the strong encryption by opening the **Help/About** menu to read about the key length that is currently activated. Figure 33 shows the dialog box presented by Microsoft Windows Internet Explorer 8.0*.

Figure 33: Internet Explorer 8* Displaying Encryption Key Length

In order to use the Remote Console (KVM) window of your managed server, Java Runtime Environment* (JRE*) Version 6 Update 22 or higher must be installed.

Note: The Web Console is designed for a screen size of 1280 pixels by 1024 pixels or larger. In smaller screens, the browser displays slider controls to enable the user to see the full content of each web page.

5.2 Logging In

Enter the configured IP address of the Intel® RMM4 or your configured BMC on-board NIC into your web browser. In order to use a secure connection, type `https://<IPaddress>/`. This will take you to the Intel® Integrated BMC Web Console module login page as shown in Figure 34.

Figure 34: Intel® Integrated BMC Web Console Login Page

Log in by entering the username and password.

For example:

- Username = root
- Password = superuser

Click the **Login** button (shown in Figure 34) to view the home page.

After the initial login, system administrators may change passwords, create new users, and have full control over access to the RMM4 enabled advanced features.

Note: The username and password are case sensitive. Any username and password can be used (except anonymous).

5.3 Navigation

After successful login to the Integrated BMC Web Console module, the Integrated BMC Web Console home page appears as shown in Figure 35.

Figure 35: Integrated BMC Web Console Home Page

The top horizontal toolbar within the Integrated BMC Web Console home page has four tabs. Click these tabs to get specific system information and perform tasks as shown in the following table.

Table 9: Integrated BMC Web Console Home Page Tabs

Tab	Function
System Information	Click this tab to access general information about the server. The tab automatically opens the System Information page: • System Information • FRU Information • CPU Information (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • DIMM Information
Server Health	Click this tab for access to the sensors and event log. The tab automatically opens the Sensor Readings page: • Sensor Readings • Event Log • Power Statistics

Tab	Function
Configuration	Click this tab to configure various settings for the server. The tab automatically opens the Network configuration page: • Network/IPv4 Network • IPv6 Network (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • Users • Login • LDAP • VLAN (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • SSL • Remote Session • Mouse Mode • Keyboard Macros • Alerts • Alert Email • Node Manager (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families)
Remote Control	Click this tab for access to the remote console and to control the power state of the server: • Console Redirection • Server Power Control • Virtual Front Panel (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families)

The four tabs on the horizontal menu allow you to navigate within the Integrated BMC Web Console. Each of these tabs contains a secondary menu on the left edge of the browser window. For detailed information on the specific functions of secondary menu item see Chapter 7.

The top horizontal toolbar also has the **Logout**, **Refresh**, and **Help** buttons. Click these buttons to perform tasks as shown in the following table.

Table 10: Horizontal Toolbar Buttons

Button	Function
LOGOUT	Click this button to end the current Web Console session. Note that a remote console (KVM) window, if active, will be closed when you log out. After logging out, the Web Console will return to the Login screen.
REFRESH	Click this button to refresh the current web page, including any data shown on the page. **Note:** Using the web browsers refresh/reload button or pressing the function key <F5> to do a refresh/reload is not supported for reloading the Web Console pages. Using either of them can cause unexpected results.
HELP	Click this button to view a brief description of the current page in a frame at the right side of the browser window. Close the Help frame by clicking the "X" in the upper right corner of the frame or by clicking the **HELP** button again.
ABOUT	Click this button to view the Intel® copyright information and a statement about the use of open source code.

5.4 Online Help

The Web Console user interface provides specific online help for each page. For additional information on a certain topic or group of options, click the HELP button on the top horizontal toolbar to view the online help as shown in Figure 36. The right **Help** frame is visible only when the online **Help** is being accessed.

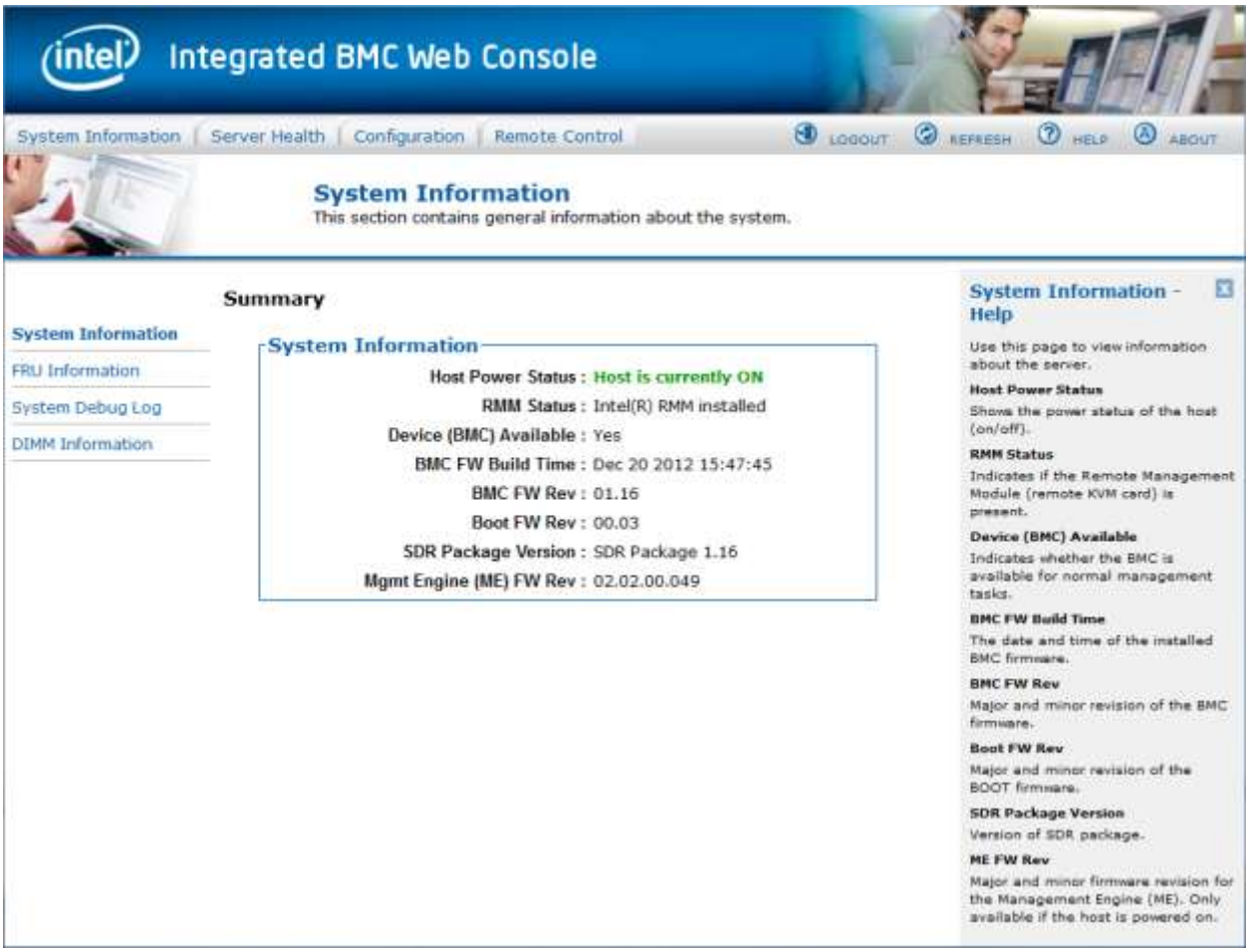


Figure 36: Launching the Online Help

5.5 Logging Out

Click the

button to log out the current user and revert to a new login screen as shown in Figure 37 and Figure 38.

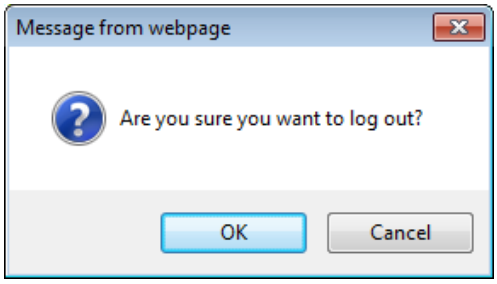


Figure 37: Logging Out of Integrated BMC Web Console – Step 1

Figure 38: Logging Out of Integrated BMC Web Console – Step 2

Note: Automatic Timeout – If there is no user activity detected by the Web Console for 30 minutes, the current session will be automatically terminated. If the user has an open KVM remote console window, the web session will not automatically timeout. The next action attempted by the user after the automatic timeout will inform the user of the need to login again for continued access to the Web Console.

6. Remote Console (KVM) Operation

The Remote Console is the redirected keyboard, video, and mouse of the remote host system where the Intel® RMM4 module is installed. To use the Remote Console window of your managed host system, the browser must include a Java Runtime Environment* plug-in. If the browser has no Java* support, such as with a small handheld device, the user can maintain the remote host system using the administration forms displayed by the browser.

Starting the Remote Console opens a new window to display the screen content of the host system. The Remote Console acts as if the administrator were sitting directly in front of the screen of the remote system. This means the keyboard and mouse can be used in the usual way.

6.1 Launching the Redirection Console

The Remote Console is the redirected keyboard, video, and mouse of the remote host system where the Intel® RMM4 module is installed. Launch the remote console KVM redirection window from this page.

Note: If you are using Microsoft Windows Internet Explorer*, the Smart Screen is enabled, and the system is on a network with no direct connectivity to the internet, it may take an extremely long time to open a KVM window.

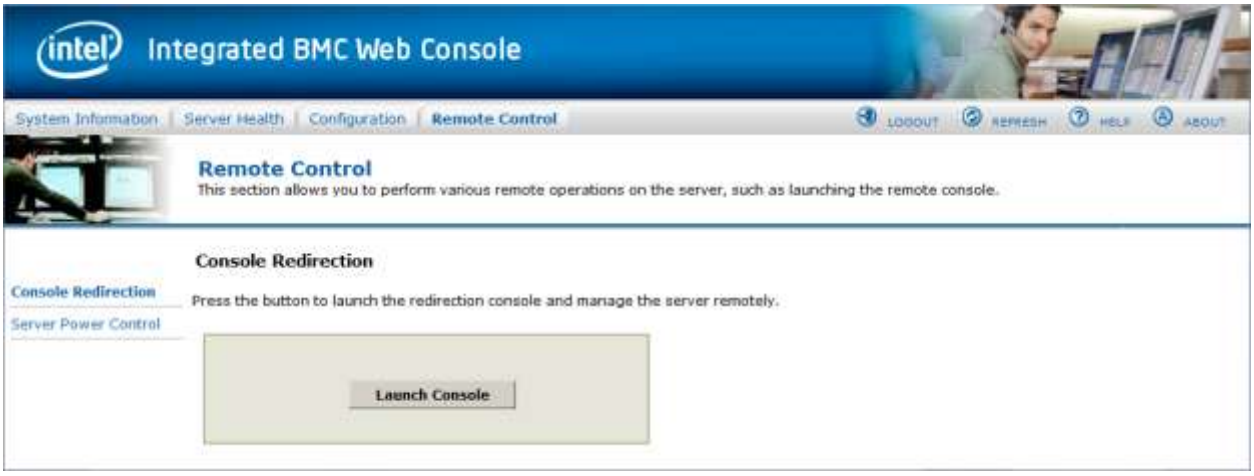


Figure 39: Remote Control Console Redirection Page

Click the **Launch Console** button to launch the redirection console and manage the server remotely.

When the **Launch Console** button is clicked, a pop-up window is displayed to download the Java Network Launch Protocol*, `jviewer.jnlp` file. This in turn downloads the standalone Java* application implementing the Remote Console.

Both Microsoft Internet Explorer* and Mozilla Firefox* browsers are supported.

Notes:

- Java Runtime Environment* (JRE*, Version 6 Update 22 or higher) must be installed on the client before the launch of a JNLP file.
- The client browser must allow pop-up windows from the Integrated BMC Web Console IP address.

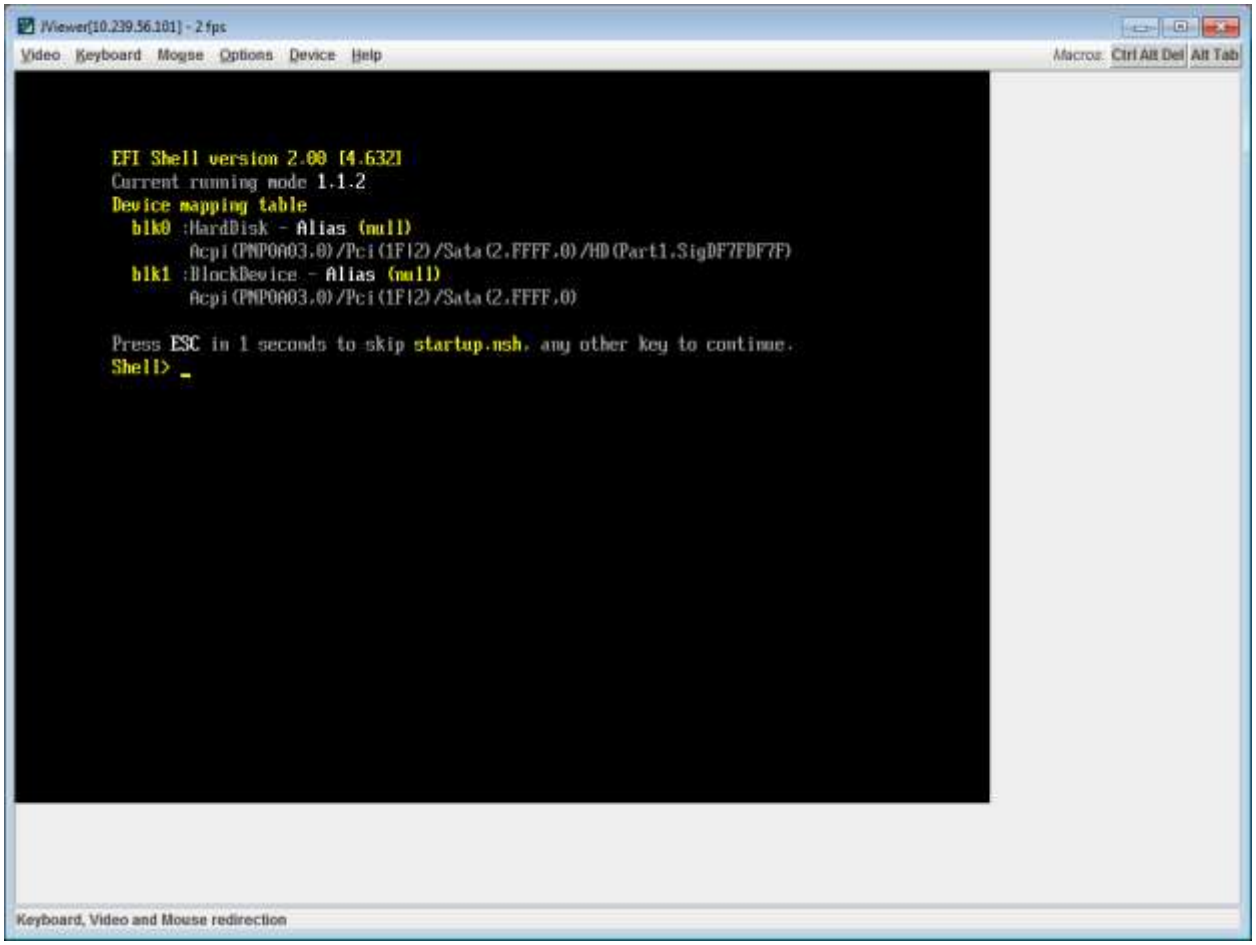


Figure 40: Remote Console

The Remote Console window is a Java Applet* that establishes TCP connections to the Integrated BMC Web Console. The protocol that is used to run these connections is a unique KVM protocol and not HTTP or HTTPS. This protocol uses ports #7578 for KVM, #5120 for CDROM media redirection, and #5123 for Floppy/USB media redirection. Your local network environment must permit these connections to be made, that is, your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

6.2 Main Window

Starting the Remote Console opens an additional window as shown in Figure 41.

