



Intel® Remote Management Module 4 User Guide

Revision 1.0

February, 2011

Enterprise Platforms and Services Division

Revision History

Date	Revision Number	Modifications
December 2010	0.5	First Pre-release.
December 2010	0.7	Ready for first review.
February 2011	0.85	After first review.
	1.0	After second review. Screen captures updated.

Disclaimers

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

Intel server boards contain a number of high-density VLSI and power delivery components that need adequate airflow for cooling. Intel's own chassis are designed and tested to meet the intended thermal requirements of these components when the fully integrated system is used together. It is the responsibility of the system integrator that chooses not to use Intel developed server building blocks to consult vendor datasheets and operating parameters to determine the amount of airflow required for their specific application and environmental conditions. Intel Corporation cannot be held responsible if components fail or the server board does not operate correctly when used outside any of their published operating or non-operating limits.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft, Windows, and Windows Server are trademarks, or registered trademarks of Microsoft® Corporation in the United States and/or other countries.

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

Copyright © 2011 – 2016 Intel Corporation. All rights reserved.

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	8
2.3.2 Client System	8
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 Intel® RMM4 Lite on Intel® Server Boards S1200BTL	10
3.3.2 Installation of the Intel® Dedicated Server Management NIC on an Intel® Server System R1304BTLSFAN/R1304BTLSHBN	12
3.3.3 Installation of the Intel® Dedicated Server Management NIC on an Intel® Server System P4304BTLSHCN/P4304BTLSEFCN	15
3.3.4 Installation of the Intel® Dedicated Server Management NIC on a 3 rd Party Pedestal Chassis	17
4. Configuring Intel® RMM4	19
4.1 Configuring your Intel® RMM4 through BIOS setup	20
4.2 Configuring Your Intel® RMM4 Using the Intel® Deployment Assistant (IDA)	21
4.3 Configuring Your Server Using Intel System Configuration Utility (SysConfig)	30
4.3.1 Configure User	30
4.3.2 Configuring IP address	30
4.3.3 Configuring Serial Over LAN	30
5. Getting Started with Intel® RMM4 Operation	31
5.1 Before You Begin	31
5.1.1 Client Browsers	31
5.2 Logging In	32
5.3 Navigation	33
5.4 Online Help	34
5.5 Logging Out	35
6. Remote Console (KVM) Operation	37
6.1 Launching the Redirection Console	37

6.2	Main Window.....	38
6.3	Remote Console Control Bar.....	39
6.3.1	Remote Console Video Menu.....	40
6.3.2	Remote Console Keyboard Menu.....	40
6.3.3	Remote Console Mouse Menu.....	43
6.3.4	Remote Console Options Menu.....	45
6.3.5	Remote Console Device Menu.....	45
6.4	Remote Console Status Line.....	46
7.	Intel® Integrated BMC Web Console Options	47
7.1	System Information Tab.....	48
7.1.1	Viewing System Information.....	48
7.1.2	Viewing Field Replaceable Unit (FRU) Information.....	49
7.1.3	Viewing System Diagnostics Information.....	49
7.1.4	Viewing DIMM Information.....	50
7.2	Server Health Tab.....	51
7.2.1	Viewing Sensor Readings.....	51
7.2.2	Viewing Event Log.....	53
7.2.3	Viewing Power Statistics.....	54
7.3	Configuration Tab.....	55
7.3.1	Configuring Network Settings.....	56
7.3.2	Managing Users.....	57
7.3.3	Login Security Settings.....	59
7.3.4	Configuring LDAP Settings.....	60
7.3.5	Configuring SSL Upload.....	61
7.3.6	Configuring Remote Session.....	62
7.3.7	Configuring Mouse Mode.....	63
7.3.8	Configuring Keyboard Macros.....	64
7.3.9	Configuring Alerts.....	66
7.3.10	Configuring Alert Email.....	67
7.4	Remote Control tab.....	68
7.4.1	Console Redirection.....	68
7.4.2	Server Power Control.....	69

List of Figures

Figure 1: Intel® RMM4 Lite	7
Figure 2: Intel® Dedicated Server Management NIC	7
Figure 3: Installing Intel® RMM4 Lite on Intel® Server Boards S1200BTL	11
Figure 4: Attaching the bracket to Intel® Dedicated Server Management NIC module.....	12
Figure 5: Attaching the cable to Intel® Dedicated Server Management NIC module.....	13
Figure 6: Adding the Intel® Dedicated Server Management NIC module in the Server System R1304BTLSFAN/R1304BTLSHBN	14
Figure 7: Attaching the bracket to Intel® Dedicated Server Management NIC module.....	15
Figure 8: Adding the Intel® Dedicated Server Management NIC module in the Server System P4304BTLSHCN/P4304BTLSFCN	16
Figure 9: Attaching the bracket to Intel® Dedicated Server Management NIC module.....	17
Figure 10: Mounting the Intel® Dedicated Server Management NIC module to the PCI Slot bracket	17
Figure 11: Adding the Intel® Dedicated Server Management NIC module on a 3rd Party Chassis	18
Figure 12: Server Management.....	20
Figure 13: IDA Configure Server: Communication Options Window.....	21
Figure 14: IDA Configure Server: Communication Options Window No Dedicated Server Management NIC installed.	22
Figure 15: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) IP Address from a DHCP server window	23
Figure 16: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) Static IP Address window	24
Figure 17: IDA Configure Server: Set Up Users window	25
Figure 18: IDA Configure Server: Edit User Information window.....	26
Figure 19: IDA Configure Server: Apply Configuration window.....	27
Figure 20: IDA Configure Server: Applying Configuration progress window	28
Figure 21: IDA Configure Server: Restart Server	29
Figure 22: Internet Explorer displaying encryption key length	31
Figure 23: Intel® Integrated BMC Web Console Login Page.....	32
Figure 24: Integrated BMC Web Console Home Page.....	33
Figure 25: Launching the Online Help	35
Figure 26: Logging Out of Integrated BMC Web Console – Step 1	35
Figure 27: Logging Out of Integrated BMC Web Console – Step 2	36
Figure 28: Remote Control Console Redirection window.....	37
Figure 29: Remote Console	38
Figure 30: Remote Console Main Window	39

Figure 31: Remote Console Control Bar	40
Figure 32: Remote Console Video Menu	40
Figure 33: Remote Console Keyboard Menu	41
Figure 34: Remote Console Keyboard Language Sub Menu	41
Figure 35: Remote Console Keyboard Soft Keyboard Sub Menu.....	43
Figure 36: Remote KVM Soft Keyboard.....	43
Figure 37: Remote Console Mouse Menu	44
Figure 38: Remote Console Options Menu	45
Figure 39: Remote Console Device Menu.....	45
Figure 40: Status Line.....	46
Figure 41: Busy Indicator Bar.....	47
Figure 42: System Information page.....	48
Figure 43: System Information FRU Information page.....	49
Figure 44: System Information System Diagnostics page.....	50
Figure 45: System Information DIMM Information page	50
Figure 46: Server Health Sensor Reading's window (Thresholds not displayed).....	51
Figure 47: Server Health Sensor Reading's window (Thresholds displayed).....	52
Figure 48: Server Health Event Log	53
Figure 49: Server Health Power Statistics	54
Figure 50: Configuration.....	55
Figure 51: Configuration Network Settings window.....	56
Figure 52: Configuring User List window.....	57
Figure 53: Configuring Users Add User window	58
Figure 54: Configuring Users Modify User window.....	58
Figure 55: Configuring Login Security Settings window.....	59
Figure 56: Configuring LDAP Settings window	60
Figure 57: Configuring SSL Upload window.....	61
Figure 58: Configuring Remote Session window.....	62
Figure 59: Configuring Mouse Mode Setting window	63
Figure 60: Configuring Keyboard Macros window.....	64
Figure 61: Configuring Alerts window.....	66
Figure 62: Configuring Alert Email window.....	67
Figure 63: Remote Control Console Redirection window.....	68
Figure 64: Server Power Control window	69

List of Tables

Table 1: Terminology	1
Table 2: Integrated BMC Web Console home page tabs.....	33
Table 3: Horizontal Toolbar Buttons	34
Table 4: System Information Details	48
Table 5: Server Health (Sensor Readings) Options	52
Table 6: Server Health (Event Log) Options	53
Table 7: Configuration (Network Settings) Options.....	56
Table 8: Configuration (LDAP Settings) Options	60
Table 9: Configuration (Remote Session) Options.....	62
Table 10: Macro Non-printable Key Names.....	65
Table 11: Configuration (Alerts) Options.....	66
Table 12: Configuration (Alert Email) Options.....	67
Table 13: Remote Control (Power Control) Options.....	69

<This page is intentionally left blank.>

1. Introduction

The Intel® RMM4 works as an integrated solution on your server system. Based on an embedded operating system, the Intel® RMM4 add-on card 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® RMM4 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), this small form-factor mezzanine card enables server control via a built-in Web Console from anywhere, anytime.

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

1.1 Target Audience

This Guide is intended for system technicians who are responsible for installing, troubleshooting, upgrading, and repairing the Intel® RMM4. As a system administrator, you can use it to work on the Intel® RMM4 to gain location-independent remote access to respond to critical incidents.

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
OOB	Out Of Band- No operating system interaction on Server
SDR	Sensor Data Record

Word/Acronym	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol

1.3 Safety Information

⚠ **WARNING**

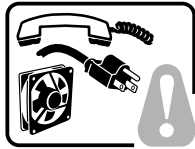
Before working with your Intel® RMM4 server product - whether you are using this guide or any other resource as a reference - pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications 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.

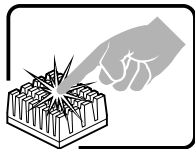
⚠ Safety Cautions

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.

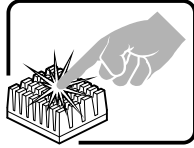
⚠ Wichtige Sicherheitshinweise

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>.



SICHERHEISSMASSNAHMEN: 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 beschriftet 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.



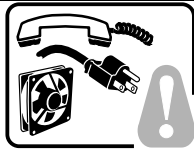
Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

⚠ 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》）。

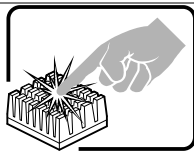
⚠ Consignes de sécurité

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.

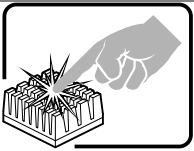
⚠ Instrucciones de seguridad importantes

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 sujeta 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.