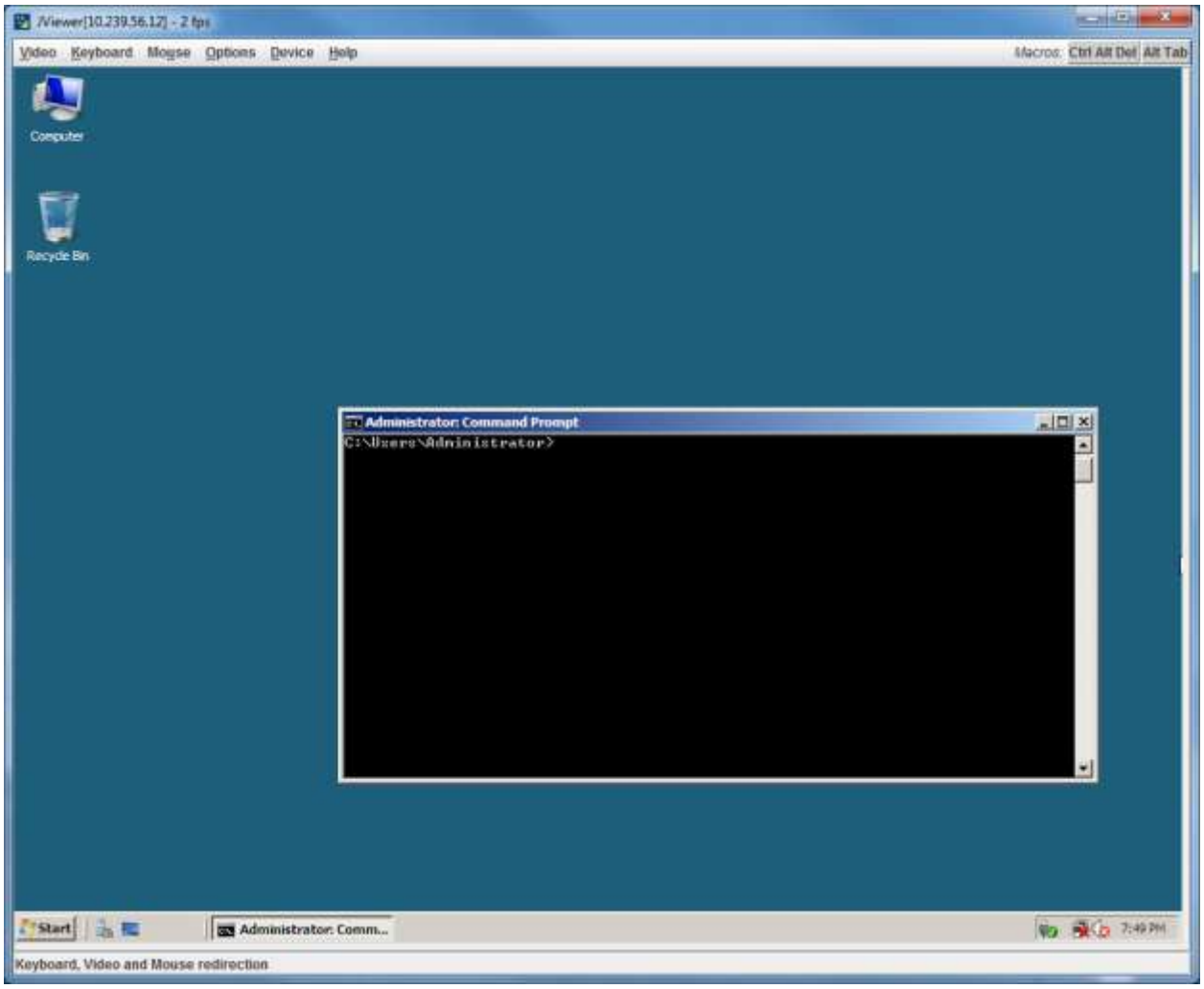


Figure 41: Remote Console Main Window

It displays the screen content of your remote server. The Remote Console behaves as if you were located at the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between Integrated BMC Web Console and Remote Console. Enabling KVM and/or media encryption on the **Configuration** > **Remote Session** web page will degrade performance as well.

The Remote Console window always shows the remote screen in its *optimal size*. This means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window as usual.

6.3 Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings.

Figure 42: Remote Console Control Bar

The following sub sections describe the tasks you can perform within each control.

6.3.1 Remote Console Video Menu

Click **Video** in the Remote Console control bar to open the Video menu as shown in Figure 43.

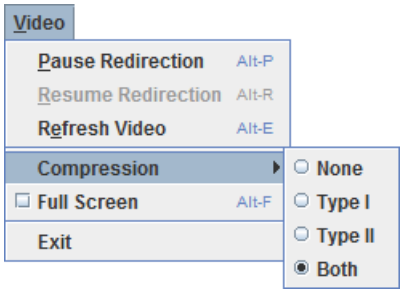


Figure 43: Remote Console Video Menu

Using this menu, you can do the following:

- **Pause Redirection.** Temporarily pauses the redirection of keyboard, video, and mouse. The Remote Console window stops being updated. Keyboard shortcut is Alt+P.
- **Resume Redirection.** Resumes the redirection after a pause. Shortcut is Alt+R.
- **Refresh Video.** Refreshes the Remote Console window. Shortcut is Alt+E.
- **Compression.** Enabling compression improves the responsiveness of the Remote Console. Disabling compression maximizes the quality of the redirected video.
- **Full Screen.** Toggles windowed/full screen mode of the Remote Console. Shortcut is Alt+F.
- **Exit.** Closes the Remote Console window.

6.3.2 Remote Console Keyboard Menu

Click **Keyboard** to open the Keyboard menu as shown in Figure 44.

Figure 44: Remote Console Keyboard Menu

Using this menu, you can do the following:

- **Language.** Controls the keyboard language layout.
- **Soft Keyboard.** Displays and controls the Soft Keyboard window.
- **Hold Ctrl/Alt/Windows* keys.** Allows simulation by holding down these special keys on the remote keyboard. On the local keyboard these special keys are processed by the local OS and not passed on to the remote OS.
- **Ctrl+Alt+Del, Ctrl+Alt+Backspace, Ctrl+Alt+Left, Ctrl+Alt+Right.** Issues a fixed special key combination to the remote OS.

6.3.2.1 Keyboard Language Layout

The Remote Console supports the following keyboard language layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

Figure 45: Remote Console Keyboard Language Sub Menu

In order for local key strokes to be interpreted correctly at the remote end, the client OS, the target OS, and the Remote Console must all be configured for the same language layout.

The Remote Console Java* application reversely translates local key strokes based on the selected language layout. If there is a mismatch, sometimes it works fine anyway, otherwise it mostly works except for a few mistranslated or unresponsive keys and in some mismatched configurations most of the keys are mishandled.

6.3.2.1.1 Windows Language Layouts*

The Remote Console supports the Windows* default keyboard variants for the supported languages.

In Windows*, the language is the current Language Bar setting (initially configured in **Control Panel** > **Regional and Language Options** > **Languages** > **Text Services and Input Languages**). If you are using one of the supported language keyboards, you don't have to manually select the language in the Remote Console because any Language Bar changes can be detected automatically and immediately. Manually setting the language would typically be useful if you are using a keyboard close but not identical to one of the supported ones.

6.3.2.1.2 Linux Language Layouts*

The Remote Console supports the Linux* default keyboard variants for supported languages, except Russian, where it is the "Russian Winkeys" variant. The Dutch layout is "Belgium" in Linux*.

In Linux* you typically select the language at the login screen; it can also be changed with the "locale" command but not while an application, such as the Remote Console, is running. There is also an OS keyboard layout that can be changed independently of the language. If the OS keyboard layout does not match the OS language setting, you may need to manually select the Remote Console layout.

On the other hand, with Linux* Java*, there is less reverse translation required by the application than in Microsoft Windows* and is more likely that a mismatched configuration will work anyway.

6.3.2.2 Soft Keyboard

Click **Keyboard** to open the Keyboard menu as shown in Figure 46.

Figure 46: Remote Console Keyboard Soft Keyboard Sub Menu

The Soft Keyboard window is displayed and closed either by selecting the **Keyboard** > **Soft Keyboard** > **Show** checkbox or by the Alt+S shortcut.

Figure 47: Remote KVM Soft Keyboard

Buttons clicked on the Soft Keyboard window get sent as key strokes to the remote target.

The Soft Keyboard is also a convenient way to see the exact layouts supported for the local keyboards because they are the same.

The Soft Keyboard language layout follows the local keyboard language setting when the default **Keyboard** > **Soft Keyboard** > **Follow Local** option is selected. This can be manually overridden by selecting a language.

Note: The Soft Keyboard keystrokes get retranslated by the remote target OS just like the local physical keystrokes and are subject to the same mismatched configuration issues.

6.3.3 Remote Console Mouse Menu

Click **Mouse** to open the Mouse menu as shown in Figure 48.

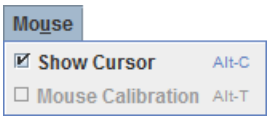


Figure 48: Remote Console Mouse Menu

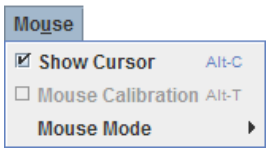


Figure 49: Remote Console Mouse Menu on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

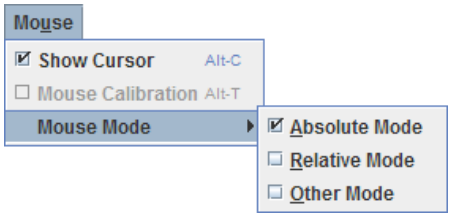


Figure 50: Remote Console Mouse Menu – Mode Selection on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The Mouse submenu offers two or three options:

- **Show Cursor**. This option toggles the cursor display in the Remote Console window. It does not affect the remote system cursor. Shortcut is Alt+C.

- **Mouse Calibration**. This option is used to detect the threshold and acceleration settings on the remote system and set the local client's mouse settings accordingly. It only applies when in Relative Mouse Mode, selected on the web page **Configuration** > **Mouse Mode**. Absolute Mouse Mode does not require calibration. Shortcut is Alt+T.

- **Mouse Mode.** This option is only available on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families. See Figure 49. This allows you to select the mouse mode being used. You can select Absolute, Relative, or Other as shown in Figure 50. For a description of these modes, see Section 7.3.9. Note that the functionality of this option is the same as changing then saving the mode on the Mouse Mode page. Any selections that you make will be saved for the next time when the remote console window is opened.

Relative Mode Mouse Calibration Procedure

1. If the remote mouse and local mouse cursors are not in sync, start mouse calibration by selecting the **Mouse Calibration** menu item or pressing Alt+T.

2. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in red color and the remote cursor is part of the remote video screen. Both cursors will be in sync in the beginning.

3. Use number pad '+' or '-' keys to change the threshold settings until both cursors go out of sync.

4. Detect the first reading at which the cursors go out of sync.

5. After the reading is detected, use Alt-T to save the threshold value.

6. In this step, the mouse acceleration settings on the remote server will be discovered. The local mouse cursor is displayed in red color and the remote cursor is part of the remote video screen. Both cursors will be out of sync in the beginning.

7. Use number pad '+' or '-' keys to change the acceleration settings in steps of 1, or use Alt-'+' or Alt-'-' keys to change the acceleration settings in steps of 0.1 until both cursors are in sync.

8. Detect the first reading at which the cursors are in sync.

9. After the reading is detected, use Alt-T to save the acceleration value.

6.3.4 Remote Console Options Menu

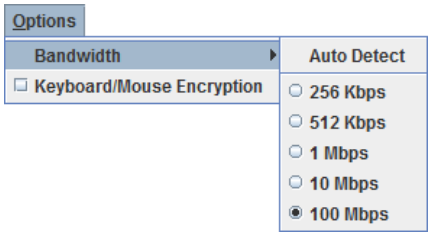


Figure 51: Remote Console Options Menu

Using this menu, you can do the following:

- **Bandwidth.** Changing the bandwidth setting affects low-level connection protocol parameters such as fragment size and timeouts. If you experience performance problems when operating over a slow connection such as a modem, the bandwidth setting may need to be adjusted. Use the **Auto Detect** option to find the correct setting for your connection.

- **Keyboard/Mouse Encryption.** Keyboard and mouse data is normally encrypted before being sent over the connection, but this can be disabled for a small performance increase.

6.3.5 Remote Console Device Menu

Figure 52: Remote Console Device Menu

This menu option allows starting/stopping remote media redirection. The first two options allow you to redirect either a local CDROM/DVD drive or else an ISO image on your local client file system as a virtual CDROM device on the remote system. The third option allows you to redirect either a local floppy drive or local USB key drive. The fourth option allows you to redirect a floppy or USB Key `.img` file on your local client file system as a virtual floppy device on the remote system.

Note: When trying to attach a local floppy or local USB key drive, if it is in use by the operating system or any other application it will fail to attach.

With Microsoft Windows 2008*, Microsoft Windows Vista*, Microsoft Windows 2008* R2, and Microsoft Windows 7* if a Windows Explorer* GUI is opened after the USB Key has been installed in the local system, you may not be able to attach the USB Key as remote media.

With Microsoft Windows 2003* and Microsoft Windows XP* if a Windows Explorer* GUI is opened after the USB Key has been installed in the local system and you then browse through the USB Key, you may not be able to attach the USB Key as remote media.

The virtual devices act just like any other CDROM/DVD or floppy on the remote system. They can be read, written (assuming they are not read-only), and booted. The pair of virtual devices only appears on the remote OS or BIOS setup menus when some media redirection is active. The virtual devices persist across remote system resets and power up/downs. They do not disappear from the remote system until the checkboxes are unchecked in the Remote Console window.

Note: The virtual devices are not limited to normal floppy/CDROM sizes and will be as large as the device or file being redirected. A USB Key drive is redirected as a virtual floppy device rather than a USB device to allow the loading of custom device drivers during remote OS installation which may require a floppy drive.

There is only one virtual CDROM and one virtual floppy device on the remote system allowed so only one local item of each type can be redirected at a time. Only one Remote Console window can be doing media redirection at any given time.

6.4 Remote Console Status Line

The status line at the bottom of the Remote Console screen shows the console state as shown in Figure 53. When you navigate the menu options, the status line provides a more detailed definition of each option.

Figure 53: Status Line

7. Intel® Integrated BMC Web Console Options

This chapter gives you a detailed description of each Integrated BMC Web Console page. It is organized in sections corresponding to the four tabs in the horizontal menu. Within each section, each menu on the left side is illustrated and described in detail.

Notes:

- The first menu item for each tab is the default page that appears when the tab is selected.
- Similar information about each page is available in the Web Console by clicking the **HELP** button at the right side of the horizontal menu.
- When the Web Console is working on current user request, a busy indicator bar appears as shown in Figure 54.

Figure 54: Busy Indicator Bar

- Not all of the following sections are used by or directly related to the RMM4 enabled features but have been added here for completeness.

7.1 System Information Tab

The System Information tab contains general information about the system as explained in the following sub sections.

Click the **System Information** tab to select the various pages. By default, the Integrated BMC Web Console home page opens the System Information page.

7.1.1 System Information Page

The System Information page displays a summary of the general system information. This includes the power status and the version of firmware. Figure 55 shows the details for a S1200BTL system.

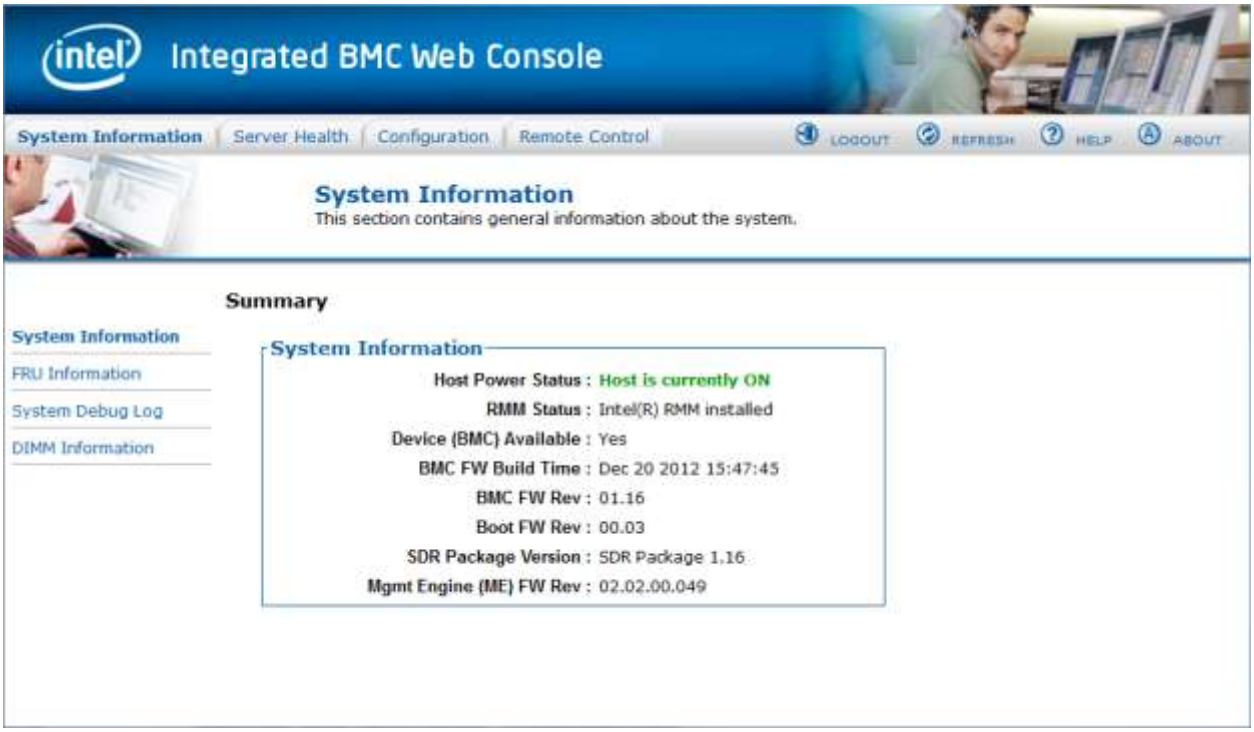


Figure 55: System Information Page on S1200BTL Platforms

The System Information page has the following information about the server.

Table 11: System Information Details

Information	Details
Host Power Status	Shows the power status of the host (on/off).
RMM Status	Indicates whether the Intel® RMM4 card is present.
Device (BMC) Available	Indicates whether the BMC is available for normal management tasks.
BMC FW Build Time	The date and time of the installed BMC firmware.
BMC FW Rev	Major and minor revision of the BMC firmware.
Boot FW Rev	Major and minor revision of the BOOT firmware.
SDR Package Version	Version of the Sensor Data Record.
Mgmt Engine (ME) FW Rev	Major and minor revision of the Management Engine firmware.

On an EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you also get an **Overall System Health** indication. See Figure 56 for details. These are a general indication of the system heath:

- Left (Green) = System Ready LED
- Center (Amber) = System Fault LED
- Right (Blue) = Chassis ID LED

Figure 56: System Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

On S1200V3RP Product Family the Baseboard Serial Number is added to display along with the **Overall System Health** indication. See Figure 57 for details. These are a general indication of the system heath:

- Left (Green) = System Ready LED
- Center (Amber) = System Fault LED
- Right (Blue) = Chassis ID LED

Figure 57: System Information Page on S1200V3RP Product Family

7.1.2 Field Replaceable Unit (FRU) Information Page

The Field Replaceable Unit (FRU) Information page displays information from the FRU repository of the host system. See Figure 58 for details.

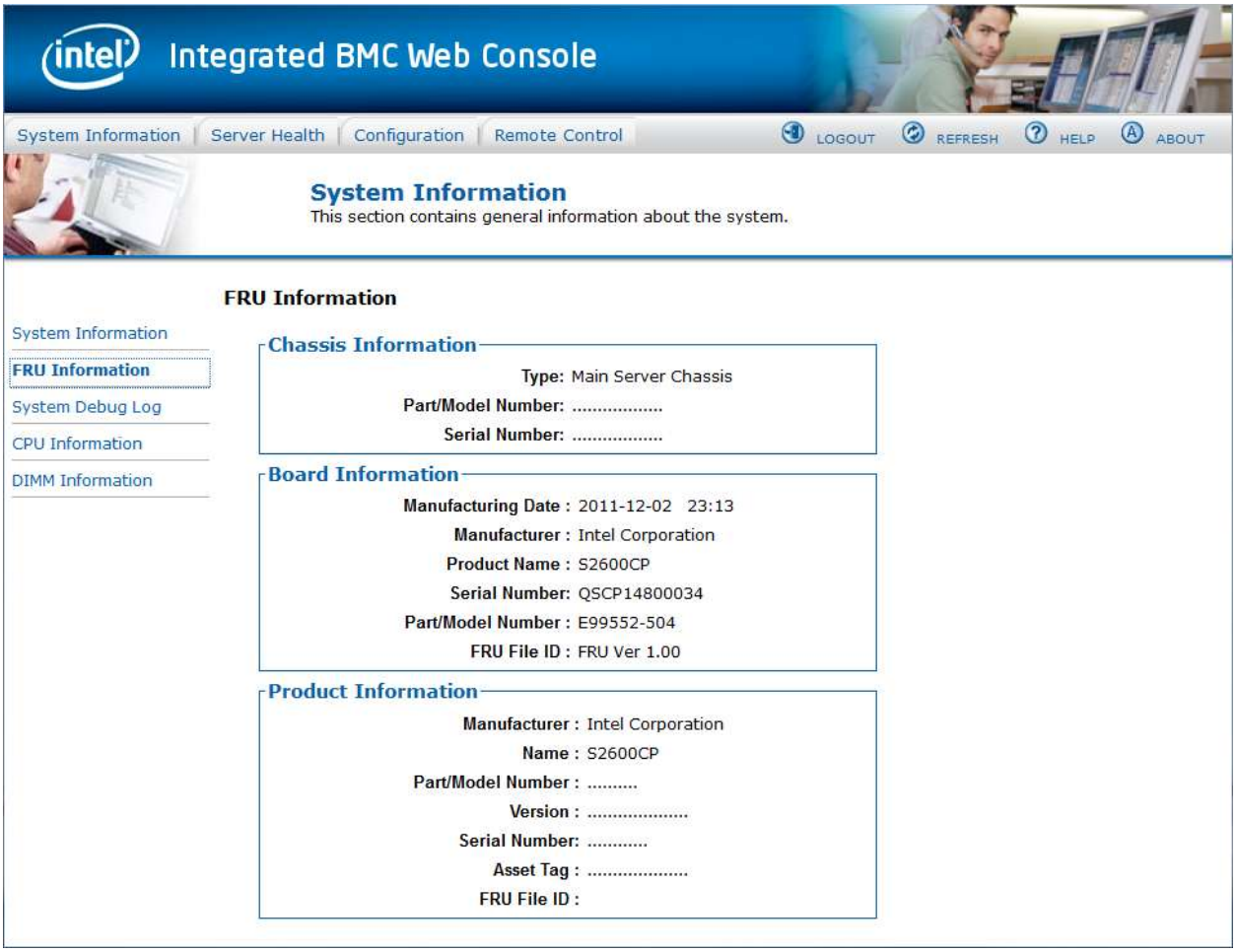


Figure 58: System Information FRU Information Page

7.1.3 System Debug Log Page

The System Debug Log page allows administrators to collect system debug information. This feature allows a user to export data into a file that is retrievable for the purpose of sending to an Intel engineer or Intel partners for enhanced debugging capability. The files are compressed, encrypted, and password protected. The files are not meant to be viewable by the end user but rather to provide additional debugging capability to your system manufacturer or an Intel support engineer.

7.1.3.1 System Debug Log Page on S1200BTL Platforms

The System Debug Log page can be used to collect system debug information on S1200BTL systems. See Figure 59 for details.

From the System Debug Log page you can run the System Debug Log dump.

Click the **Generate Log** button. It may take some time for the debug information to be collected.

After the debug log dump is finished, you can click the debug log filename to save the results as a .zip file on your client system. The file can then be sent to your system manufacturer or an Intel support engineer for analysis.

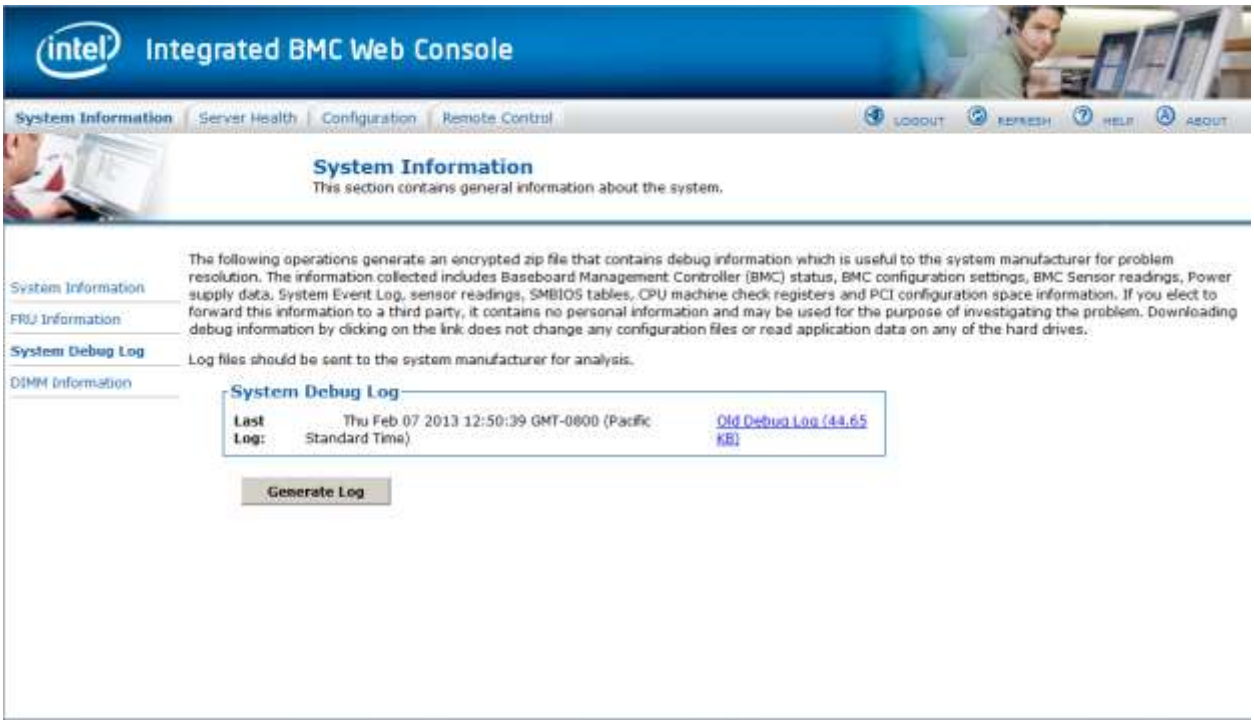


Figure 59: System Information System Debug Log Page on S1200BTL Platforms

A list of data that may be captured using this feature includes but is not limited to:

- **Platform sensor readings** – This includes all “readable” sensors that can be accessed by the BMC FW and have associated SDRs populated in the SDR repository. This does not include any “event-only” sensors. (All BIOS sensors and some BMC and ME sensors

are “event-only”, meaning that they are not readable using an IPMI *Get Sensor Reading* command but rather are used just for event logging purposes.)

- **SEL** – The current SEL contents are saved in both hexadecimal and text format.
- **CPU/memory register data useful for diagnosing the cause of the following system errors: CATERR, ERR[2], SMI timeout, PERR, and SERR** – The debug data is saved and timestamped for the last three occurrences of the error conditions.
    - PCI error registers
    - MSR registers
    - Integrated Memory Controller (iMC) and Integrated I/O (IIO) module registers
- **BMC configuration data**
- **BMC FW debug log** (that is, SysLog) – Captures FW debug messages.

7.1.3.2 System Debug Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The System Debug Log page can be used to collect system debug information on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family. See Figure 60 for details.

Click the **Generate Log** button. It may take some time for the debug information to be collected.

After the debug log dump is finished, you can click the debug log filename to save the results as a .zip file on your client system. The file can then be sent to your system manufacturer or an Intel support engineer for analysis.

Figure 60: System Information System Debug Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

A list of data that may be captured using this feature includes but is not limited to:

- **Platform sensor readings** – This includes all "readable" sensors that can be accessed by the BMC FW and have associated SDRs populated in the SDR repository. This does not include any "event-only" sensors. (All BIOS sensors and some BMC and ME sensors are "event-only", meaning that they are not readable using an IPMI *Get Sensor Reading* command but rather are used just for event logging purposes.)

- **SEL** – The current SEL contents are saved in both hexadecimal and text format.

- **CPU/memory register data useful for diagnosing the cause of the following system errors: CATERR, ERR[2], SMI timeout, PERR, and SERR** – The debug data is saved and timestamped for the last three occurrences of the error conditions.

    - PCI error registers

    - MSR registers

    - Integrated Memory Controller (iMC) and Integrated I/O (IIO) module registers

- **BMC configuration data**

- **BMC FW debug log** (that is, SysLog) – Captures FW debug messages.

- **SMBIOS table data** – The entire SMBIOS table is captured from the last boot.

- **System memory map** – The system memory map is provided by BIOS on the current boot. This includes the EFI memory map and the Legacy (E820) memory map depending on the current boot.

- **Capture of power supply data and power supply asset information** – Power supply vendors are adding the capability to store debug data within the power supply itself. The platform debug feature provides a means to capture this data for each installed power supply. The data can be analyzed by Intel for failure analysis and possibly provided to the power supply vendor as well. The BMC gets this data from the power supplies by using PMBus* manufacturer-specific commands.

- **POST code sequence for the two most recent boots** – This is a best-effort data collection by the BMC as the BMC real-time response cannot guarantee that all POST codes are captured.

- **Support for multiple debug files** – The platform debug feature provides the ability to save data to two separate files that are encrypted with different passwords.

    - *System Debug Log* file can be viewed by Intel engineers and Intel partners.

    - *System and BMC Debug Log* file is strictly for viewing by Intel engineers and may contain additional BMC log messages and other debug data that Intel firmware developers deem useful in addition to the data specified above.

7.1.4 DIMM Information Page

The DIMM Information page displays information on DIMM modules installed on the host system. See Figure 61 for details.

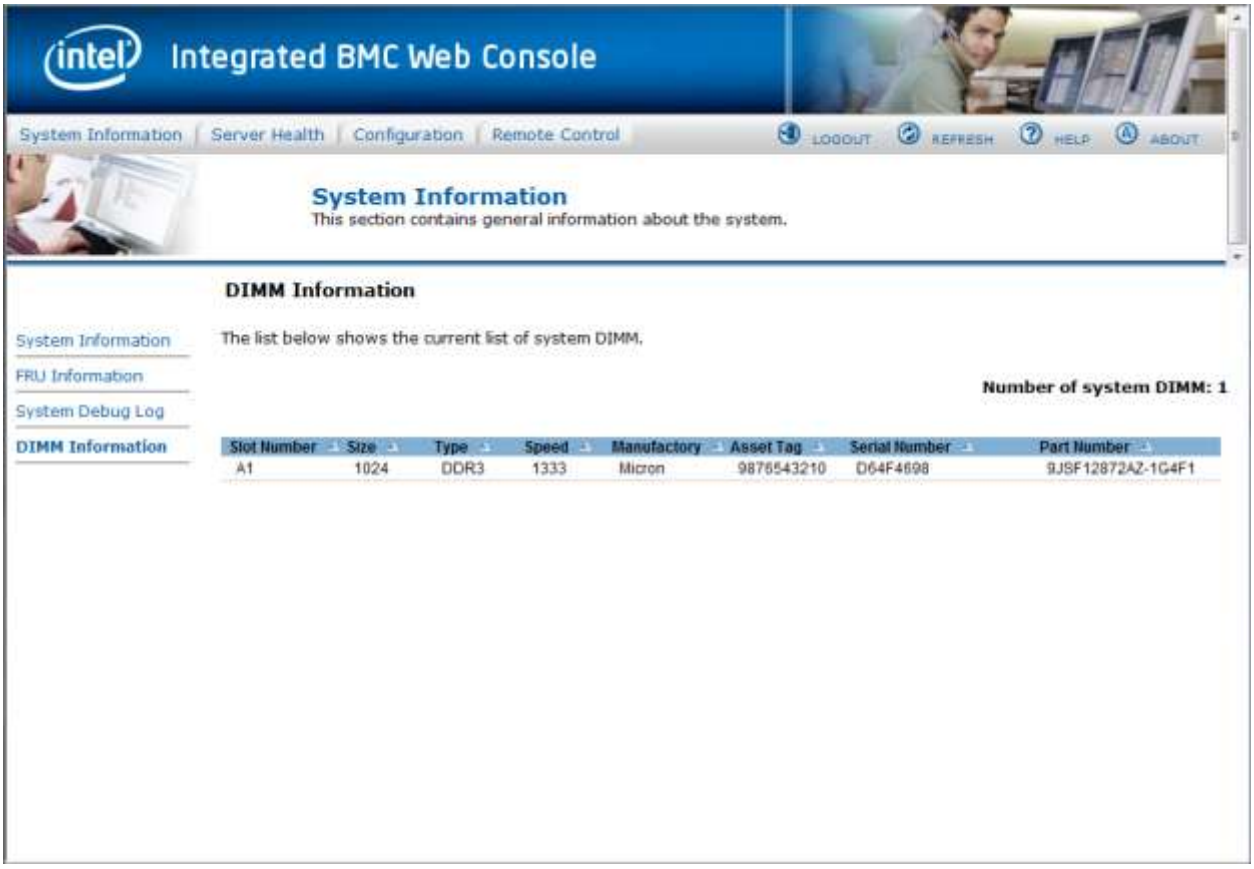


Figure 61: System Information DIMM Information Page

7.1.5 CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The CPU Information page displays information on the processors that are installed on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family. See Figure 62 for details.

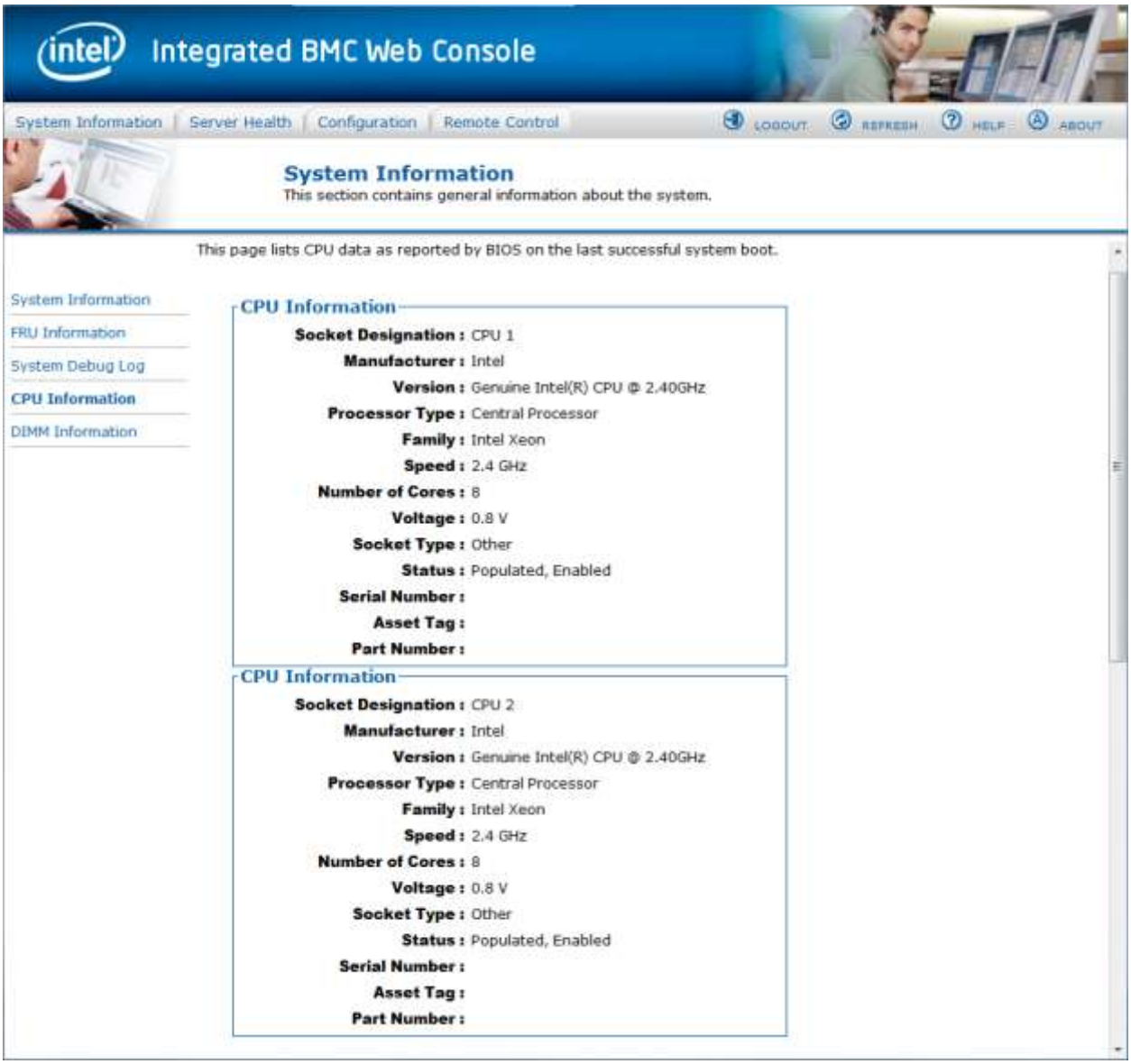


Figure 62: System Information CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

7.1.6 Current Users Page on S1200V3RP Product Family

The Current Users page shows users currently logged in to the BMC via the embedded web server, IPMI 1.5, or IPMI 2.0 session.