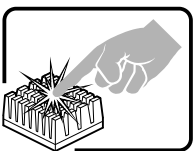
Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

⚠ 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/accesso 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

World Wide Web: http://www.intel.com/p/en_US/support

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

1. Visit the following Intel Support web page: 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 web site:
<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

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 1Gb 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.

If the optional Dedicated Server Management NIC is not used then the traffic can go through the onboard Integrated BMC-shared NIC and 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 via 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 via 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. Once 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 independent of the host operating system on the server where it is installed except during Remote Console (KVM) connections. During Remote Console connections the Keyboard, Mouse and Video 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* SP2 IA32- and EM64T
- Microsoft Windows Server 2008* R2
- Red Hat* Enterprise Linux 6 for IA32 and EM64T
- SUSE* Enterprise Linux 11 SP1 for IA32 and EM64T

2.3.2 Client System

The following client-Internet browsers have been tested:

- Microsoft Internet Explorer 7.0*
- Microsoft Internet Explorer 8.0*
- Microsoft Internet Explorer 9.0*
- Mozilla Firefox 3.0*
- Mozilla Firefox 3.5*

- Mozilla Firefox 3.6*

3. Hardware Installations and Initial Configuration

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

3.1 Before You Begin

Please 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® Remote Management Module 4 is currently supported on the following Intel® server boards and systems:

- All SKUs of Intel® Server Board S1200BTL
- Intel® Server System R1304BTLSFAN/R1304BTLSHBN
- Intel® Server System P4304BTLSHCN/P4304BTL SFCN

The Intel® RMM4 has two different packages, RMM4 Lite edition (AXXRMM4Lite) and RMM4 full edition (AXXRMM4).

RMM4 Lite edition box contains Intel® Remote Management Module 4 Lite module.

RMM4 full edition box contains the following components:

- Intel® Remote Management Module 4 Lite module
- Intel® Dedicated Server Management Network Interface Card (NIC) module
- Plastic bag containing screws, metal fastening bracket, PCI slot brackets, and cabling

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

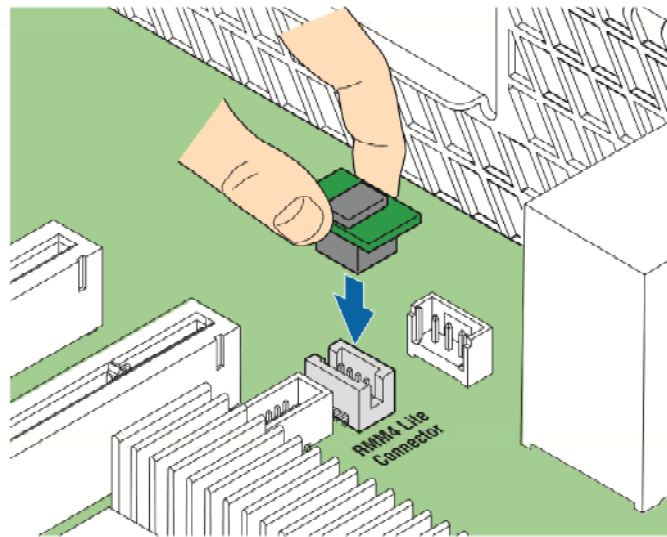
▲ Caution: Intel® RMM4 Lite and RMM4 DMN are NOT hot-swappable. Before removing or replacing it, you must first take the server out of service, turn off the system by pressing the power button and unplug the AC power cord from the system or wall outlet and wait for at least 10 seconds before installing the module.

3.3.1 Installation Intel® RMM4 Lite on Intel® Server Boards S1200BTL

The following are steps of installing Intel® RMM4 Lite on Intel® Server Board S1200BTL. The Intel® Server System R1304BTLSFAN/R1304BTLSHBN/P4304BTLSHCN/P4304BTL SFCN all

use the same Intel® Server Board S1200BTL, the same installation steps apply to those 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 RMM4 Lite connector (J4B1) on server board S1200BTL
3. Carefully pickup RMM4 Lite module, keep the direction of broken pin of the RMM4 Lite connector and insert the RMM4 Lite header into that connector.



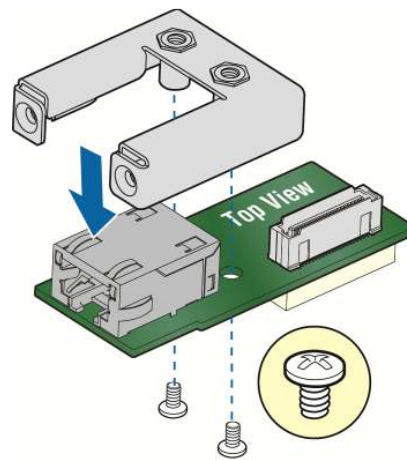
AF003760

Figure 3: Installing Intel® RMM4 Lite on Intel® Server Boards S1200BTL

3.3.2 Installation of the Intel® Dedicated Server Management NIC on an Intel® Server System R1304BTLFAN/R1304BTLHBN

Intel® Server System R1304BTLFAN and R1304BTLHBN are rack servers that are based on the Intel® Server Board S1200BTL. The following are steps should be used when installing the 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 Intel® Dedicated Server Management NIC module.

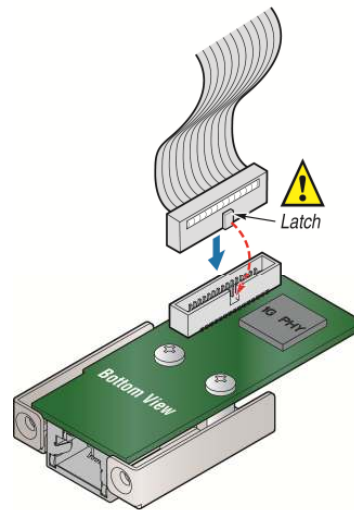


AF003756

Figure 4: Attaching the bracket to Intel® Dedicated Server Management NIC module

3. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module.

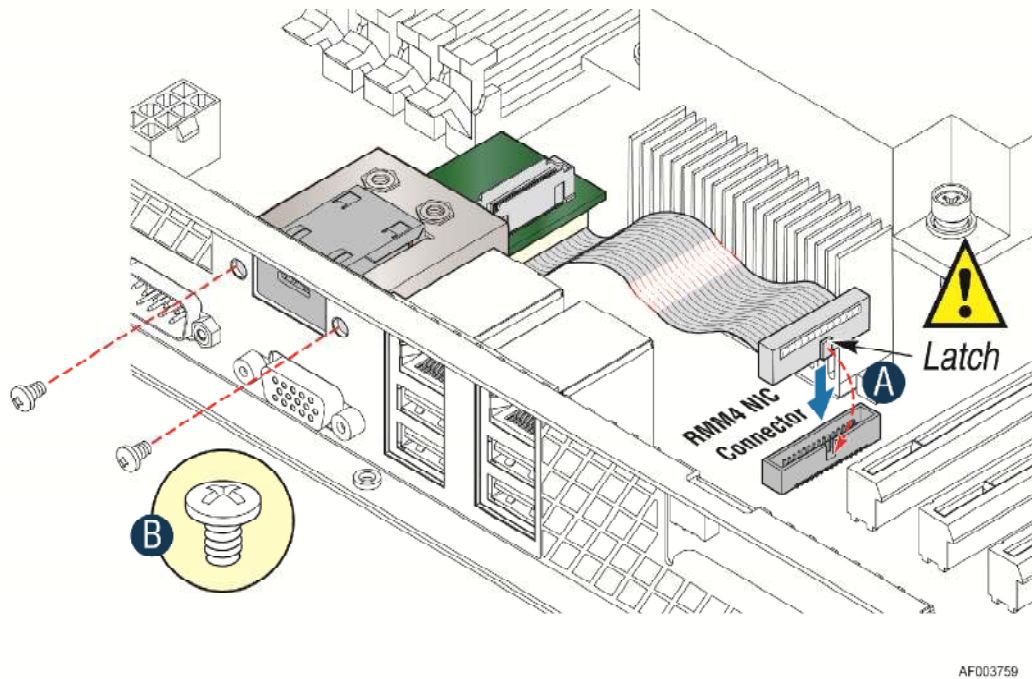
▲ Caution: Care should be used when attaching or removing this cable. Mishandling the cable could cause damage.



AF003758

Figure 5: Attaching the cable to Intel® Dedicated Server Management NIC module

4. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.
5. Attach the cable to the RMM4 NIC connector (J5C1) on the server board as shown in Figure 6 (A). Mount the NIC module to the back of the chassis and secure the metal fastening bracket with two screws as shown in Figure 6 (B). This will align the RJ-45 with the opening in the chassis.



AF003759

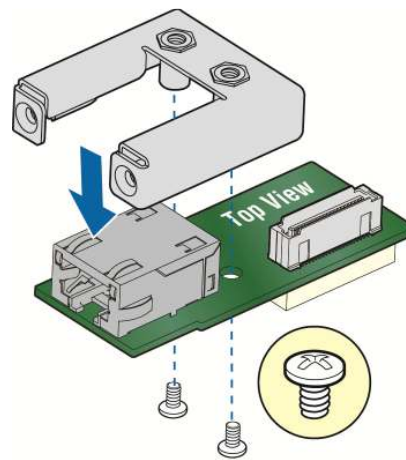
Figure 6: Adding the Intel® Dedicated Server Management NIC module in the Server System R1304BTLSFAN/R1304BTLSHBN

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

3.3.3 Installation of the Intel® Dedicated Server Management NIC on an Intel® Server System P4304BTLSHCN/P4304BTLFCN

Intel® Server System P4304BTLSHCN/P4304BTLFCN are pedestal servers that are based on the Intel® Server Board S1200BTL. The following are steps should be used when installing the 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 Intel® Dedicated Server Management NIC module.



AF003756

Figure 7: Attaching the bracket to Intel® Dedicated Server Management NIC module

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 finger has potential risk.
4. Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module as shown in Figure 8 (A). Mount the NIC module to the back of the chassis and secure the metal fastening bracket with two screws as shown in Figure 8 (B). This will align the RJ-45 with the opening in the chassis. Attach the cable to the RMM4 NIC connector (J5C1) on the server board as shown in Figure 8 (C).
- ▲ Caution:** Care should be used when attaching or removing this cable. Mishandling the cable could cause damage.

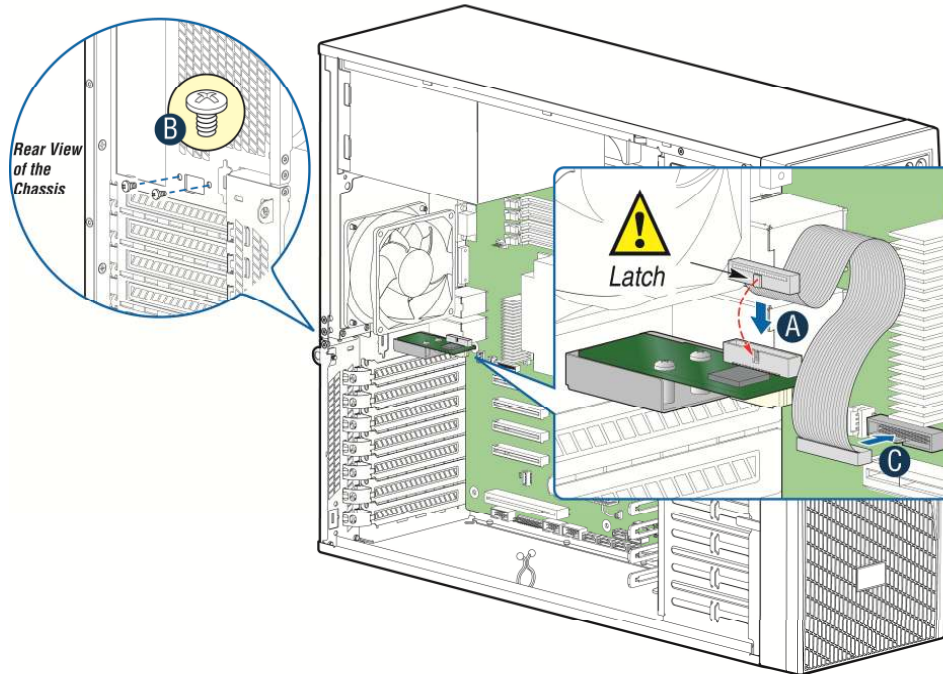


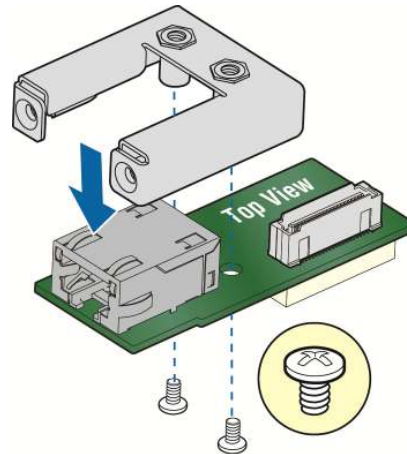
Figure 8: Adding the Intel® Dedicated Server Management NIC module in the Server System P4304BTLSHCN/P4304BTL SFCN

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

3.3.4 Installation of the Intel® Dedicated Server Management NIC on a 3rd Party Pedestal Chassis

The following are steps should be used when installing the Dedicated Server Management NIC module on a 3rd party pedestal chassis with the Intel® Server Board S1200BTL.

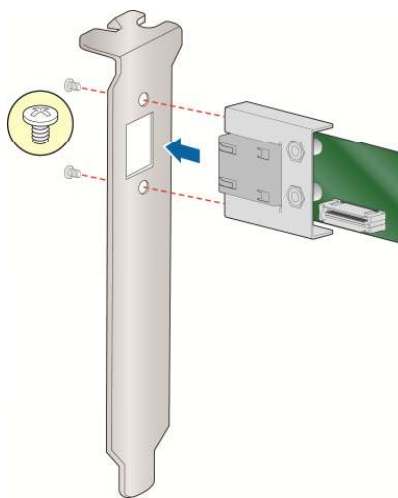
1. Ensure that AC power has been removed from the system and that you have waited at least 10 seconds after removing power.
2. Attach the metal fastening bracket to Intel® Dedicated Server Management NIC module.



AF003756

Figure 9: Attaching the bracket to Intel® Dedicated Server Management NIC module

3. Secure the metal fastening bracket with NIC module to PCI slot bracket with two screws as shown in Figure 10. This will align the RJ-45 with the opening in the PCI slot bracket.

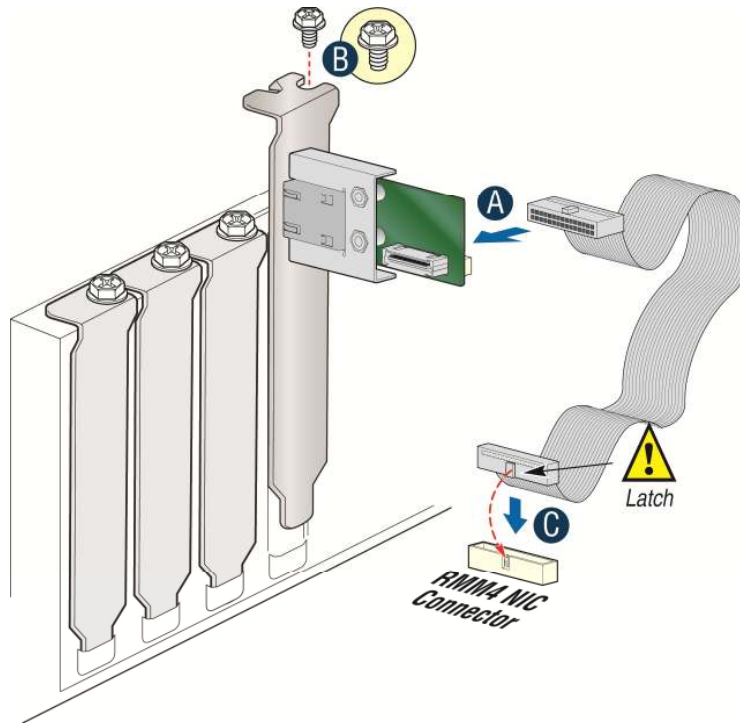


AF003787

Figure 10: Mounting the Intel® Dedicated Server Management NIC module to the PCI Slot bracket

- Attach the cable to the cable connector on the Intel® Dedicated Server Management NIC module as shown in Figure 11 (A). Mount the PCI slot bracket with NIC module to the 3rd chassis and secure with screw as shown in Figure 11 (B). Attach the cable to the RMM4 NIC connector (J5C1) on the server board as shown in Figure 11 (C).

⚠ Caution: Care should be used when attaching or removing this cable. Mishandling the cable could cause damage.



AF003786

Figure 11: Adding the Intel® Dedicated Server Management NIC module on a 3rd Party Chassis

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

4. Configuring Intel® RMM4

This section discusses using the Server Utilities to enable an Intel® RMM4 from a new unconfigured state to an operational one.

When first powered on, by default, the Intel® RMM4 uses a static IP address of 0.0.0.0.

The Intel® RMM4 can be configured in many 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 disc that is shipped with the server board.
- SYSCFG - <http://downloadcenter.intel.com/default.aspx> > relevant server platforms page

Two steps are necessary before 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 channel(s).

4.1 Configuring your Intel® RMM4 through BIOS setup

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. Scroll down to Intel® RMM4 LAN Configuration - **IP source**. And then select either **Static** or **Dynamic**.
 - a. If **Static** was selected configure the **IP address**, **Subnet mask** and **Gateway IP** as needed.
 - b. If **Dynamic** was selected configure the **BMC DHCP host name**.

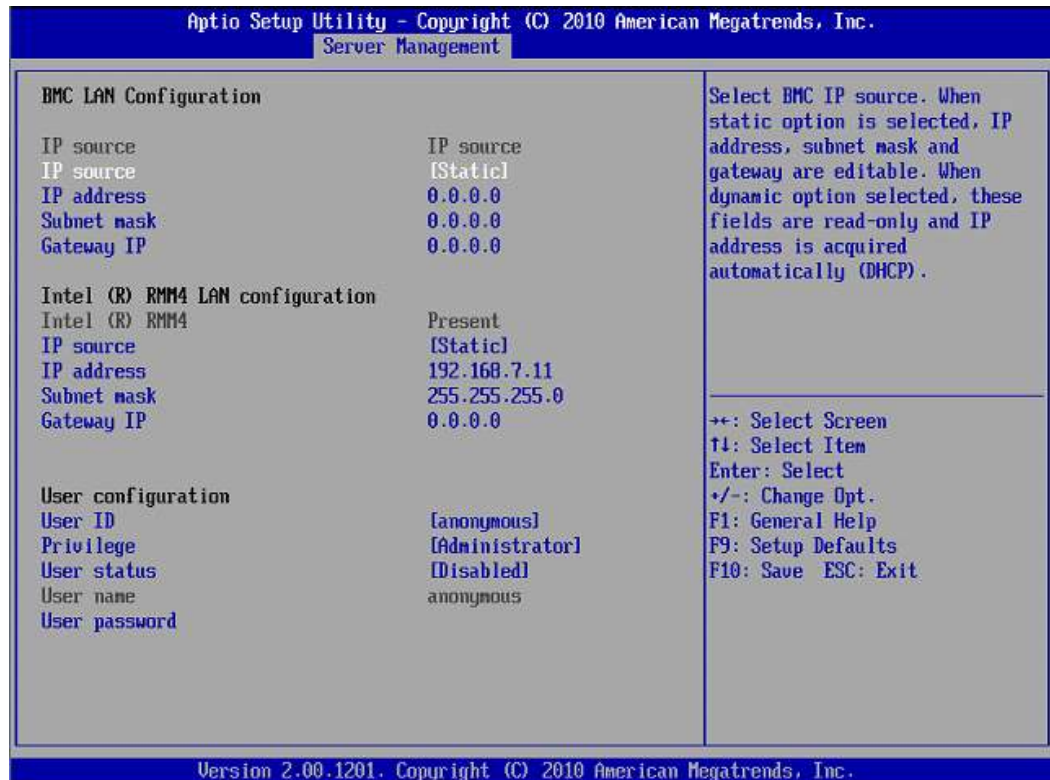


Figure 12: Server Management

4.2 Configuring Your Intel® RMM4 Using the Intel® Deployment Assistant (IDA)

The following section explains the RMM4 configuration using IDA:

⚠ WARNING

If you need to configure both LAN Channel 1 and LAN channel 3 (RMM4 Dedicated Server Management NIC), ensure that they are configured with different subnets.

Note: When the Dedicated Server Management NIC is not installed, since the RMM4 Lite has no dedicated NIC, the LAN Channel 3 is not displayed. The user can access RMM4 Lite advance features via LAN channel 1 (onboard NIC1). See Figure 14.