Web sessions over a secure socket layer (SSL) are denoted by "Secure" in parentheses.

The number of active KVM sessions opened by a "Web" user is noted in parentheses after the KVM notation.

Figure 63: Current Users Page on S1200V3RP Product Family

7.2 Server Health Tab

The **Server Health** tab shows you data related to the server's health, such as sensor readings, the event log, and power statistics as explained in the following sub sections.

Click the **Server Health** tab to select the various pages. By default, this tab opens the Sensor Readings page.

7.2.1 Sensor Readings Page

The Sensor Readings page displays system sensor information including status, health, and reading as shown in Figure 64 and Figure 65.

By default, the sensor readings are updated every 60 seconds but this can be changed by entering a value in the **Set auto-refresh in seconds** selection box and then clicking the **Set** button.

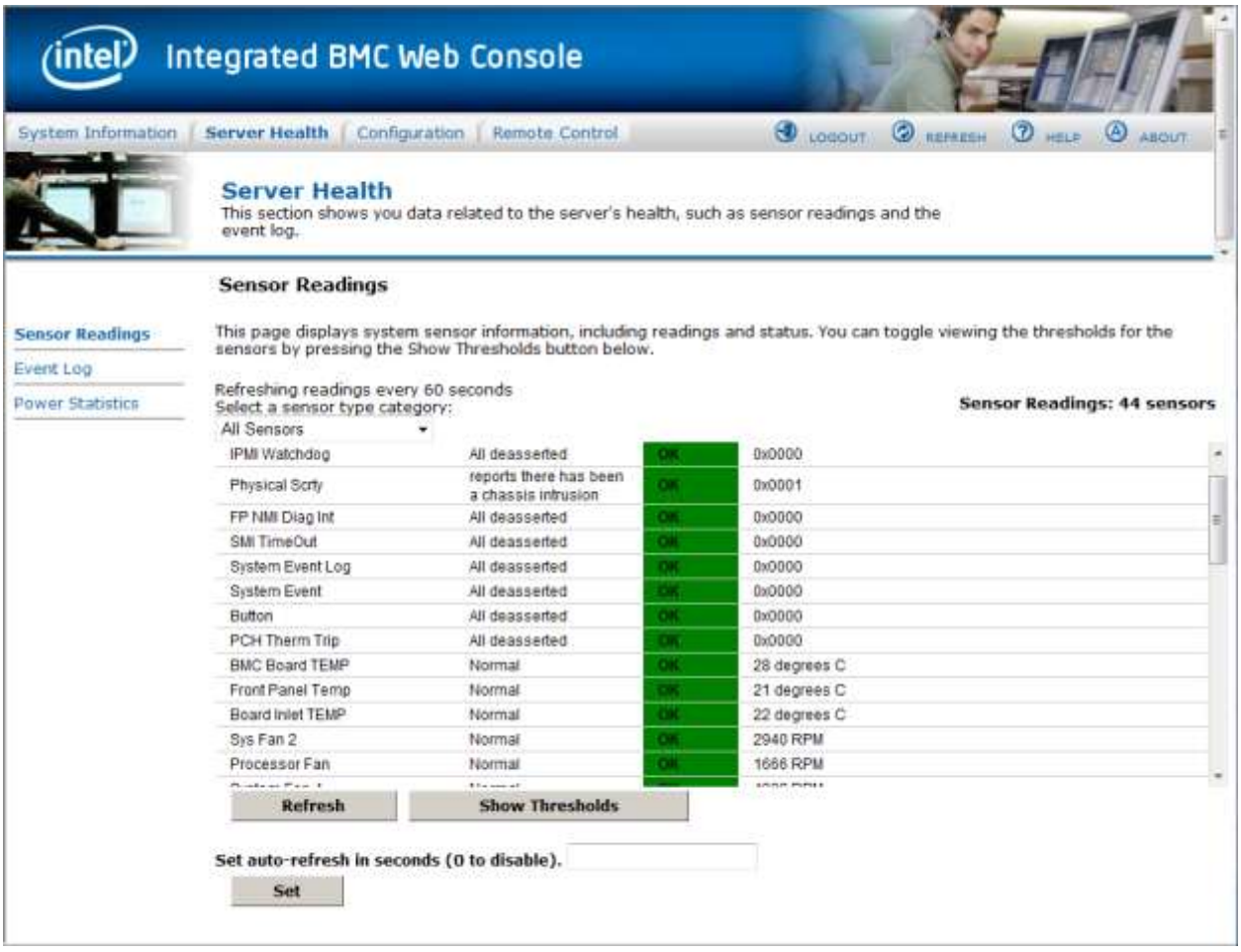


Figure 64: Server Health Sensor Readings Page (Thresholds not Displayed)

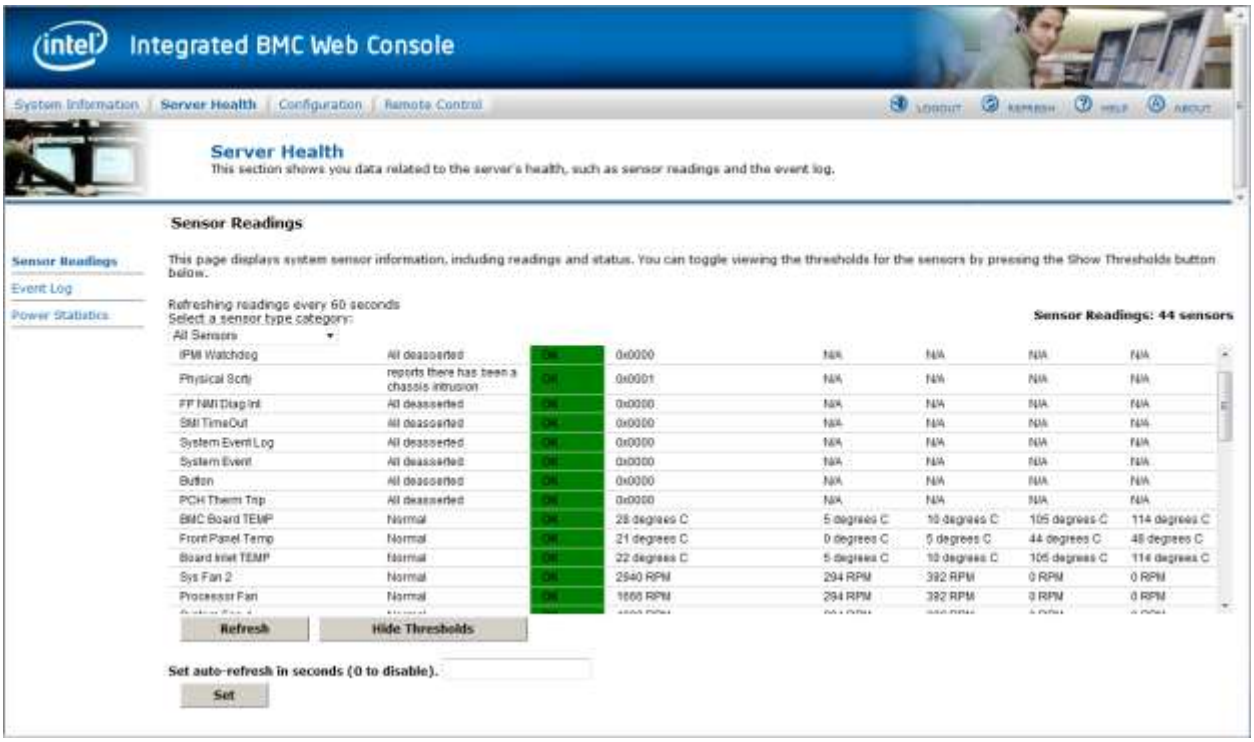


Figure 65: Server Health Sensor Readings Page (Thresholds Displayed)

The following table lists the options available in this page.

Table 12: Server Health Sensor Readings Options

Option	Task
Sensor Selection pull-down box	Select the type of sensor readings to display in the list. The default is to display all sensors.
Sensor Readings list	Selected sensors shown with their name, status, health, and readings.
Refresh button	Click to refresh the selected sensor readings.
Show Thresholds button	Click to expand the list, showing low and high threshold assignments. Shows the critical (CT) and non-critical (NC) thresholds for the selected sensors. Use scroll bar at the bottom to move the display left and right.
Hide Thresholds button	Click to return to the original display, hiding the threshold values.
Set auto-refresh in seconds (0 to disable) selection	Enter the time (in seconds) to wait between updates of the Sensor Readings and then click the **Set** button.

7.2.2 Event Log Page

The Event Log page displays the systems server management Event Log. Figure 66 shows the details for an S1200BTL system.

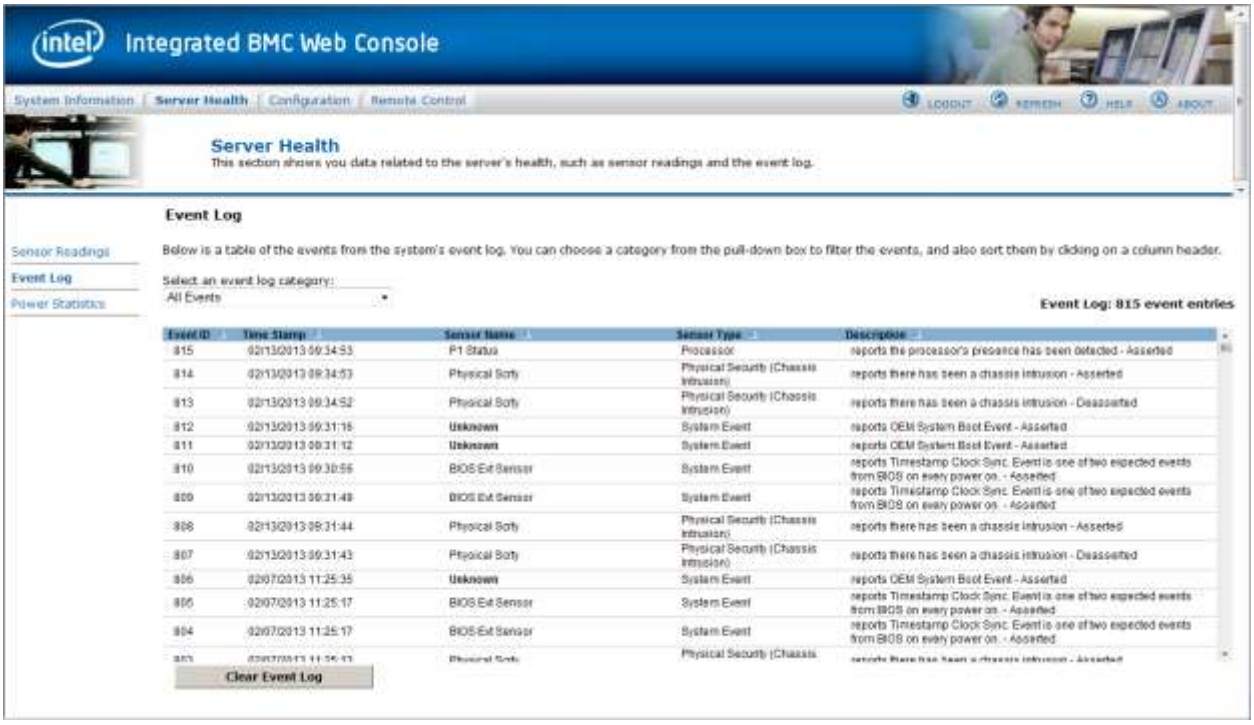


Figure 66: Server Health Event Log Page on S1200BTL Platforms

The following table lists the options available in this page.

Table 13: Server Health Event Log Options on S1200BTL Platforms

Option	Task
Event Log Category pull-down box	Select the type of events to display in the list.
Event Log List	Selected sensors are shown with their name, status, and readings. This includes a list of the events with their ID, time stamp, sensor name, sensor type, and description.
Clear Event Log button	Click to clear the event logs.

On an EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you also get a **Save Event Log** button. See Figure 67 for details.

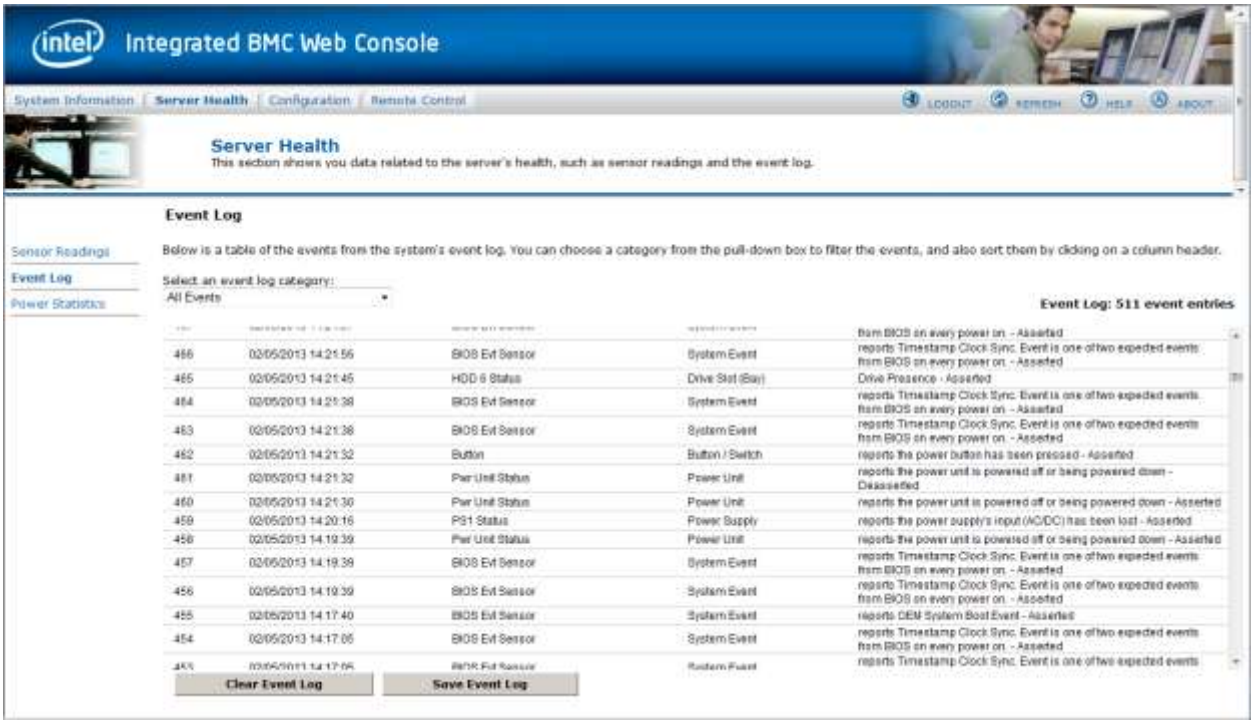


Figure 67: Server Health Event Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

On S1200V3RP Product Family there is an indicator towards the top of the page that gives an indication of how full the Event Log is. In addition towards the bottom of the page a selection is added that allows you to select going to another page of the recorded events. The selection is plus and/or minus two pages from the current page and a selection to go to the first and/or the last page of events.