1. Select which channel to configure.

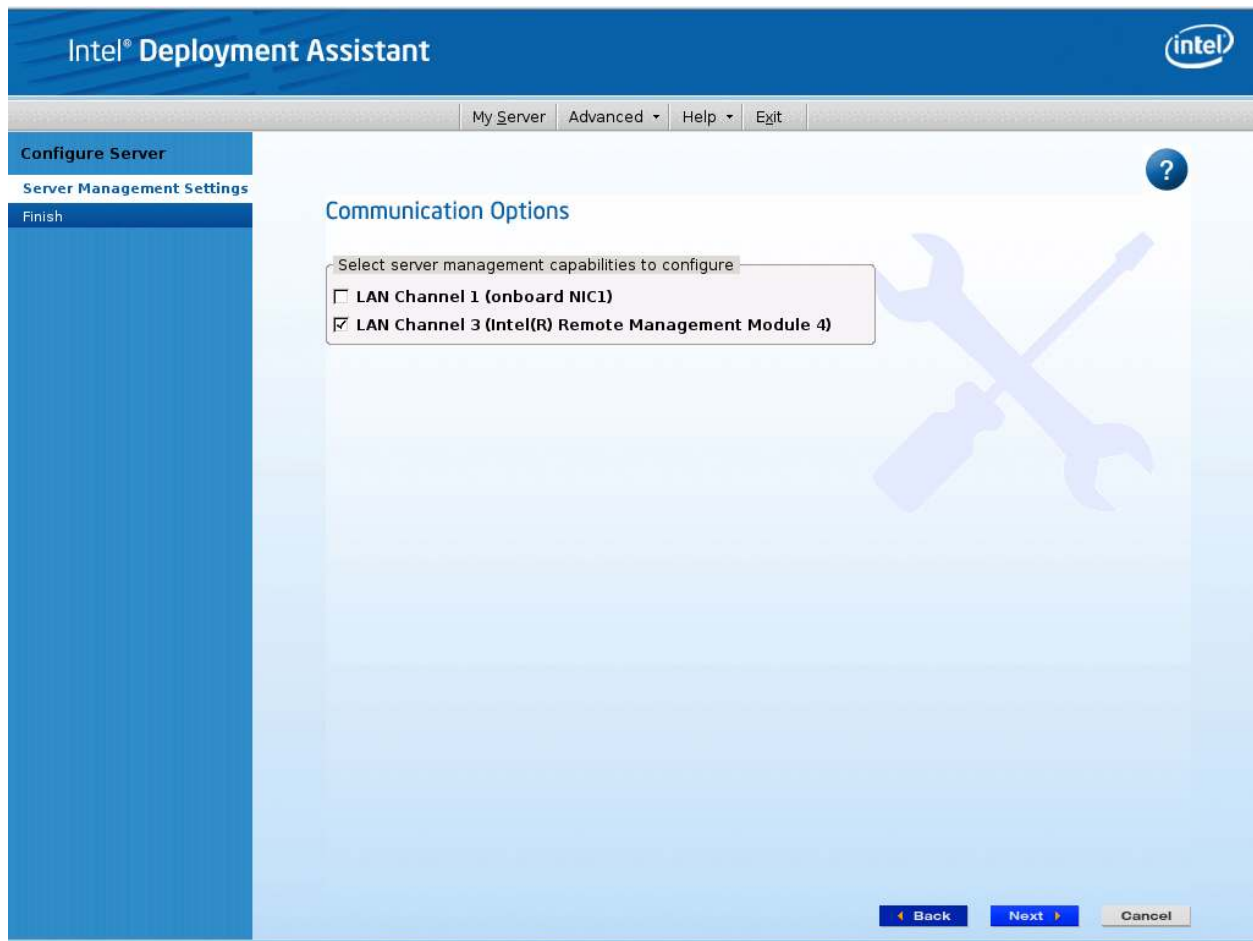
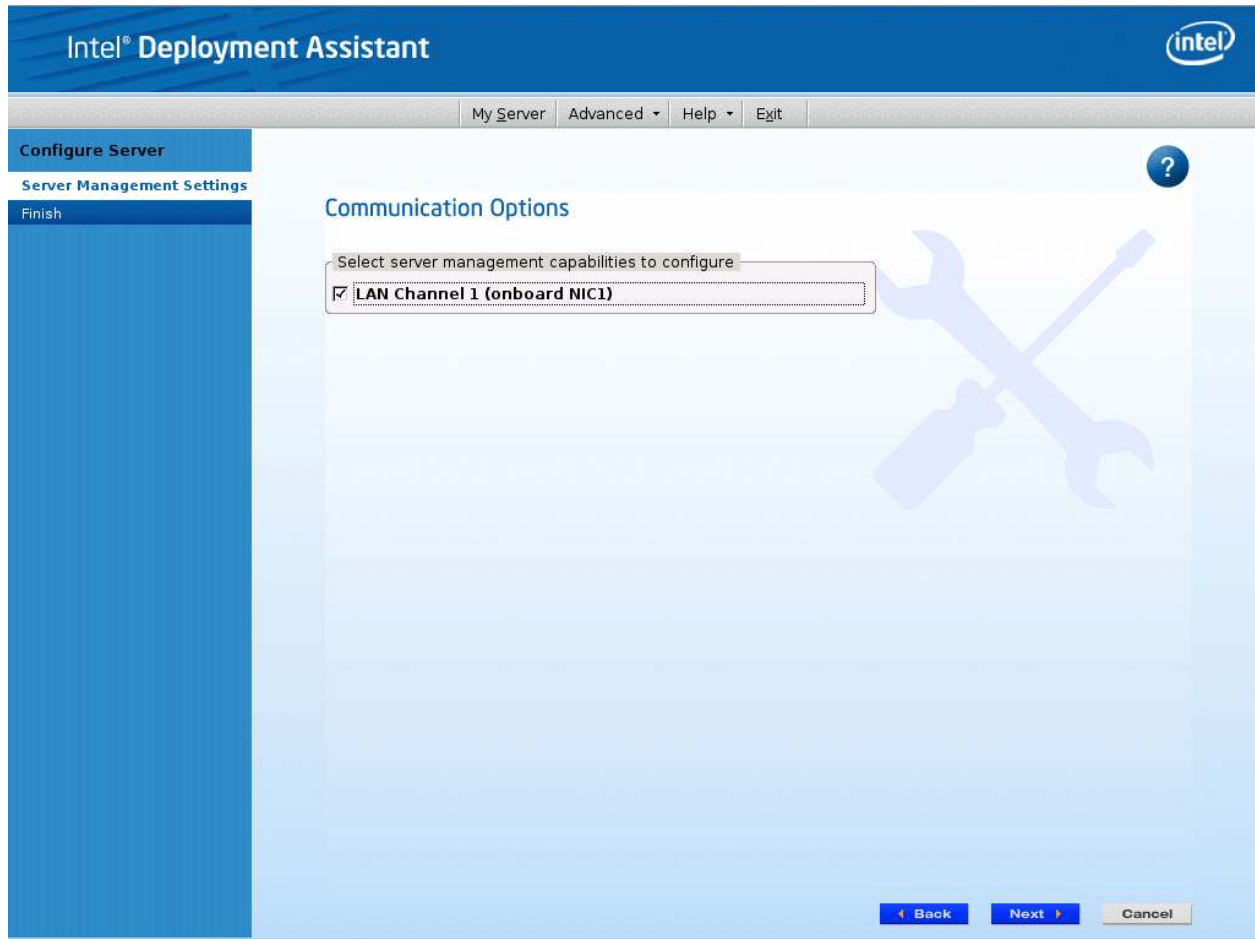


Figure 13: IDA Configure Server: Communication Options Window



**Figure 14: IDA Configure Server: Communication Options Window
No 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 15.
 - b. If **Static IP Address** is selected configure the **IP address**, **Subnet Mask** and **Gateway** as shown in Figure 16.
3. You can also select **Enable Serial Over LAN** and **Configure Alert** on these screens.

The screenshot shows the 'Configure LAN Channel 3' window in the Intel Deployment Assistant. The window title is 'LAN Channel 3 (Intel® Remote Management Module)'. The main content area is titled 'Configure the LAN Channel 3 access settings.' and includes the following options:

- Enable LAN Channel 3**
- IP Address from a DHCP server**
 - DHCP Host Name:
- Static IP Address**
- Enable Serial Over LAN**
- Configure Alert**

At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

Figure 15: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) IP Address from a DHCP server window



Figure 16: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM4 DMN) Static IP Address window

4. [Optional] Setup the users by selecting the **User Name** and then clicking on **Edit**. The Edit User Data window opens.

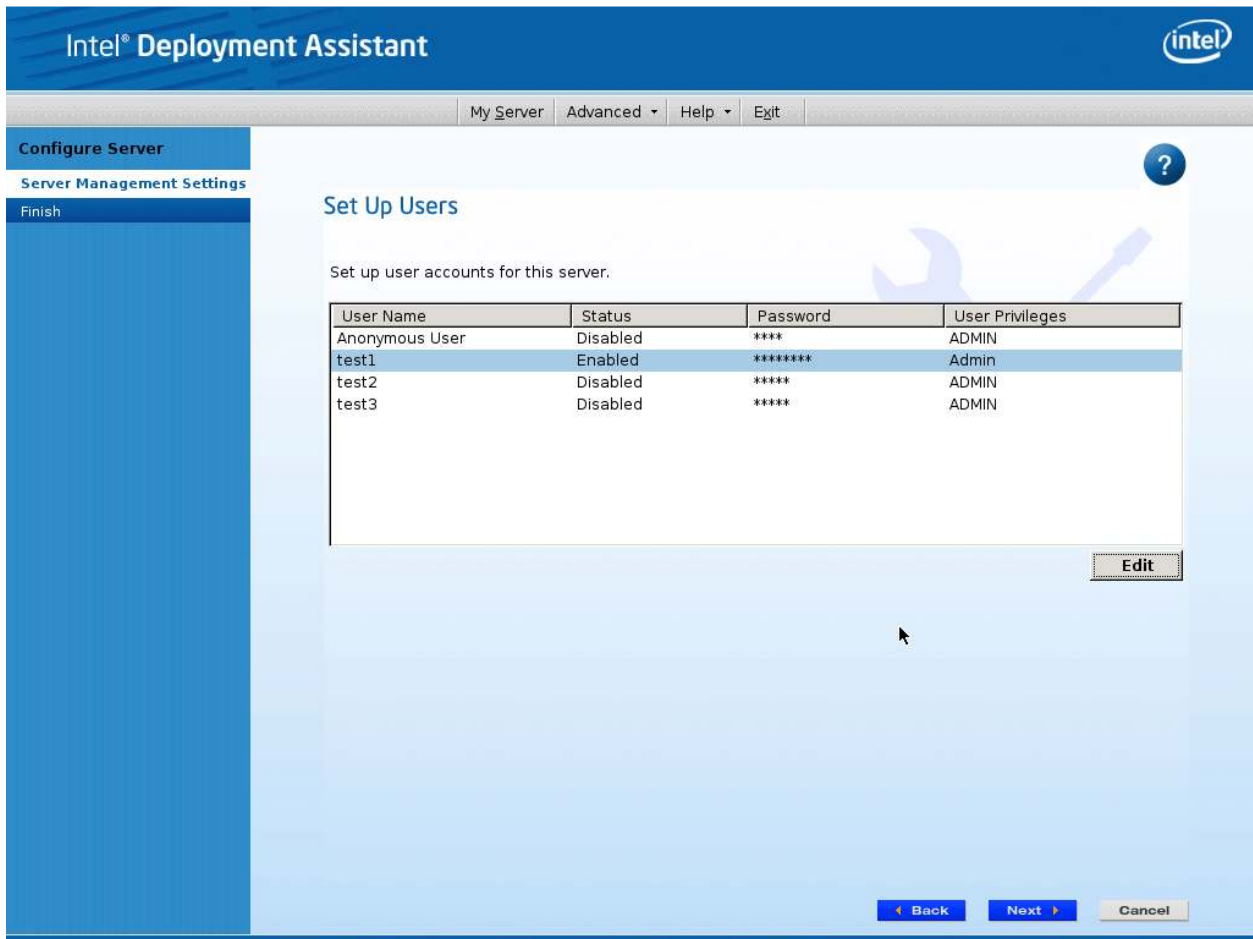


Figure 17: IDA Configure Server: Set Up Users window

Notes:

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

5. Edit the User information and click OK to apply configuration.

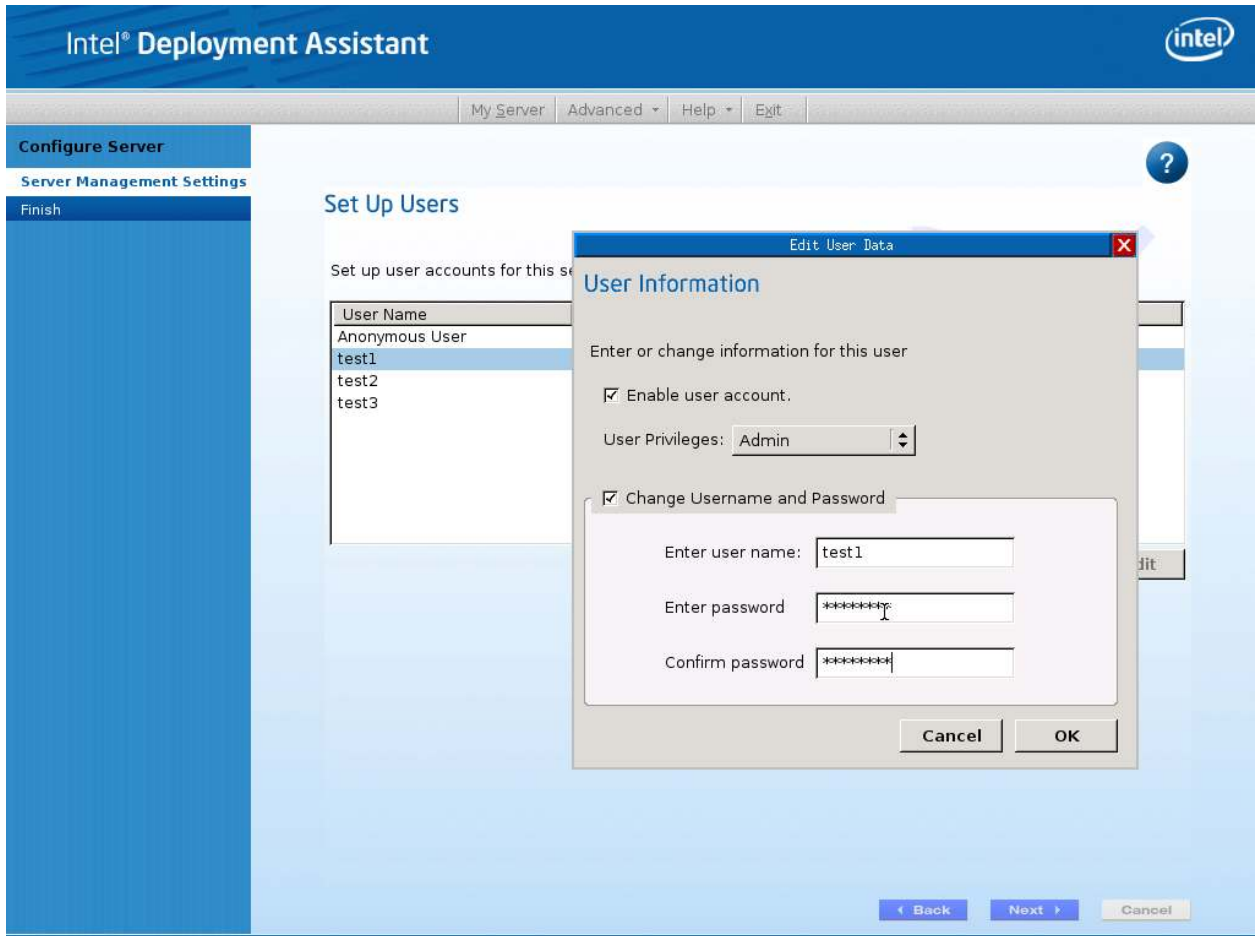


Figure 18: IDA Configure Server: Edit User Information window

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

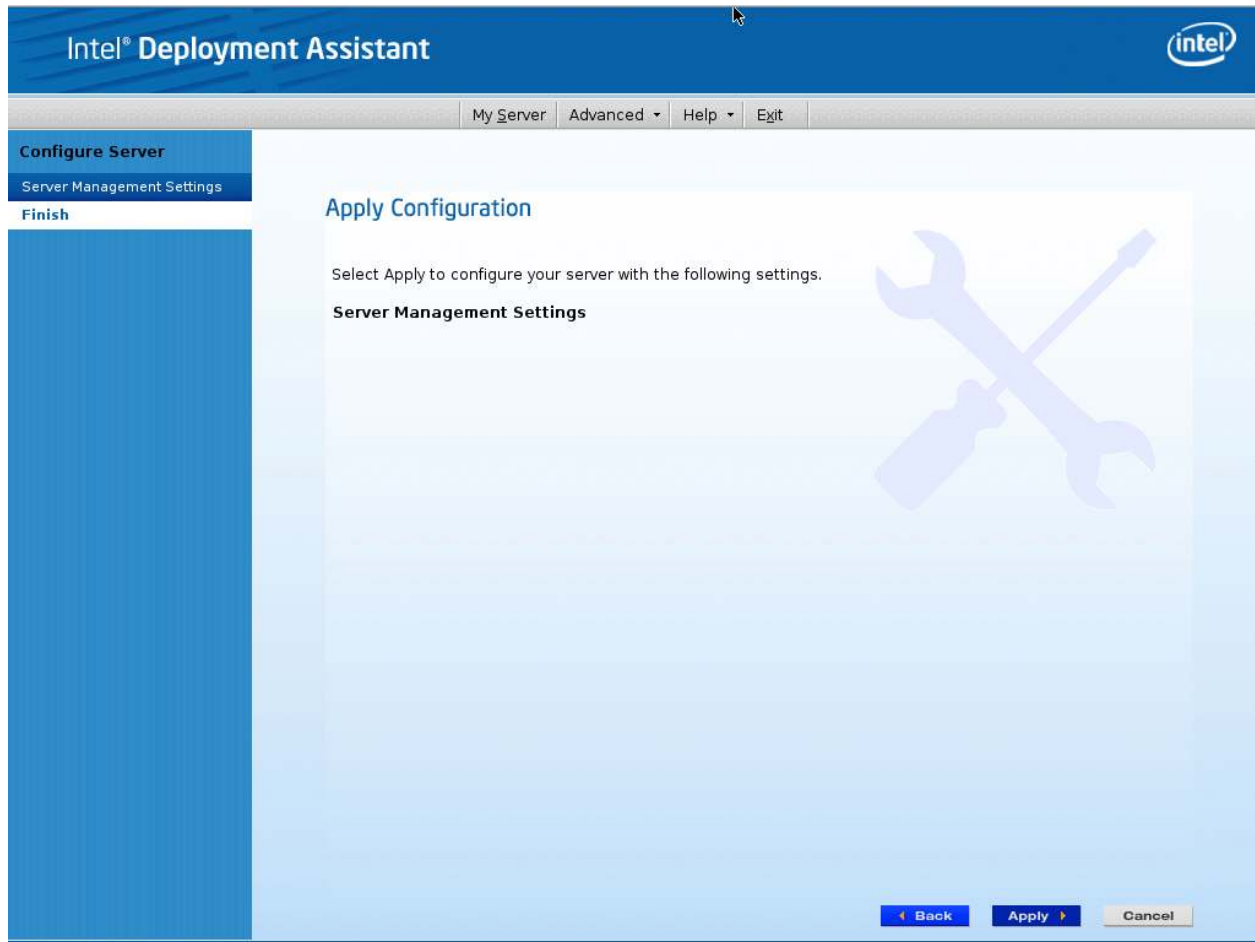


Figure 19: IDA Configure Server: Apply Configuration window

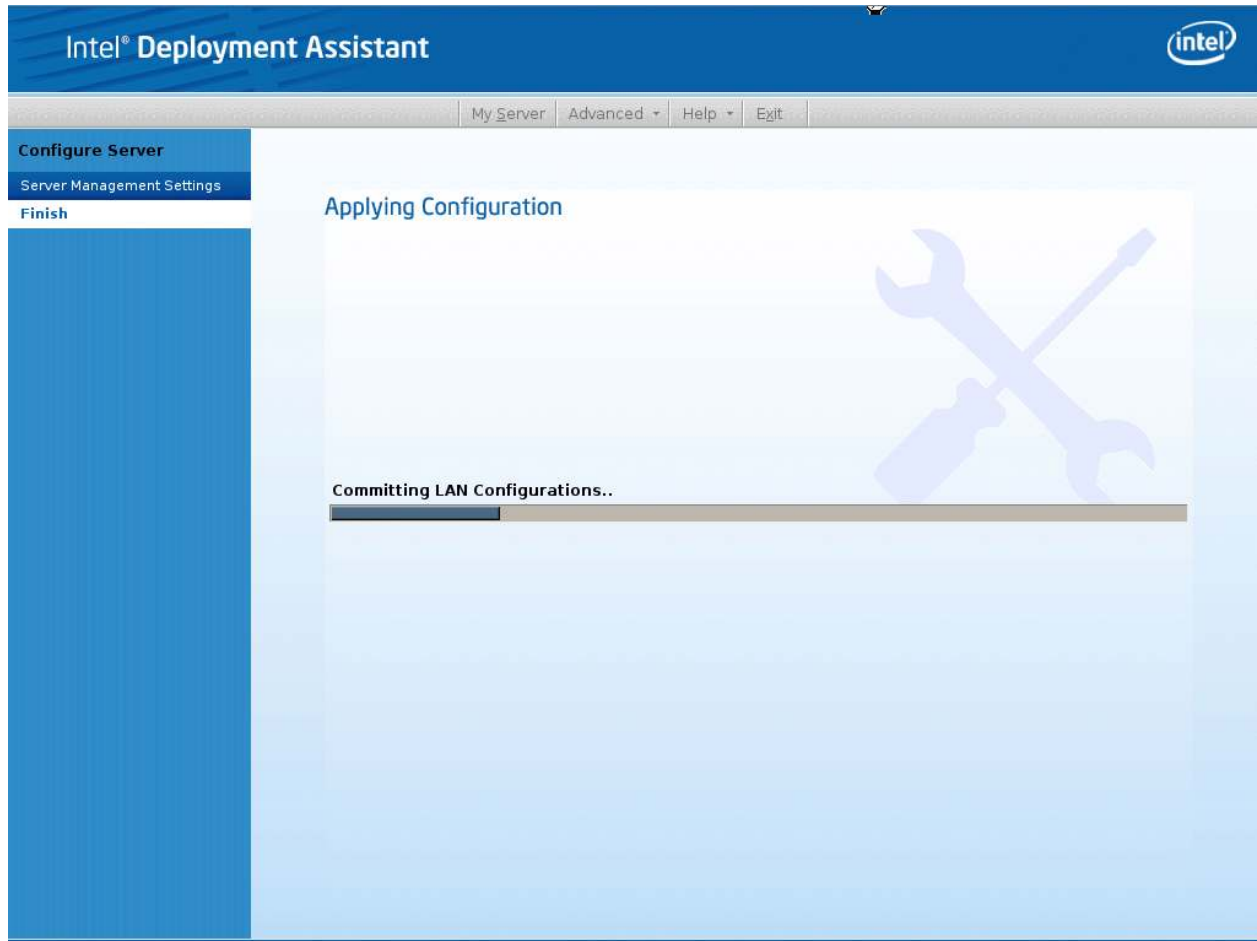


Figure 20: IDA Configure Server: Applying Configuration progress window

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. Select the **Restart** button.

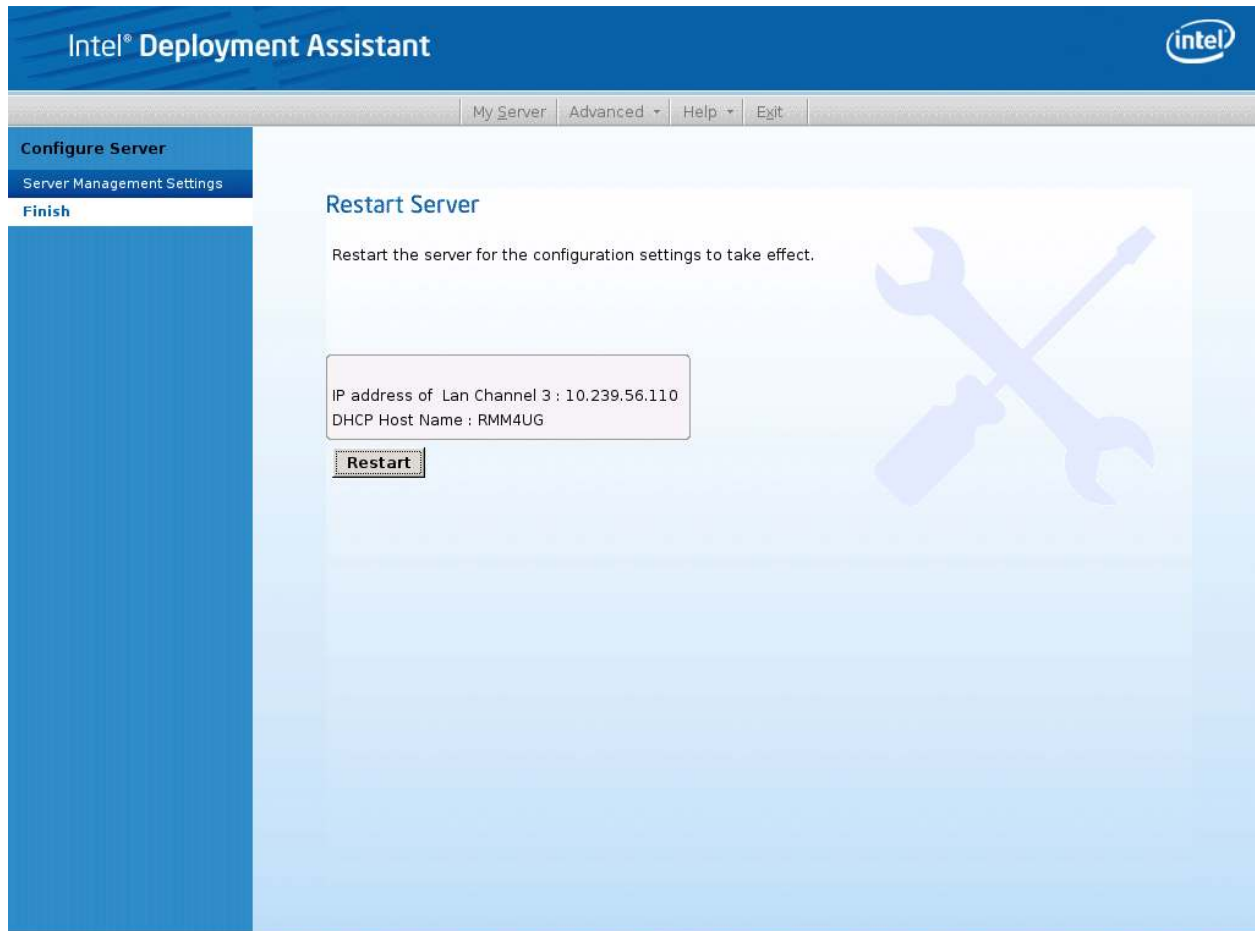


Figure 21: IDA Configure Server: Restart Server

4.3 Configuring Your Server Using Intel System Configuration Utility (SysConfig)

This section gives the basic commands needed to configure the RMM4 using SysConfig commands. This utility is supported in EFI, Linux*, and Windows*. The commands are the same for all the versions. At a minimum, you will 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 are using RMM4 Dedicated Server Management NIC LAN channel 3. If you are not using the RMM4 Dedicated Server Management NIC then substitute the appropriate channel number.

4.3.1 Configure User

Step by step instructions to enable a user for the RMM4

1. Set password for BMC user 2 (root) by typing:

```
syscfg /u 2 "root" "p@ssw0rd" (password is "p@ssw0rd" in this example)
```
2. Enable the BMC user 2 on LAN channel 3 by typing:

```
syscfg /ue 2 enable 3
```
3. Enable "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
```

4.3.2 Configuring 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
```

4.3.3 Configuring Serial Over LAN

- If needed, Serial Over LAN (SOL) can be enabled 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 via LAN or Internet. The Intel® Integrated BMC Web Console is part of the standard IBMC 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 Chapter 4. Before you log in, you must enable the intended user. The examples in this chapter will 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 via 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 will 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 strong encryption by opening the “Help/About” menu to read about the key length that is currently activated. Figure 22 shows the dialog box presented by the Internet Explorer 8.0*.



Figure 22: Internet Explorer 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 will display 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 add-on card into your web browser. In order to use a secure connection, type `https://<IPaddress of RMM4>/`. This will take you to the Intel® Integrated BMC Web Console module login page as shown in Figure 23.



Figure 23: 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 23) to view the RMM4 home page.

After the initial log in, 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 could 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 24:

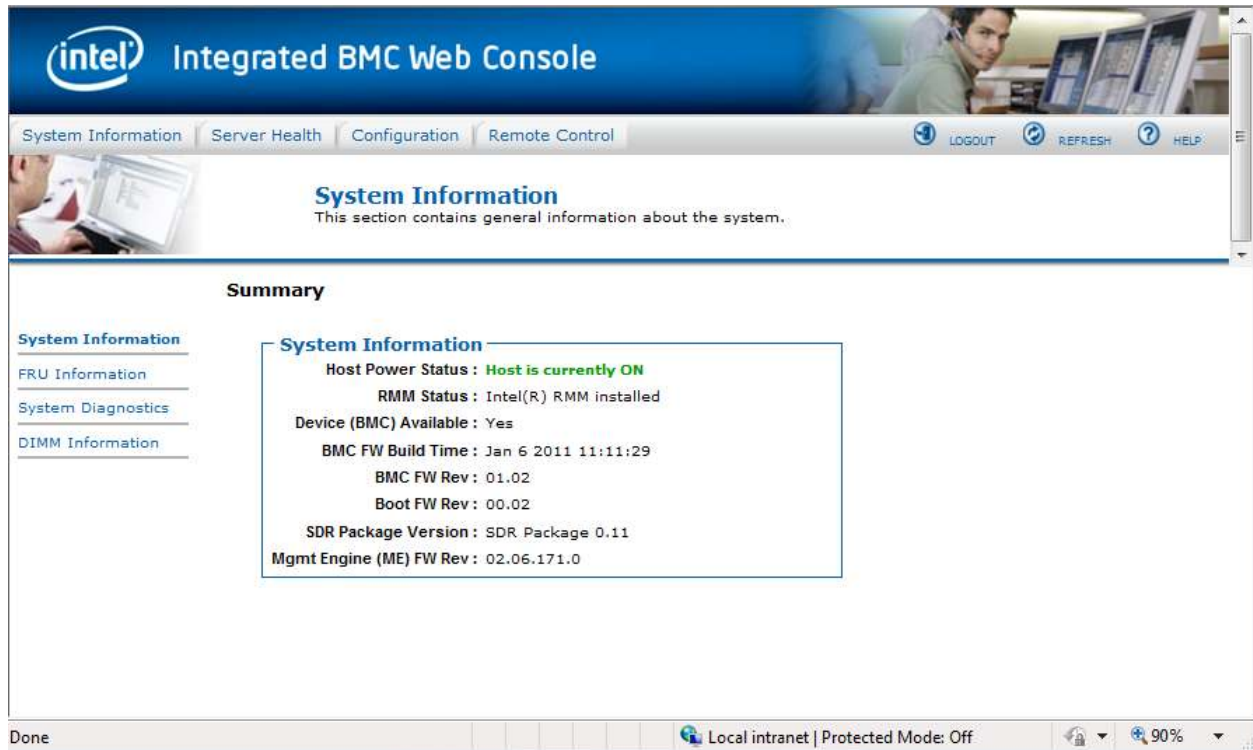

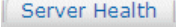




Figure 24: Integrated BMC Web Console Home Page

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 2: Integrated BMC Web Console home page tabs