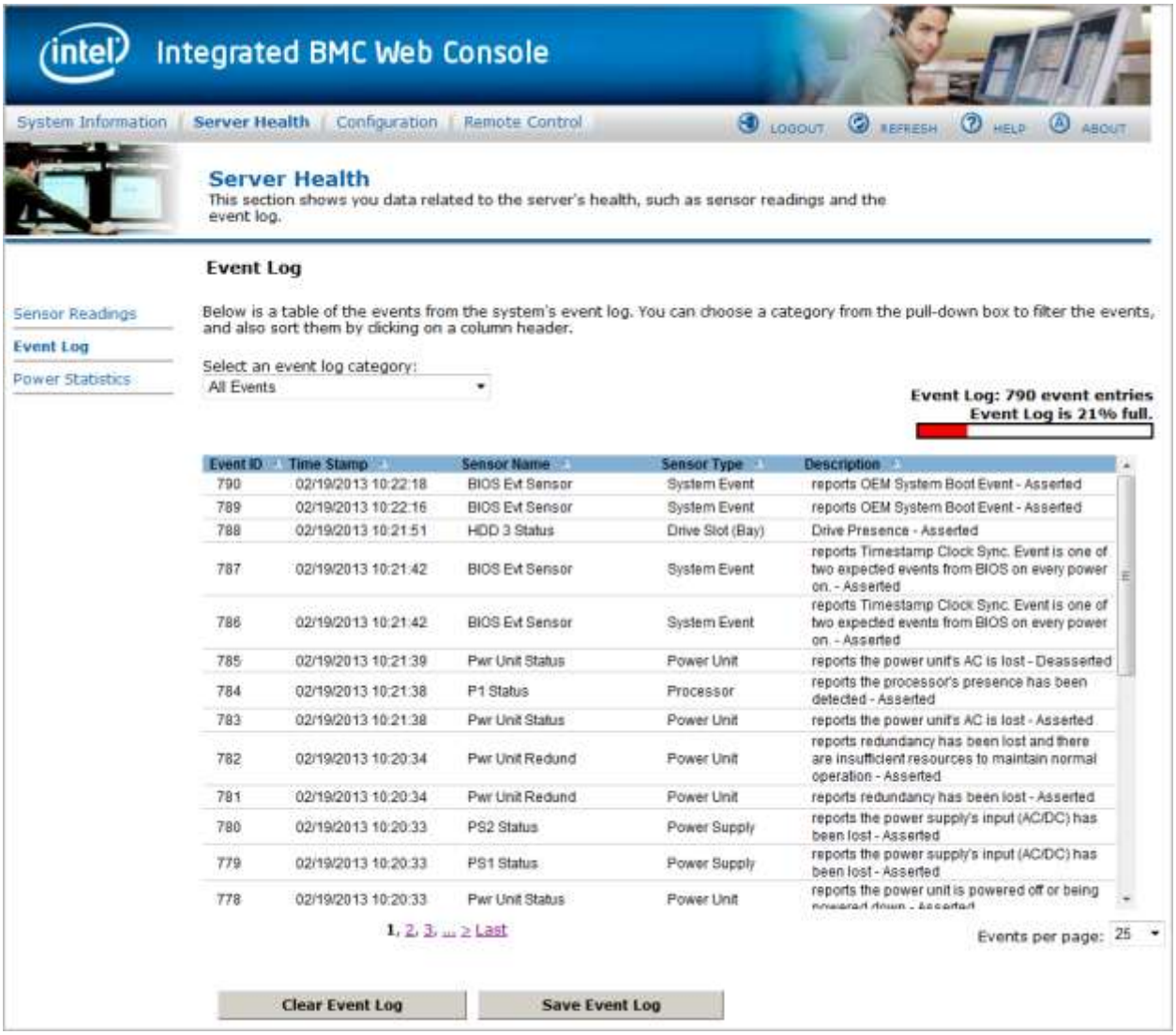


Figure 68: Server Health Event Log Page on S1200V3RP Product Family

7.2.3 Power Statistics Page

The Power Statistics page displays the systems power statistics in watts as shown in Figure 69.

Figure 69: Server Health Power Statistics Page on S1200BTL Platforms and S1200V3RP Product Family

On an EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you can see the length of time that the statistics have been getting collected. See Figure 70 for details.

Figure 70: Server Health Power Statistic Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.3 Configuration Tab

The **Configuration** tab is used to configure various settings such as IPv4 Network, Users Login, LDAP SSL, Remote Session, Mouse Mode, Keyboard Macros, Alerts, and Alert Email as discussed in the following subsections. In addition, EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families IPv6, VLAN, and Node Manager can also be configured.

Click the **Configuration** tab to select the various pages. By default, this tab opens the Network Settings page or the IPv4 Network page.

7.3.1 Network or IPv4 Network Page

The Network or IPv4 settings page is used to configure the IPv4 network settings for the server management LAN interface to the BMC controller. See Figure 71 or Figure 72 for details.

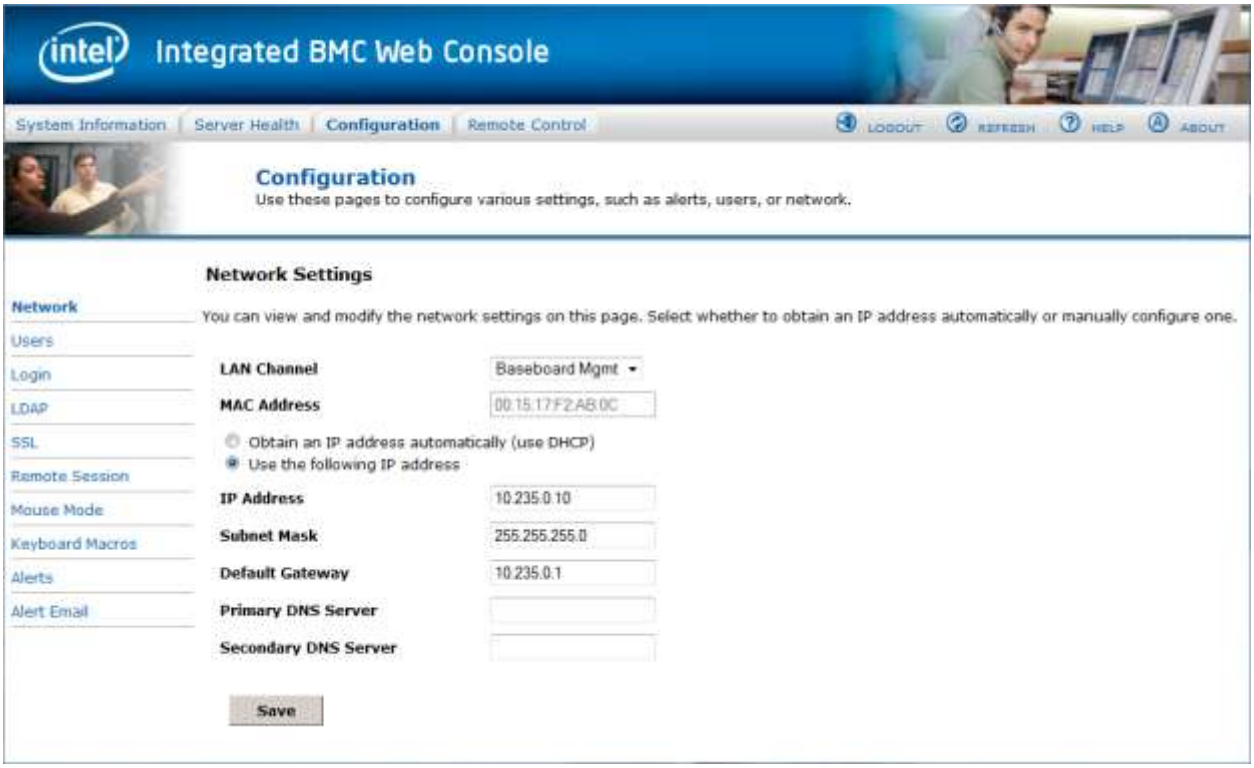


Figure 71: Configuration Network Settings Page on S1200BTL Platforms

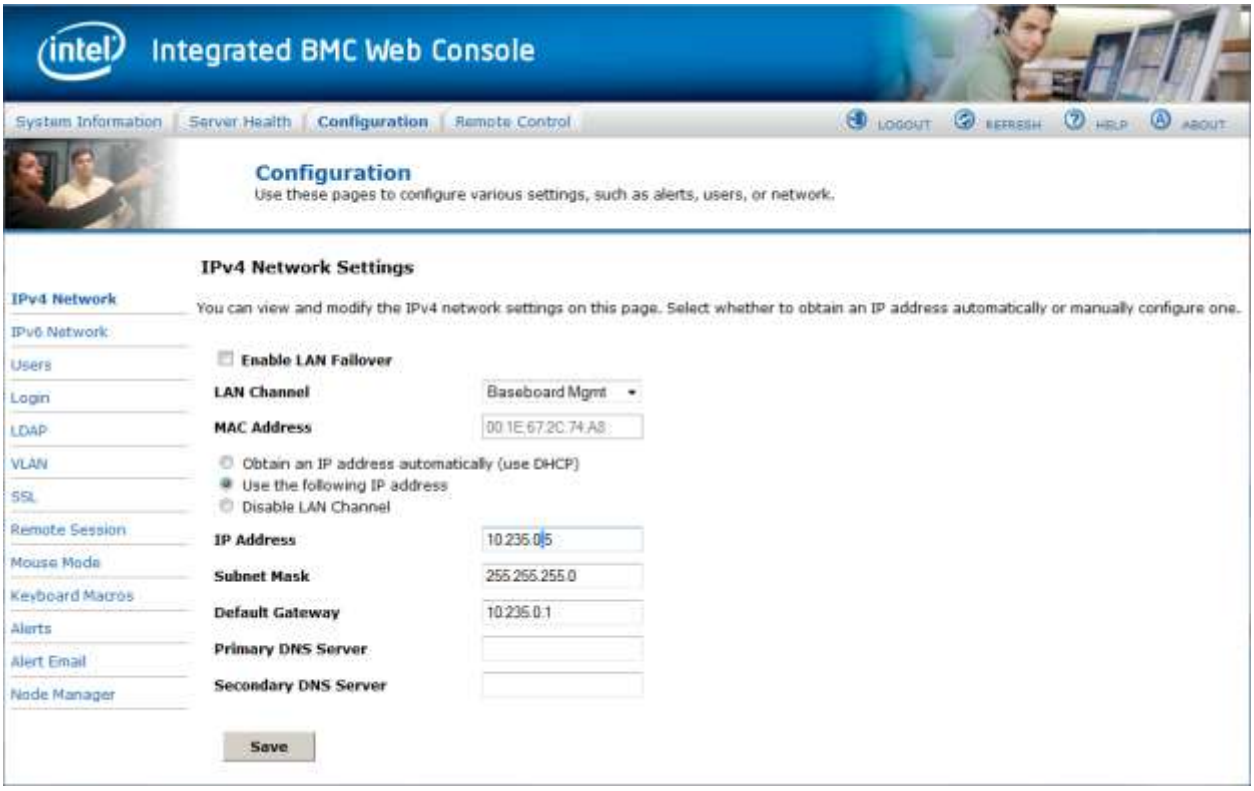


Figure 72: Configuration IPv4 Network Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

⚠ WARNING

Each network controller must be on a different subnet than all other controllers used for management traffic.

⚠ WARNING

When LAN failover is enabled, the system administrator must ensure that each network controller connection, which can be seen by the BMC, has connectivity to the same networks. If there is a loss of functionality on the primary network controller channel, it will randomly failover to any of the other network controller channels that are connected and seen by the BMC.

The following table lists the options available in this page.

Table 14: Configuration IPv4 Network Settings Options

Option	Task
Enable LAN Failover	Used to enable LAN Failover (only available on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families).

Option	Task
LAN Channel drop-down box	Used to select the channel on which you want to configure the network settings. Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server. • Intel(R) RMM (BMC LAN Channel 3) is the add-in RMM4 Dedicated Management NIC. • Baseboard Mgmt (BMC LAN Channel 1) is the on-board, shared NIC configured for management and shared with the operating system. • Baseboard Mgmt 2 (BMC LAN Channel 2) is the second on-board, shared NIC configured for management and shared with the operating system.
MAC Address	The MAC address of the device (read only).
IP address radio buttons	Select one of the three options for configuring the IP address: • Obtain an IP address automatically (use DHCP) – Uses DHCP to obtain the IP address. • Use the following IP address – Manually configure the IP address. • Disable LAN Channel – Sets the IP address, Subnet Mask, and Default Gateway to 0.0.0.0.
IP Address **Subnet Mask** **Gateway**	If configuring a static IP, enter the requested address, subnet mask, and gateway in the given fields. The IP Address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". 'xxx' ranges from 0 to 255. First 'xxx' must not be 0.
Primary DNS Server **Secondary DNS Server**	If configuring a dynamic IP, enter the Primary and Secondary DNS servers.
Save button	Click to save any changes made.

7.3.2 IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The IPv6 settings page is used to enable and configure the IPv6 network settings. You can also enable and configure LAN Failover on this page. See Figure 73 for details.

Figure 73: Configuration IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

⚠ WARNING

Each network controller must be on a different subnet than all other controllers used for management traffic.

⚠ WARNING

When LAN failover is enabled, the system administrator must ensure that each network controller connection, which can be seen by the BMC, has connectivity to the same networks. If there is a loss of functionality on the primary network controller channel, it will randomly failover to any of the other network controller channels that are connected and seen by the BMC.

The following table lists the options available in this page.

Table 15: Configuration IPv6 Network Settings Options

Option	Task
Enable LAN Failover	Used to enable LAN Failover.
LAN Channel drop-down box	Used to select the channel on which you want to configure the network settings. Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server. • Intel(R) RMM (BMC LAN Channel 3) is the add-in RMM4 Dedicated Management NIC. • Baseboard Mgmt (BMC LAN Channel 1) is the on-board, shared NIC configured for management and shared with the operating system. • Baseboard Mgmt 2 (BMC LAN Channel 2) is the second on-board, shared NIC configured for management and shared with the operating system.
MAC Address	The MAC address of the device (read only).
Enable IPv6 on this channel selection box	Used to enable IPv6 on the channel selected in the **LAN Channel** drop-down box.
IP address radio buttons	Select one of the three options for configuring the IP address: • Use IPv6 auto-configuration (stateless ICMPv6 discovery) – Uses ICMPv6 to obtain the IP address. • Obtain an IP address automatically (use DHCPv6) – Uses DHCPv6 to obtain the IP address. • Use the following IP address – Manually configure the IP address.
IP Address **Gateway**	If configuring a static IP, enter the requested address and gateway in the given fields. The IP Address and Gateway are 128-bit fields made of eight hexadecimal numbers separated by colons as in "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx". 'xxxx' ranges from 0 to FFFF. First 'xxxx' must not be 0. One or more consecutive groups of zero value may be replaced with a single empty group using two consecutive colons (`::`).
IPv6 prefix length (0 to 128)	Select the routing prefix length.
Save button	Click to save any changes made.

7.3.3 Users Page

The User List page lists the configured users, along with their status and network privilege. It also provides the capability to add, modify, and delete users. See Figure 74 for details.

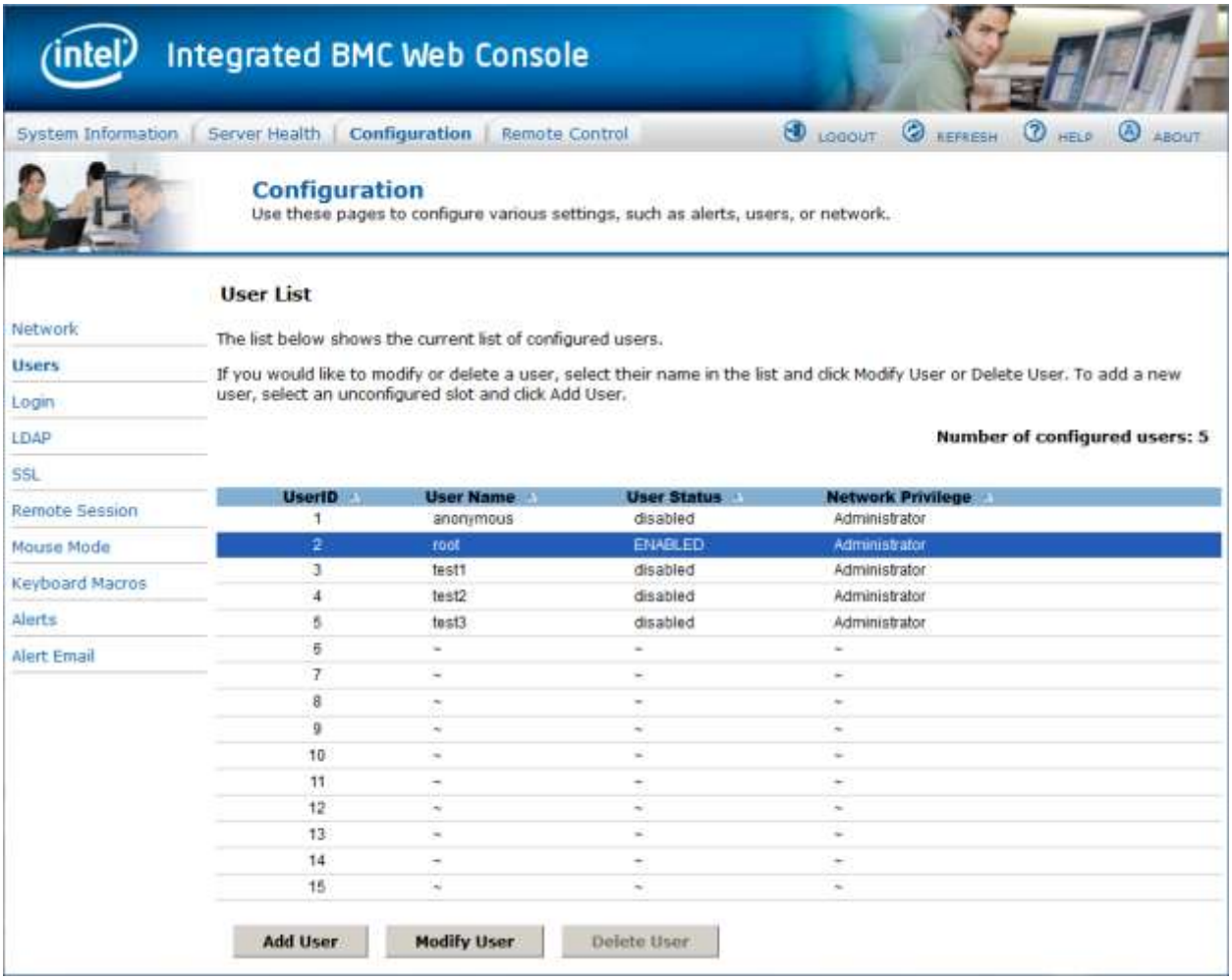


Figure 74: Configuration User List Page

This page allows the operator to configure the IPMI users and privileges for this server:

- UserID 1 (anonymous) may not be renamed or deleted.
- UserID 2 (root) may not be renamed or deleted, nor can the network privileges of UserID 2 be changed.
- User Names cannot be changed. To rename a user you must first delete the existing user, and then add the user with the new name.

To delete a user, select the user in the list and click **Delete User**.

To add a user, select an empty slot in the list and click **Add User**. This allows you to set the User Name, Password, and Network Privileges as shown in Figure 75.

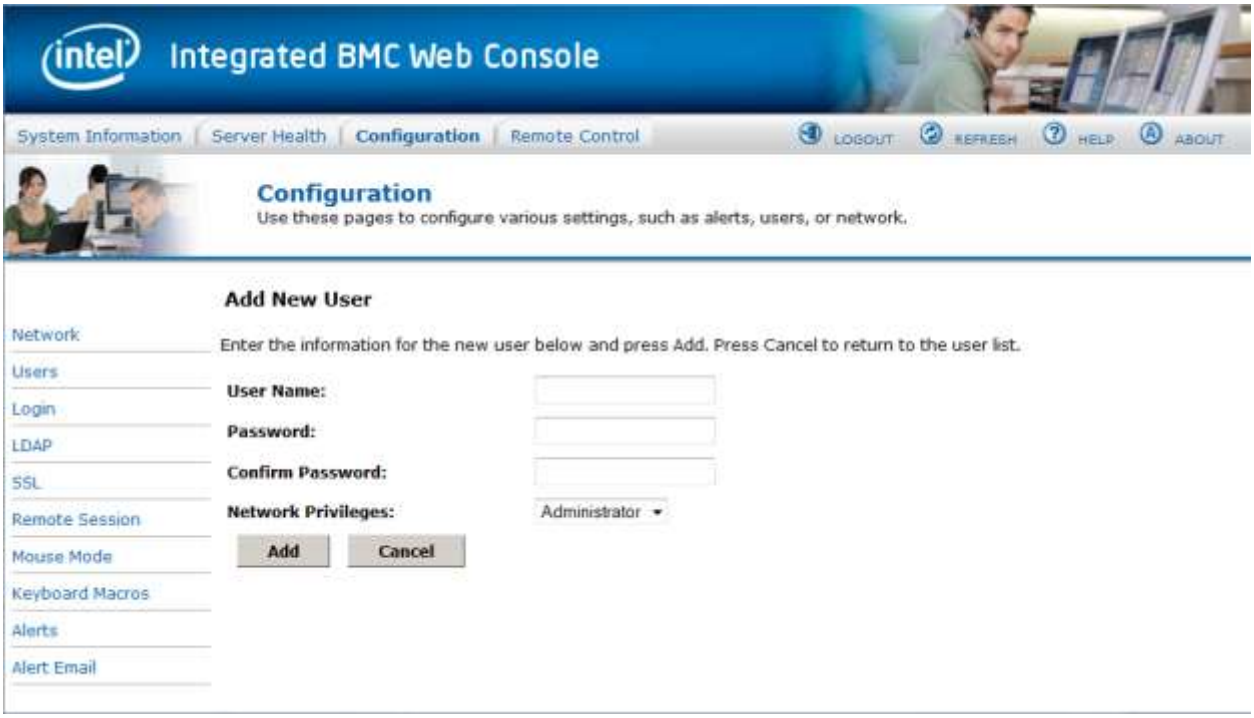


Figure 75: Configuration Users Add User Page

To modify a user, select a user in the list and click **Modify User**. This allows you to change the Password, Enable Access, and change Network Privileges as shown in Figure 76.

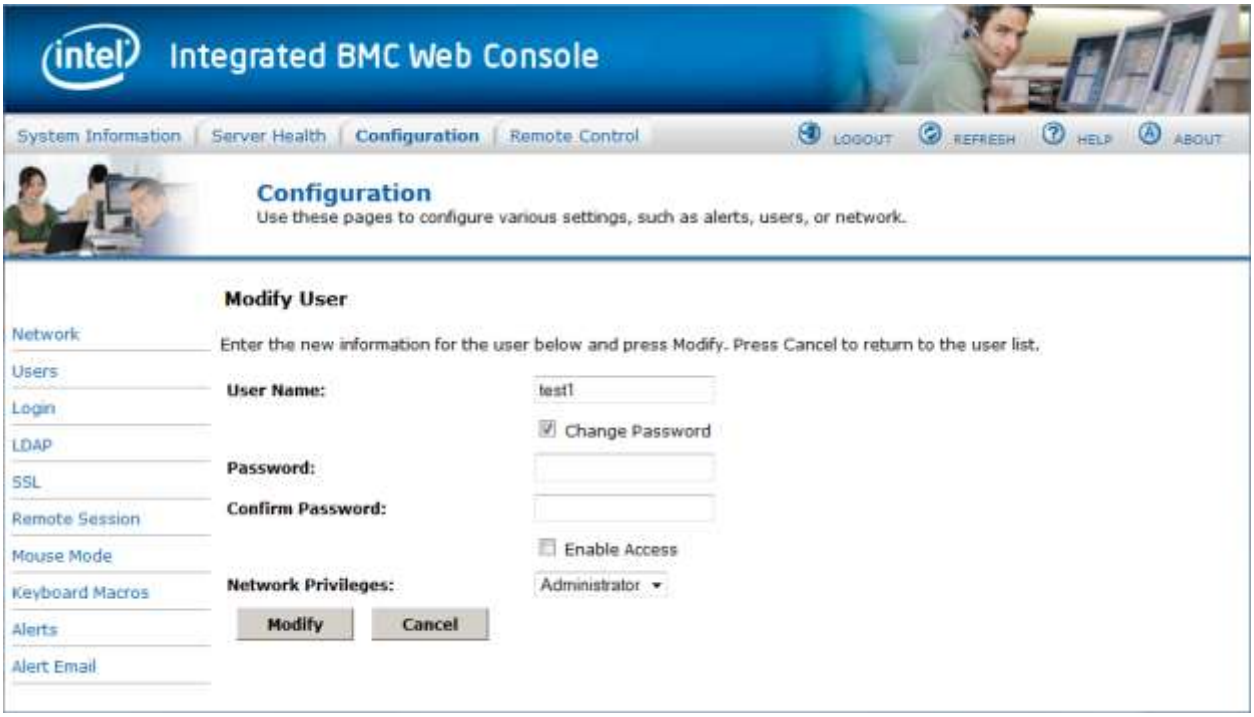


Figure 76: Configuration Users Modify User Page

7.3.4 Login Security Settings Page

Users can be locked out if they supply incorrect passwords too many times in a row. This is a security feature to prevent brute force hacking attacks. Only that user is locked out – other users can still login.

The number of failed attempts before being locked out is configurable; as is the length of time the lockout lasts.

To turn the feature off, set the lockout time to zero. Three default failures will lock out a user for one minute.

Click the **Save** button to save any changes.

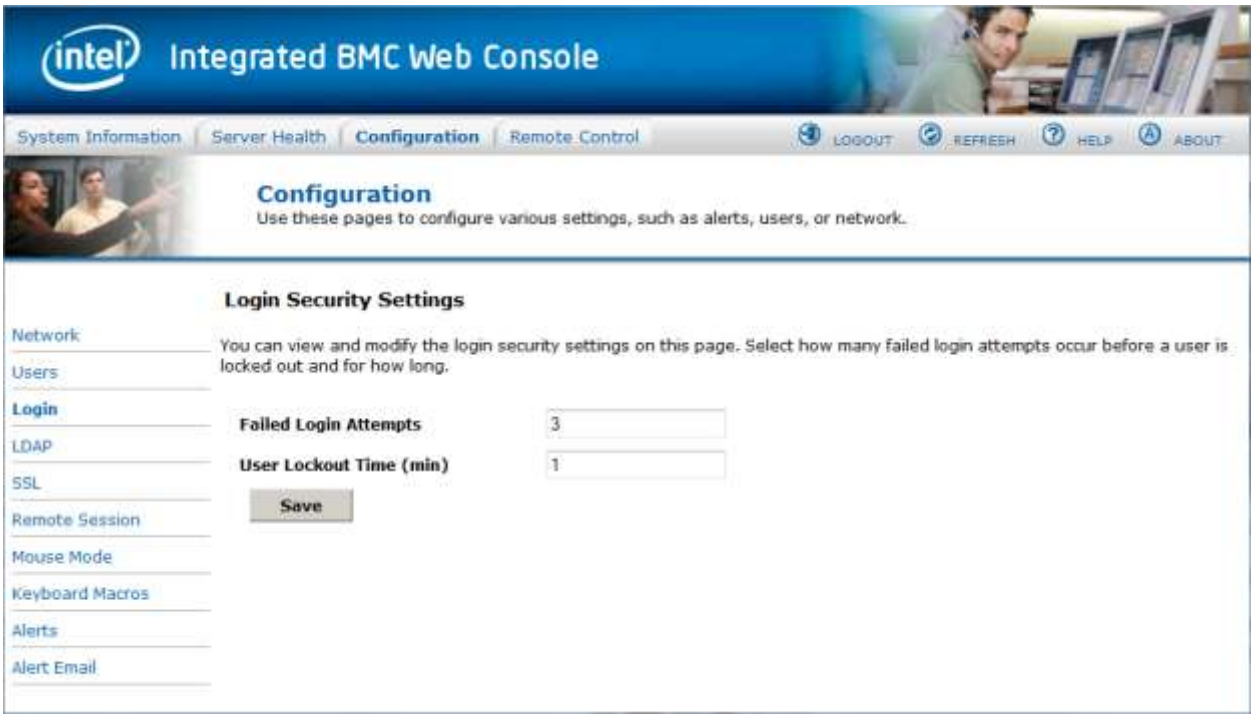


Figure 77: Configuration Login Security Settings Page on S1200BTL Platforms

For EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family you can also force the interface to HTTP Secure mode by selecting the **Force HTTPS** – **Enable** checkbox. See Figure 78 for details.

In addition the **Web Session Timeout** that locks the web session after a specified time of inactivity can be changed from the default 30 minutes (1800 seconds) by entering a new value for how long to wait before locking out the web session.

Click the **Save** button to save any changes.

Figure 78: Configuration Login Security Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

7.3.5 LDAP Settings Page

To enable/disable LDAP, check or uncheck the **Enable LDAP Authentication** checkbox respectively.

Figure 79: Configuration LDAP Settings Page

The following table lists the options available in this page.

Table 16: Configuration LDAP Settings Options

Option	Task
Enable LDAP Authentication	Check this box to enable LDAP authentication, then enter the required information to access the LDAP server.
Port	Specify the LDAP port.
IP Address	The IP address of LDAP server. The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". 'xxx' ranges from 0 to 255. First 'xxx' must not be 0.
Searchbase	The searchbase of the LDAP server, for example, "dc=my-domain, dc=com".
Bind Password	The authentication password for the LDAP server; the password must be at least four characters long.
Bind DN	The Distinguished Name of the LDAP server, for example, "cn=Manager, dc=my-domain, dc=com".
Save button	Click to save the current settings.

7.3.6 VLAN Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family this page is used to enable and configure the VLAN private network settings on the selected server management LAN channels.

Figure 80: Configuration VLAN Settings on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The following table lists the options available in this page.

Table 17: Configuration VLAN Settings Options

Option	Task
LAN Channel drop-down box	Used to select the channel on which you want to configure the network settings. Lists the LAN Channels available for VLAN. The LAN channel describes the physical NIC connection on the server. • Intel(R) RMM (BMC LAN Channel 3) is the add-in RMM4 NIC. • Baseboard Mgmt (BMC LAN Channel 1) is the on-board, shared NIC configured for management and shared with the operating system. • Baseboard Mgmt 2 (BMC LAN Channel 2) is the second on-board, shared NIC configured for management and shared with the operating system.
Enable VLAN	Used to enable VLAN for the LAN channel selected in the drop-down box.
VLAN ID (1 – 4094)	Used to set the VLAN ID.

Option	Task
VLAN Priority (0 – 7)	Used to set the VLAN priority.
Save button	Click to save the current settings.

7.3.7 SSL Upload Page

Use this page to upload an SSL certificate and privacy key, which allows the device to be accessed in a secured mode.

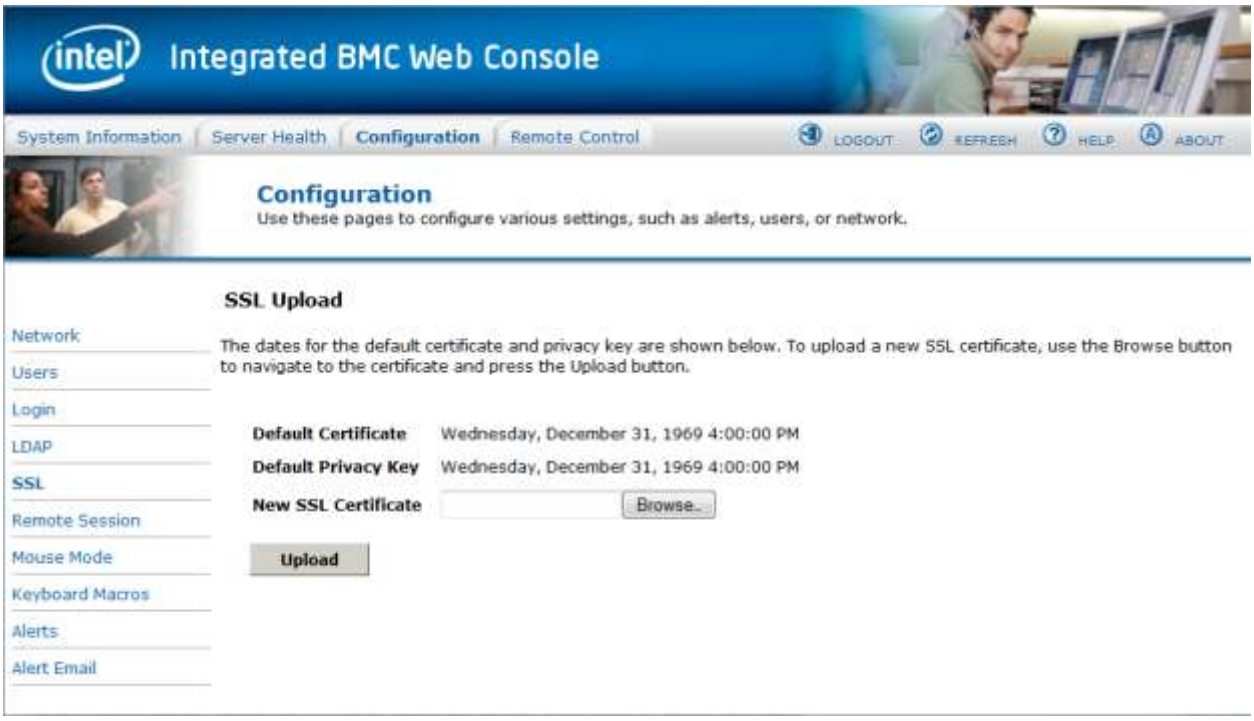


Figure 81: Configuration SSL Upload Page

First upload the SSL certificate and then the device will prompt to upload the privacy key. If either of the files is invalid, the device will notify. A notification will be displayed on successful upload. On successful upload, the device will prompt to reboot. If you want to reboot, click **Ok**. Or click **Cancel** to cancel the reboot operation.

First upload the SSL certificate and then the device will prompt to upload the privacy key. Click the **Upload** button. On successful upload, a notification appears.

7.3.8 Remote Session Page

Use this page to configure various settings for the remote sessions.

7.3.8.1 Remote Session Page on S1200BTL Platforms

Use this page to enable/disable encryption on KVM or Media during a redirection session and to select USB Key Emulation Type. Figure 82 shows the details for an S1200BTL system.

Figure 82: Configuration Remote Session Page on S1200BTL Platforms

The following table lists the options allowing you to enable or disable encryption on KVM or media data, and the USB Key Emulation type selection used during a redirection session.

Table 18: Configuration Remote Session Options

Option	Task
Enable KVM Encryption **Enable Media Encryption**	Enable/Disable encryption on KVM or Media data during a redirection session. **Note**: KVM and Media encryption are enabled by default. **Note**: Disabling encryption can improve performance of KVM or Media redirection.
USB Key Emulation Type	Select Floppy or Hard Disk emulation.

Option	Task
Port Forwarding	Only needs to be configured if there is NAT (Network Address Translation) or port forwarding on your network between the client side (web browser and JViewer application) and the BMC side. Enter the browser-side port number (1024-65535) for each of the redirection services (remote KVM, virtual CDROM, and virtual USB/Floppy) that the JVIewer client should use. If left blank, JViewer assumes no translation and uses the BMCs standard ports: 7578, 5120, 5123 (unencrypted) or else 7582, 5124, 5127 (encrypted) for remote KVM, virtual CDROM, and virtual USB/Floppy, respectively. The client-side IP address and http/https port numbers are supplied automatically by the browser and do not need to be configured.
Save button	Click to save any changes.

7.3.8.2 Remote Session Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

On EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families you can select the encryption mode and separately enable or disable the keyboard or mouse and media encryption. The ports used for Port Forwarding can also be selected. See Figure 83 for details.

Figure 83: Configuration Remote Session Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The following table lists the options that can be used to configure the settings used during a redirection session.

Table 19: Configuration Remote Session Options

Option	Task
KVM Encryption mode	Disable or select encryption mode on KVM or Media data during a redirection session. Choose any one from the supported encryption techniques (None, Stunnel*, RC4, or AES). **Note**: KVM and Media encryption are enabled by default. **Note**: Disabling encryption can improve performance of KVM or Media redirection.
Keyboard/Mouse Only	If KVM Encryption is set to None, the Keyboard and Mouse data can still be encrypted using Blowfish encryption. **Note**: This option has the least performance impact while still encrypting the most important data.
Media Encryption	Enable/Disable encryption of Media data during a redirection session. **Note:** Disabling encryption can improve performance of KVM or Media redirection.
USB Key Emulation Type	Select Floppy or Hard Disk emulation.
Port Forwarding	Only needs to be configured if there is NAT (Network Address Translation) or port forwarding on your network between the client side (web browser and JViewer application) and the BMC side. Enter the browser-side port number (1024-65535) for each of the redirection services (remote KVM, virtual CDROM, and virtual USB/Floppy) that the JVIewer client should use. If left blank, JViewer assumes no translation and uses the BMCs standard ports: 7578, 5120, 5123 (unencrypted) or else 7582, 5124, 5127 (encrypted) for remote KVM, virtual CDROM, and virtual USB/Floppy, respectively. The client-side IP address and http/https port numbers are supplied automatically by the browser and do not need to be configured.
Save button	Click to save any changes.