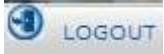


Tab	Function
	Click this tab to access general information about the server. The tab automatically opens the 'System Information' page: <ul style="list-style-type: none"> • System information • FRU information
	Click this tab for access to the sensors and event log. The tab automatically opens the 'Sensor Readings' page. <ul style="list-style-type: none"> • Sensor readings. • Event log

Tab	Function
	Click this tab to configure various settings for the server. The tab automatically opens the 'Network' configuration page. <ul style="list-style-type: none"> • Network • Users • LDAP • SSL • Remote Session • Mouse Mode
	Click this tab for access to the remote console and to control the power state of the server. <ul style="list-style-type: none"> • Console Redirection. • Server Power Control

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, Intel® Integrated BMC Web Console Options.

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 3: Horizontal Toolbar Buttons

Button	Function
	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.
	Click this button to refresh the current web page, including any data shown on the page.
	Click this button to view a brief description of the current page in a frame at the right-hand 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.

5.4 Online Help



The Web Console user interface gives specific online help for each page. For additional information on a certain topic or group of options, click the  button on the top horizontal toolbar to view the online help as shown in Figure 25. The right Help frame is visible only when the online Help is being accessed.



Figure 25: 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 26 and Figure 27.

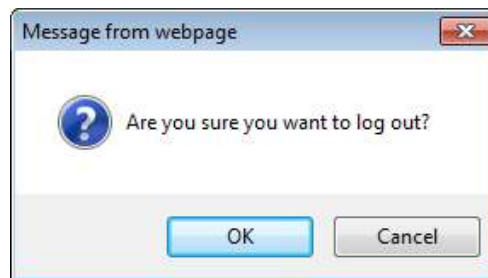


Figure 26: Logging Out of Integrated BMC Web Console – Step 1

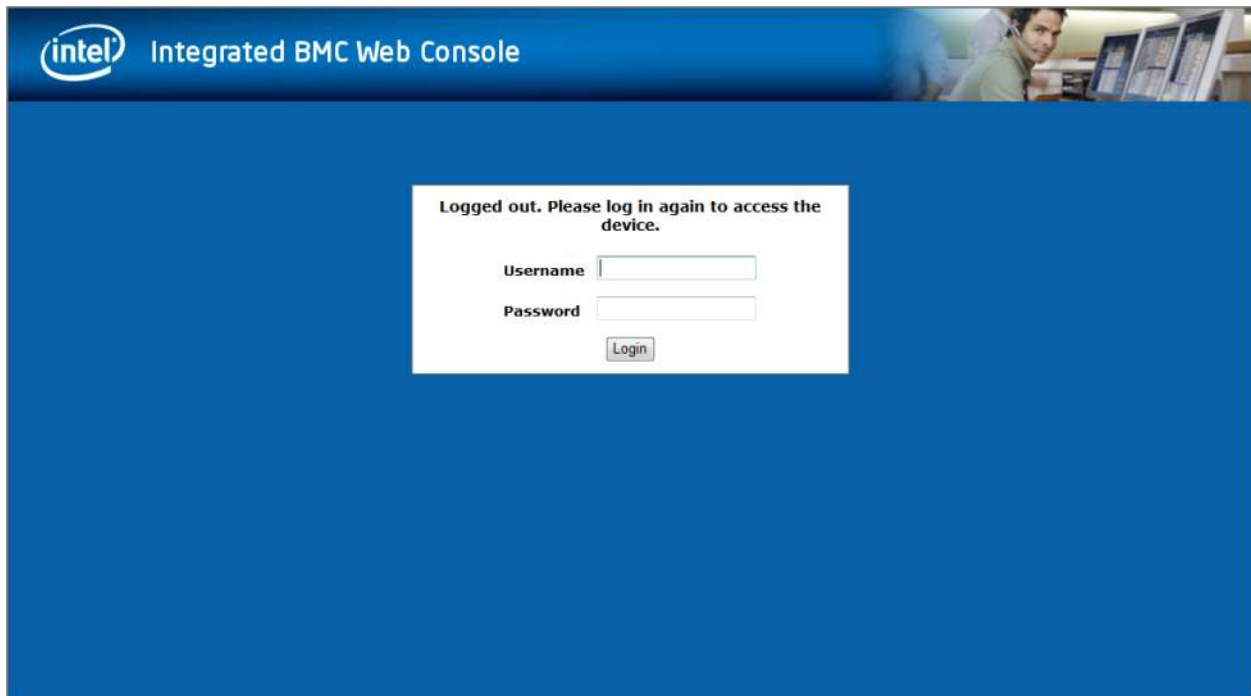


Figure 27: Logging Out of Integrated BMC Web Console – Step 2

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 screen, keyboard 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 his/her 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.



Figure 28: Remote Control Console Redirection window

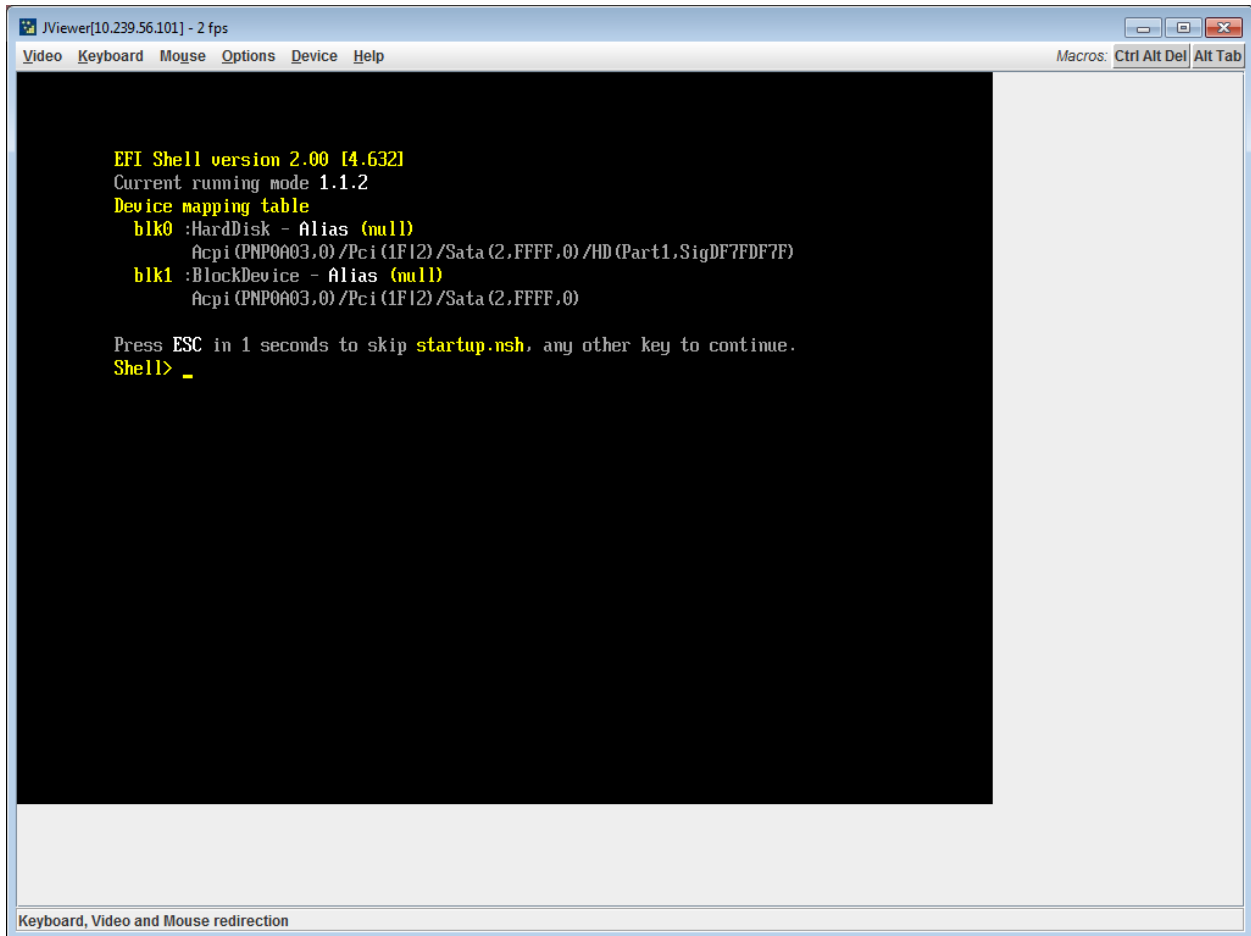
Click the **Launch Console** button to launch the redirection console and manage the server remotely.