7.3.8.3 Remote Session Page on S1200V3RP Product Family

On an S1200V3RP Product Family system you can select the encryption mode and separately enable or disable the keyboard or mouse and media encryption. The ports used for Port Forwarding can also be selected. There is also a selection for enabling Serial Over LAN on the various LAN ports. See Figure 84 for details.

Figure 84: Configuration Remote Session Page on S1200V3RP Product Family

The following table lists the options that can be used to configure the settings used during a redirection session.

Table 20: Configuration Remote Session Options on S1200V3RP Product Family

Option	Task
KVM Encryption mode	Disable or select encryption mode on KVM or Media data during a redirection session. Choose any one from the supported encryption techniques (None, Stunnel*, RC4, or AES) **Note**: KVM and Media encryption are enabled by default. **Note**: Disabling encryption can improve performance of KVM or Media redirection.
Keyboard/Mouse Only	If KVM Encryption is set to None, the Keyboard and Mouse data can still be encrypted using Blowfish encryption. **Note**: This option has the least performance impact while still encrypting the most important data.
Media Encryption	Enable/Disable encryption of Media data during a redirection session. **Note:** Disabling encryption can improve performance of KVM or Media redirection.
USB Key Emulation Type	Select Floppy or Hard Disk emulation.

Option	Task
Serial Over LAN • **Enable SOL for Baseboard Mgmt** • **Enable SOL for Baseboard Mgmt 2** • **Enable SOL for Intel(R) RMM**	Enable or disable Serial Over LAN for each LAN channel. Enable Console Redirection in BIOS Setup before activating SOL sessions; otherwise SOL will not be functional.
Port Forwarding	Only needs to be configured if there is NAT (Network Address Translation) or port forwarding on your network between the client side (web browser and JViewer application) and the BMC side. Enter the browser-side port number (1024-65535) for each of the redirection services (remote KVM, virtual CDROM, and virtual USB/Floppy) that the JVIewer client should use. If left blank, JViewer assumes no translation and uses the BMCs standard ports: 7578, 5120, 5123 (unencrypted) or else 7582, 5124, 5127 (encrypted) for remote KVM, virtual CDROM, and virtual USB/Floppy, respectively. The client-side IP address and http/https port numbers are supplied automatically by the browser and do not need to be configured.
Save button	Click to save any changes.

7.3.9 Mouse Mode Page

Use this page to select the Mouse Mode used during a Remote KVM session.

On an S1200BTL system the Redirection Console handles mouse emulation from local window to remote screen in either of two methods. Figure 85 shows the details.

- **Absolute Mode**. Select Absolute Mode to have the absolute position of the local mouse sent to the server. Use this mode for Microsoft Windows* OS.
- **Relative Mode**. Select Relative Mode to have the calculated relative mouse position displacement sent to the server. Use this mode for Linux* OS.

Click **Save** to use selected mode.

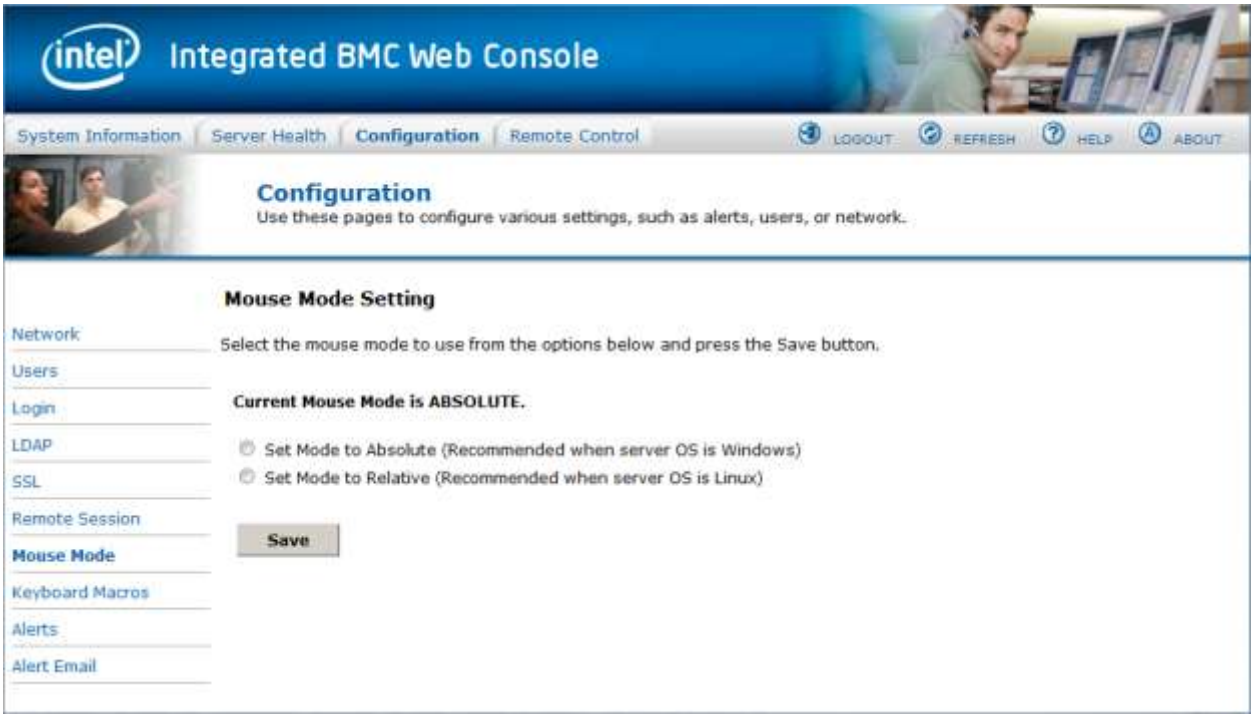


Figure 85: Configuration Mouse Mode Setting Page on S1200BTL Platforms

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family the Redirection Console handles mouse emulation from local window to remote screen in either of three methods. Figure 86 shows the details.

- **Absolute Mode**. Select Absolute Mode to have the absolute position of the local mouse sent to the server. Use this mode for Microsoft Windows* and newer Red Hat* Linux versions (RHEL 6.x).
- **Relative Mode**. Select Relative Mode to have the calculated relative mouse position displacement sent to the server. Use this mode for other Linux* versions such as SUSE* (SLES) and older versions of Red Hat* (RHEL 5.x). For best results, server OS mouse acceleration/threshold settings can be reduced, or use mouse calibration in the remote console window.

- **Other Mode**. Select Other Mode to have the calculated displacement from the local mouse in the center position, sent to the server. In this mode Alt+C can be used to switch between host and client mouse cursor. Use this mode for SLES 11 Linux* OS installation. See Section 7.3.9.1 for more details on this mode.

Click **Save** to use selected mode.

Figure 86: Configuration Mouse Mode Setting Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

7.3.9.1 Mouse Mode Setting – Other Mode Description

This mode should only be used for a SLES* 11 OS installation, and after this has been completed, the Mouse Mode Setting should be changed to the suggested Relative Mode for use within the SLES* 11 OS.

In this mode, the KVM window will be maximized to the full screen. Note that the windows resizing button in the top right corner is grayed out.

To use the mouse within the KVM window you must press Alt-C. The first time that Alt-C is pressed the mouse will appear close to the center of the window. Pressing Alt-C after that will switch between using the mouse within the KVM window and using the mouse on your host system. The mouse in the KVM window will remain in the last position that it was at when the operation is switched between the KVM Window, to the host system, and then back to the KVM window. There is a reminder of using Alt-C key in the Remote Console control bar to the left of

the keyboard macros. See Figure 87 for details. During installation, the mouse response in the KVM is slow. This is normal and expected.

Note: If the top bar of the KVM window is double clicked, the window will be resized. If this occurs, because there is no resize window button, the operator can use the Remote Console Control Bar to select Video and then perform a Full Screen (or press Alt-F) operation to go to the full screen mode.

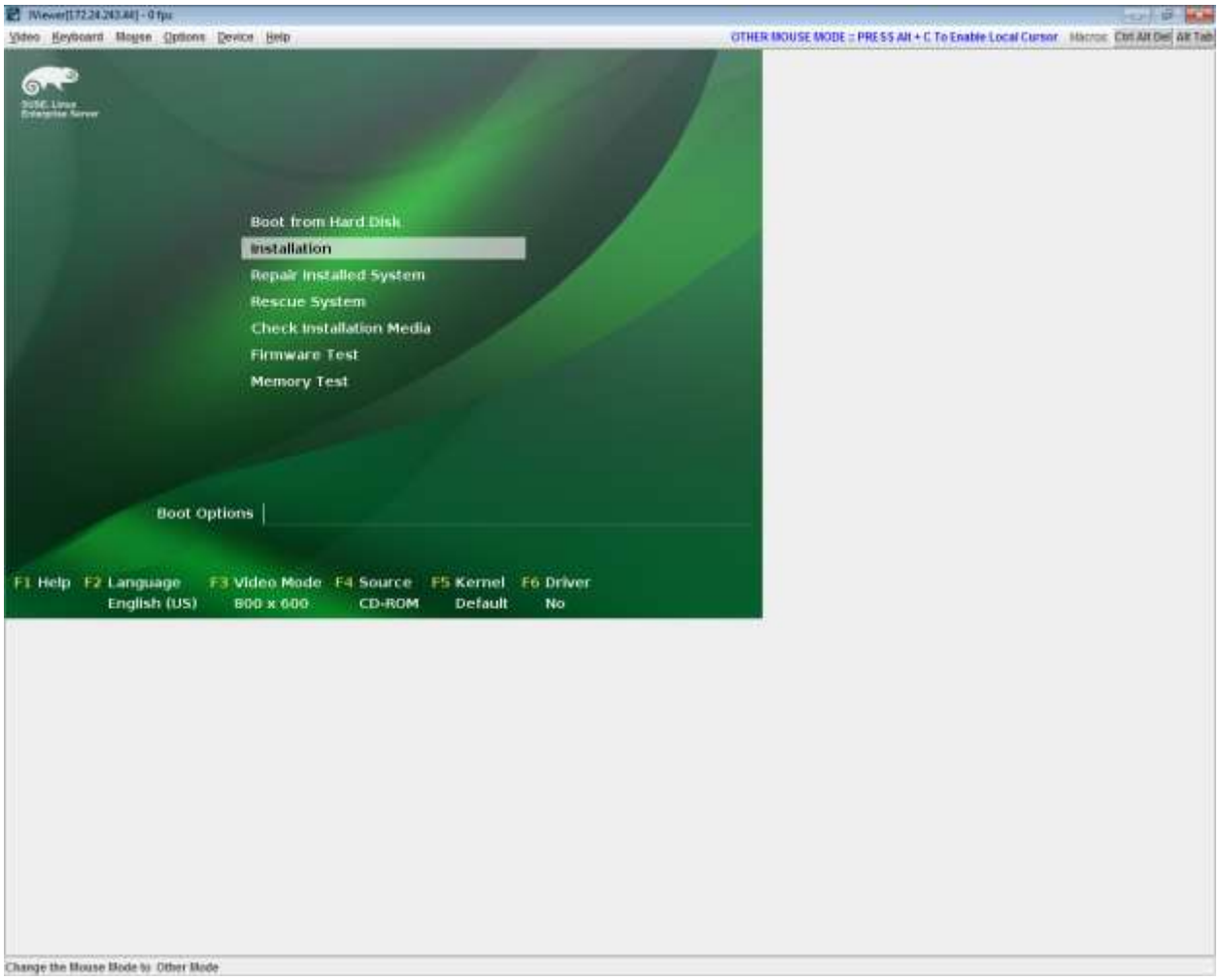


Figure 87: KVM Window with Mouse Other Mode Selected on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

7.3.10 Keyboard Macros Page

Macro buttons can be defined on this page that appear in the upper right corner of the KVM Remote Console application window. Each button is assigned a sequence of keys to execute when the button is clicked.

Figure 88: Configuration Keyboard Macros Page

This makes it convenient to quickly do oft repeated typing as well as execute key combos that are not possible directly from the local client keyboard. ‘Alt’ and ‘Win’ key combos such as Ctrl+Alt+Del are interpreted by the local client OS and are not passed through to the remote target OS. However, a macro can be set up to take care of this.

Each button can optionally be given a short mnemonic name. If this field is blank, the key sequence itself will also be used as the button label.

You must save changes before they take effect. If a Remote Console session is open at that time, you will not see the changes until that session is closed and a new session is opened.

7.3.10.1 Key Sequences

A key sequence is a set of one or more key names separated by a ‘+’ or ‘-’.

A '+' indicates keep the previous keys pressed while holding down the next key, whereas a '-' indicates release all previous keys first before pressing the next key. A '*' inserts a one second pause in the key sequence.

Key names are either a printable character such as a, 5, @, and so on or else one of the non-printable keys in the table below. Names in parentheses are aliases for the same key. Numeric keypad keys are prefixed with "NP_".

A plain '*' indicates a pause. Use '*' for the actual '*' key. The '\' key must also be escaped as '\\'.

Note: The key sequences are sent to the target as scan codes that get interpreted by the target OS, so they will be affected by modifiers such as Num Lock as well as the target OS keyboard language setting.

Table 21: Macro Non-printable Key Names

Shift (LShift)	RShift	Ctrl (LCtrl)	RCtrl
Alt (LAlt)	RAlt (AltGr)	Win (LWin)	RWin
Enter	Esc	F1 - F12	
Bksp	Tab	CapsLk	Space
Ins	Del	Home	End
PgUp	PgDn	Context (Menu)	
Up	Left	Down	Right
NumLk	NP_Div	NP_Mult	NP_Minus
NP_Plus	NP_0 - NP_9	NP_Dec	NP_Enter
PrtSc (SysRq)	ScrLk	Pause (Break)	

7.3.11 Alerts Page

Use this page to configure which system events an alert should be sent for and the destination for the alerts. Up to two destinations can be selected for each LAN channel. Figure 89 shows the details for an S1200BTL system.

Figure 89: Configuration Alerts Page on S1200BTL Platforms

The following table lists the options allowing you to select the events that alerts should be sent on and selection of where the alerts are to be sent.

Table 22: Configuration Alerts Options

Option	Task
Select the events that will trigger alerts.	Select one or more system events that will trigger an alert.
Check/Clear All buttons	Click to select or clear all events.
LAN Channel to Configure	Select either the BMC or RMM4 to configure the destination.
Alert Destination #1/#2	Select either SNMP along with the IP address or email address that the alert will be sent to. Up to two destinations can be selected for each LAN channel.

Option	Task
Save button	Click to use selected setup.
Send Test Alerts button	After configuring select this to send a test alert.

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family there are two additional options. See Figure 90 for details.

- **Globally Enable Platform Event Filtering:** This can be used to prevent sending alerts until you have fully specified your desired alerting policies.
- **Log Event on Filter Action:** This can be used to enable or disable the logging of an event into the System Event Log when a Filter Action is taken.

Figure 90: Configuration Alerts Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

7.3.12 Alert Email Page

Use this page to configure the parameters for Alert Emails.

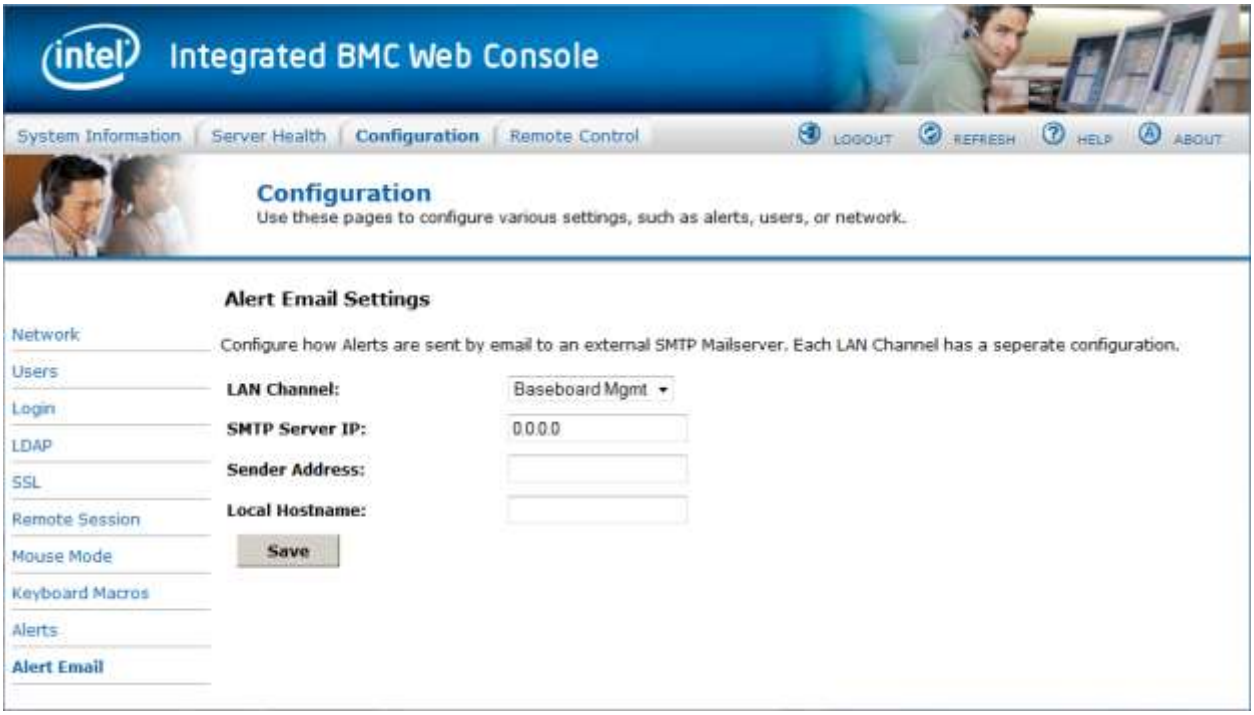


Figure 91: Configuration Alert Email Page

The following table lists the options allowing you to configure the parameters for Alert Emails.

Table 23: Configuration Alert Email Options

Option	Task
LAN Channel	Select either the BMC or RMM4 to configure the destination.
SMTP Server IP	The IP address of the remote SMTP mail server that the alert emails will be sent to. • The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". • 'xxx' ranges from 0 to 255. • First 'xxx' must not be 0.
Sender Address	The sender address string to be put in the "From:" field of outgoing alert emails.
Local Hostname	The hostname of the local machine that is generating the alert. It is put into the outgoing alert email. • The Local Hostname is a string of maximum 31 alpha-numeric characters. • Space and special characters are not allowed.
Save button	Click to use selected setup.

7.3.13 Node Manager Power Polices Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family this page is used to view, add, and configure the Node Manager Power Policies.

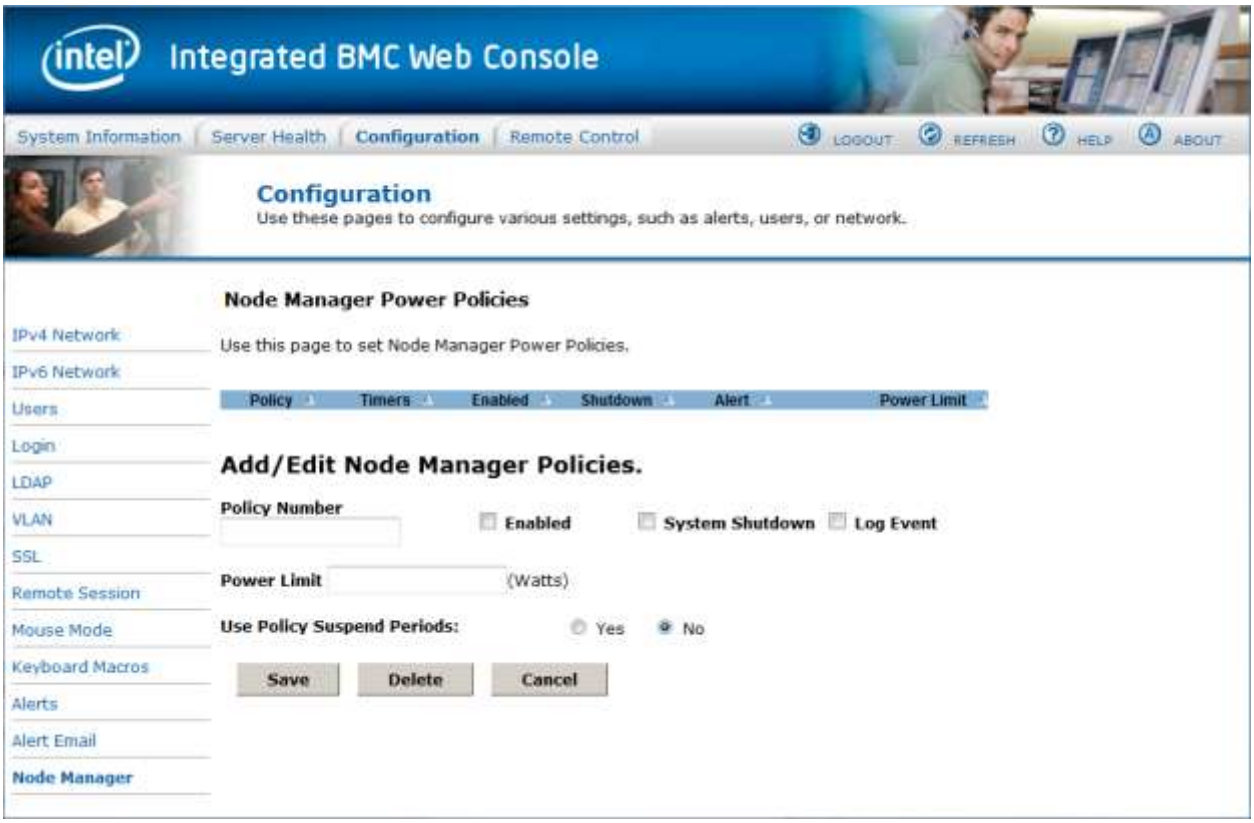


Figure 92: Configuration Node Manager Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The following table lists the options allowing you to view, add, and edit the Node Manager Power Policies.

Table 24: Configuration Node Manager Options

Option	Task
Node Manager Power Policies	This table lists the currently configured policies. Selecting an item from the table will populate the editable fields in the settings section below.
Policy Number	The policy number to add/edit/delete. Valid range is 0-255. In the policy table, policy numbers with an asterisk (*) are policies set externally using a non-platform domain. Changing parameters on these policies will not affect their triggers, trigger limits, reporting periods, correction timeouts, or aggressive CPU throttling settings.

Option	Task
Enabled check box	Check this box if the policy is to be enabled immediately.
System Shutdown check box	Check this box to enable a system shutdown if the policy is exceeded and cannot be corrected within the correction timeout period. The operating system will be given 30 seconds to shut down gracefully. If the system is still not shut down after 30 seconds, the BMC will initiate an immediate shutdown.
Log Event check box	Check this box to enable the node manager to send a platform event message to the BMC when a policy is exceeded.
Power Limit	The desired platform power limit, in watts.
Use Policy Suspend Periods	If enabled, you may configure policy suspend periods. Each policy may have up to five suspend periods (see Figure 93). Suspend periods are repeatable by day-of-week. Start and stop times are designated in 24-hour format, in increments of 6 minutes. To specify a suspended period crossing midnight, two suspend periods must be used.

For all policies set through this page, the following default values will be applied:

- **Domain: Platform** – Power for the entire platform.
- **Trigger:** None – Always monitor after end of POST.
- **Aggressive CPU Power Correction:** AUTO – Use of T-states and memory throttling controlled by policy exception actions.
- **Trigger Limit:** None.
- **Reporting Period:** 10 seconds – This is a rolling average for reporting only. It will not affect the average power monitored by the node manager.
- **Correction Timeout:** 22.555 seconds – Maximum time for the NM to correct power before taking an exception action (that is, shutdown or alert).

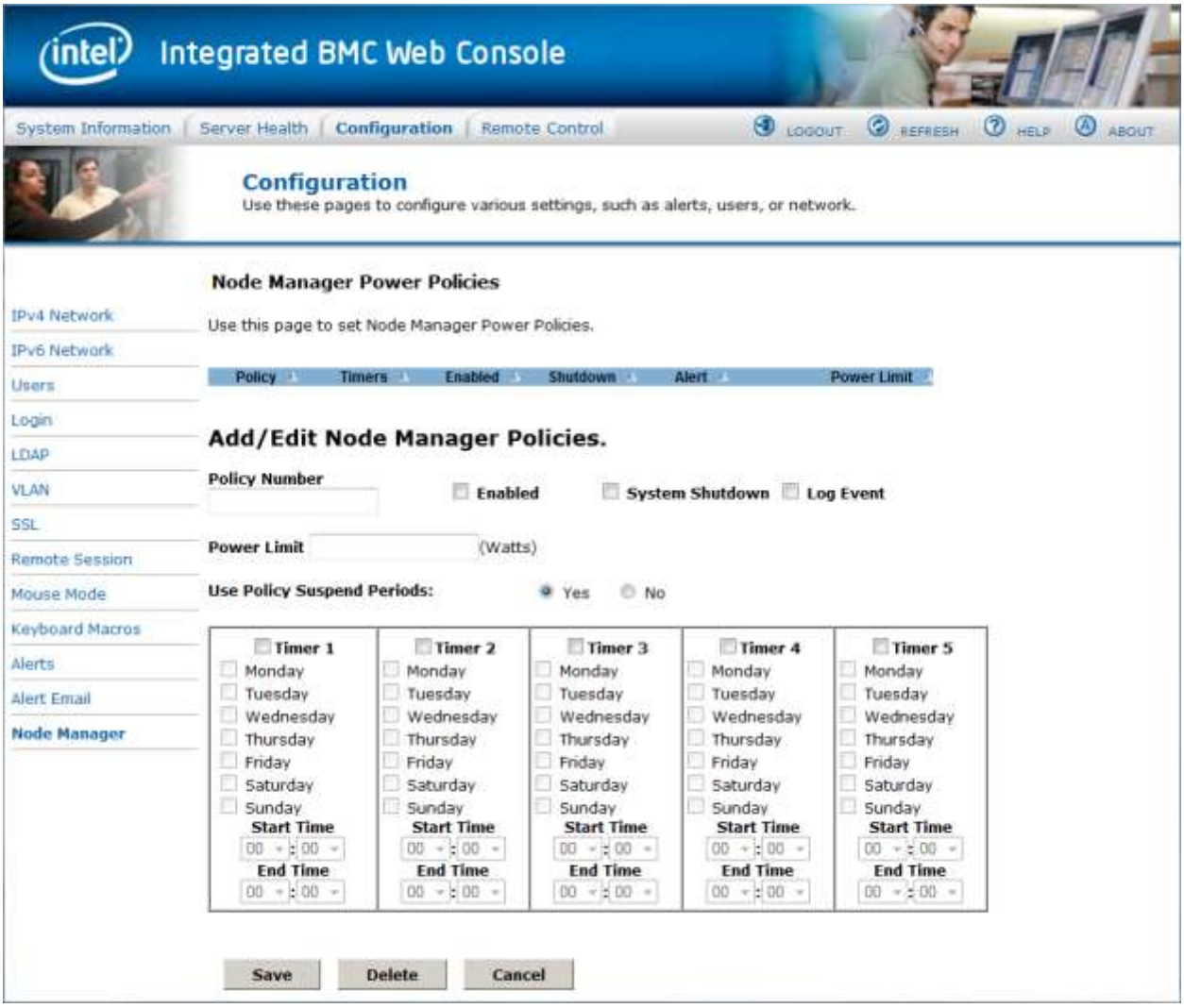


Figure 93: Configuration Node Manager Page with Use Policy Suspend Period Selected

7.4 Remote Control Tab

The **Remote Control** tab helps you perform the following remote operations on the server:

- Console redirection
- Server power control

7.4.1 Console Redirection Page

By default, the **Remote Control** tab opens the Console Redirection page. Launch the remote console KVM redirection window from this page.

Note that the **Launch Console** button will be grayed out and non-functional if the RMM4 Lite is not present.

Figure 94: Remote Control Console Redirection Page

Click the **Launch Console** button to launch the redirection console and manage the server remotely.

Note: Java Runtime Environment* (JRE* Version 6 Update 22 or higher) must be installed on the client before launch of JNLP file.

7.4.2 Server Power Control Page

The Server Power Control page shows the power status and allows power/reset control of the server. Figure 95 shows the details for an S1200BTL system.

For the Graceful OS Shutdown to function properly the OS must be ACPI aware and be configured to do the shutdown without operator intervention. After a Graceful Shutdown has been requested, if the system does not shut down as requested, the command cannot be executed again for five minutes.

Figure 95: Remote Control Server Power Control Page on S1200BTL Platforms

The following power control operations can be performed.

Table 25: Remote Control Power Control Options on S1200BTL Platforms

Option	Task
Reset Server	Select option to hard reset the host without powering off.
Power OFF Server	Select option to immediately power off the host.
Graceful Shutdown	Select option to soft power off the host.
Power ON Server	Select option to power on the host.
Power Cycle Server	Select option to immediately power off the host, and then power it back on after one second.
Perform Action button	Click to execute the selected remote power command.
Note: All power control actions are done through the BMC and are immediate actions. It is suggested to gracefully shut down the operating system using the KVM interface or other interface before initiating power actions.	

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you have an additional option **Force-enter BIOS Setup** on a reset. See Figure 96 and Table 26 for details.

For the Graceful OS Shutdown to function properly the OS must be ACPI aware and be configured to do the shutdown without operator intervention. After a Graceful Shutdown has been requested, if the system does not shut down as requested, the command cannot be executed again for five minutes.

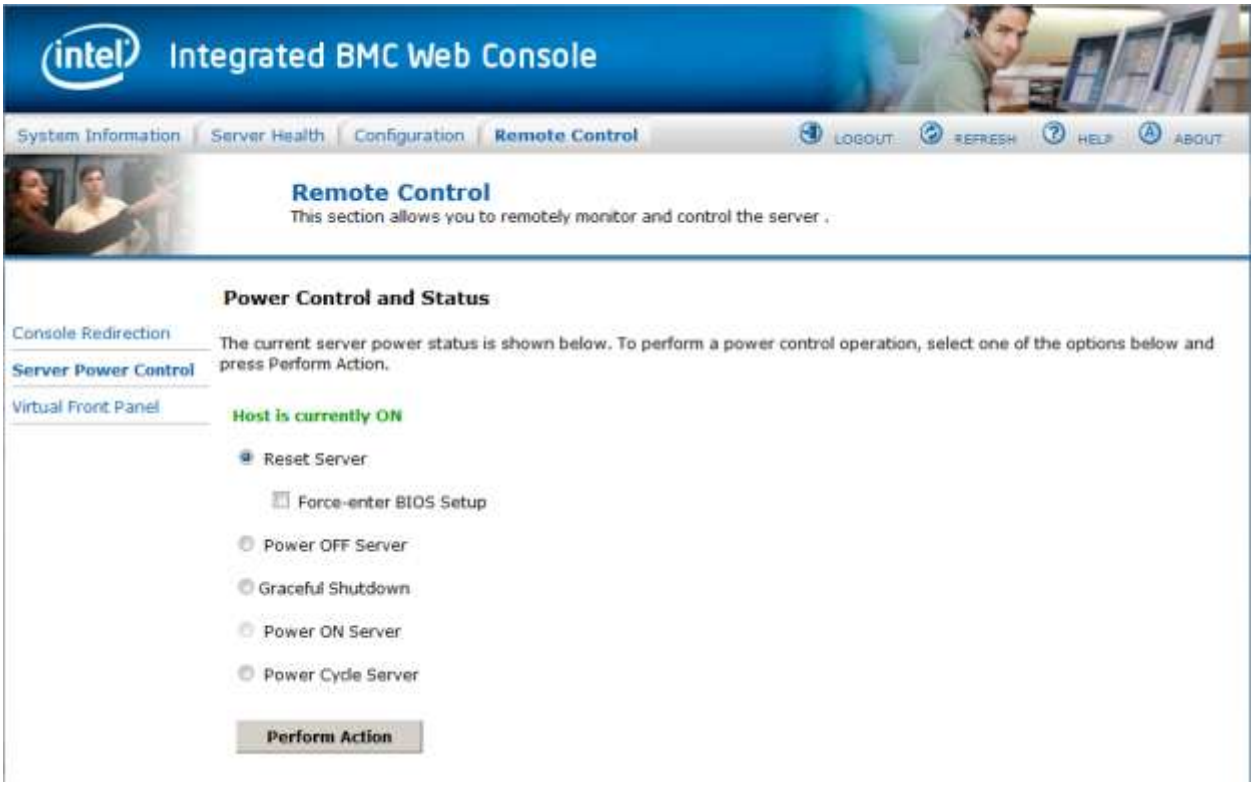


Figure 96: Remote Control Server Power Control Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

Table 26: Remote Control Power Control Options on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

Option	Task
Reset Server	Select option to hard reset the host without powering off.
Force-Enter BIOS Setup	Check this option to enter into the BIOS setup after resetting the server.
Power OFF Server	Select option to immediately power off the host.
Graceful Shutdown	Select option to soft power off the host.
Power ON Server	Select option to power on the host.
Power Cycle Server	Select option to immediately power off the host, and then power it back on after one second.
Perform Action button	Click to execute the selected remote power command.

Option	Task
Note: All power control actions are done through the BMC and are immediate actions.	

On an S1200V3RP Product Family system you have an additional option **Force-enter BIOS Setup** on a Power On. See Figure 97 and Table 27 for details.

For the Graceful OS Shutdown to function properly the OS must be ACPI aware and be configured to do the shutdown without operator intervention. After a Graceful Shutdown has been requested, if the system does not shut down as requested, the command cannot be executed again for five minutes.

Figure 97: Remote Control Server Power Control Page on S1200V3RP Product Family

Table 27: Remote Control Power Control Options on S1200V3RP Product Family

Option	Task
Reset Server	Select option to hard reset the host without powering off.
Force-Enter BIOS Setup	Check this option to enter into the BIOS setup after resetting the server.
Power OFF Server	Select option to immediately power off the host.
Graceful Shutdown	Select option to soft power off the host.
Power ON Server	Select option to power on the host.
Force-Enter BIOS Setup	Check this option to enter into the BIOS setup after powering on the server.

Option	Task
Power Cycle Server	Select option to immediately power off the host, and then power it back on after one second.
Perform Action button	Click to execute the selected remote power command.
Note: All power control actions are done through the BMC and are immediate actions.	

7.4.3 Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family this page can be used just like the systems front panel.

Figure 98: Remote Control Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families and S1200V3RP Product Family

The following power control operations can be performed.

Table 28: Remote Control Virtual Front Panel Options

Option	Task
Power Button	The Power button is used to power on or power off.
Reset Button	The Reset button is used to reset the server while system is ON.
Chassis ID Button	When the Chassis ID button is pressed, the chassis ID LED changes to solid on. If the button is pressed again, the chassis ID LED turns off.
NMI Button	At present, the NMI button is disabled.
Power LED	The Power LED shows the system power status. If the Power LED is green, the system is ON. If the Power LED is grey, the system is OFF.
Status LED	The Status LED reflects the system status LED status and it is automatically in sync with the BMC every 60 seconds. This reflects the System Status LED.
Chassis ID LED	The Chassis ID LED shows the current system chassis ID status. If the Chassis ID LED is blue, the Chassis ID is indefinite ON. If the Chassis ID LED is grey, the Chassis ID is OFF.