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

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

Notes:

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

**Figure 29: 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 30.

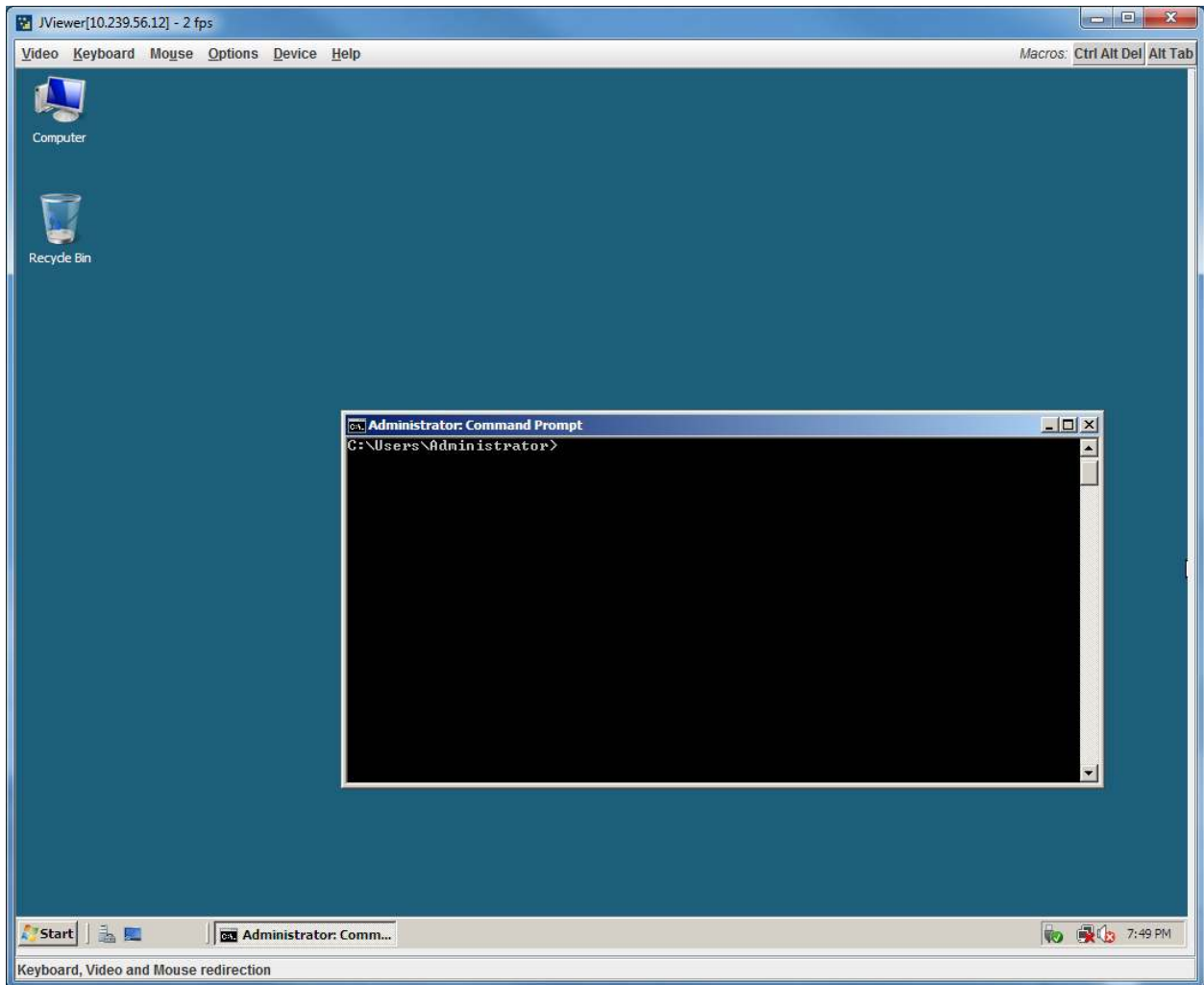


Figure 30: Remote Console Main Window

It displays the screen content of your remote server. The Remote Console will behave 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 31: 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** button in the Remote Console control bar to open the Remote console Video menu as shown in Figure 32:

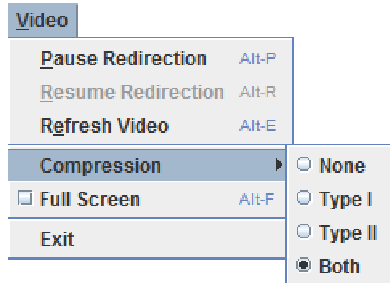


Figure 32: Remote Console Video Menu

Using this menu, you can do the following:

- **Pause Redirection.** Temporarily pauses redirection of keyboard, video, and mouse. The Remote Console window stops being updated. Keyboard shortcut is ALT+P.
- **Resume Redirection.** Resume 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 Remote Console.

6.3.2 Remote Console Keyboard Menu

Click **Keyboard** to open the Keyboard menu with options to perform tasks as shown in Figure 33:



Figure 33: 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 simulating 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.** Issue 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.

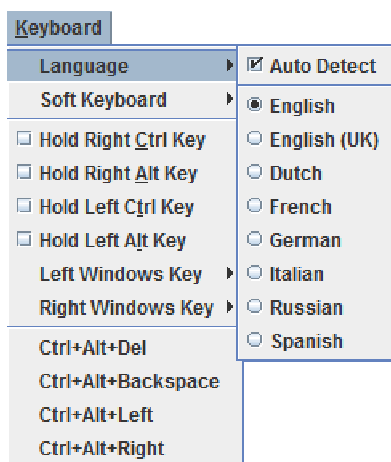


Figure 34: Remote Console Keyboard Language Sub Menu

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

The Remote Console Java application reverse 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.

Under 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 as the auto detect automatically and immediately follows any Language Bar changes. 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.

Under 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 under 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 with options to perform tasks as shown in Figure 35.



Figure 35: 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 the ALT+S shortcut.

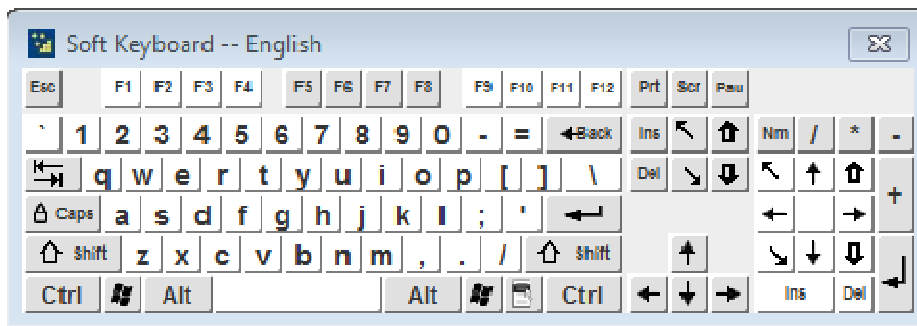


Figure 36: Remote KVM Soft Keyboard

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 since 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 with options to perform tasks as shown in Figure 37.

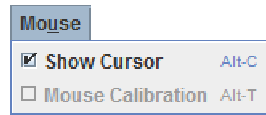


Figure 37: Remote Console Mouse Menu

The Mouse submenu offers two 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.

Relative Mode Mouse Calibration Procedure

1. If the remote mouse and local mouse cursor are not in synch, start mouse calibration by selection 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 the cursors will be IN SYNCH in the beginning.
3. Please use number pad '+' or '-' keys to change the threshold settings until both the cursors go out of synch.
4. Please detect the first reading on which cursors go out of synch.
5. Once 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 the cursors will be OUT OF SYNCH in the beginning.
7. Please 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 the cursors are in synch.
8. Please detect the first reading on which cursors are in synch.
9. Once detected, use 'ALT-T' to save the acceleration value.

6.3.4 Remote Console Options Menu

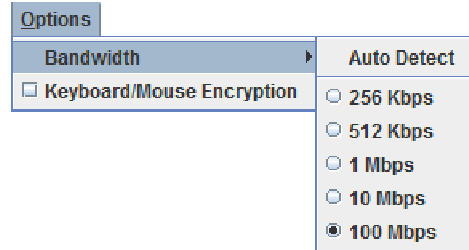


Figure 38: Remote Console Options Menu

Using this menu, you can do the following:

- **Bandwidth.** Changing the bandwidth setting affects low-level connection protocol parameters like 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 are 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

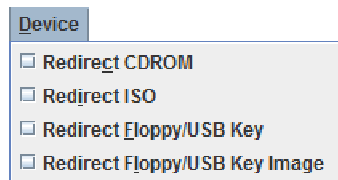


Figure 39: Remote Console Device Menu

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 last two options allow you to redirect either a local floppy drive, a local USB key drive, or a floppy .img file as a virtual floppy device on the remote system.

The virtual devices act just like any other CDROM 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.

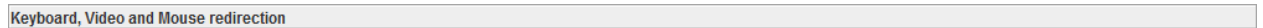
Note: The virtual devices are not limited to normal floppy/CDROM sizes and will be as large as the device or file being redirected. A USB Key drive is redirected as a virtual floppy device

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 40. As you navigate the menu options, the status line gives a more detailed definition of each option.



Keyboard, Video and Mouse redirection

Figure 40: 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-hand side is illustrated and described in detail.

Notes:

- The first menu item for each tab is the default page which 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 41.



Figure 41: 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

By default, the Integrated BMC Web Console home page opens is the System Information tab. It contains general information about the system as explained in the following sub sections.

7.1.1 Viewing System Information

The System information page displays a summary of the general system information as shown in Figure 42:

The screenshot shows the Intel Integrated BMC Web Console interface. The main content area is titled "System Information" and contains a "Summary" section. The summary lists the following details:

- Host Power Status:** Host is currently ON
- RMM Status:** Intel(R) RMM installed
- Device (BMC) Available:** Yes
- BMC FW Build Time:** Jan 6 2011 11:11:29
- BMC FW Rev:** 01.02
- Boot FW Rev:** 00.02
- SDR Package Version:** SDR Package 0.11
- Mgmt Engine (ME) FW Rev:** 02.06.171.0

A help sidebar on the right provides definitions for each status:

- Host Power Status:** Shows the power status of the host (on/off).
- RMM Status:** Indicates if the Remote Management Module (remote KVM 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 SDR package.
- ME FW Rev:** Major and minor firmware revision for the Management Engine (ME). Only available if the host is powered on.

Figure 42: System Information page

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

Table 4: System Information Details

Information	Details
Host Power Status	Shows the power status of the host (on/off).
RMM Status	Indicates if the Intel® RMM4 card is present.
Device (BMC) Available	Indicates if 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.

Information	Details
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.

7.1.2 Viewing Field Replaceable Unit (FRU) Information

The FRU Information page displays information from the FRU (Field Replaceable Unit) repository of the host system. See Figure 43 for details:

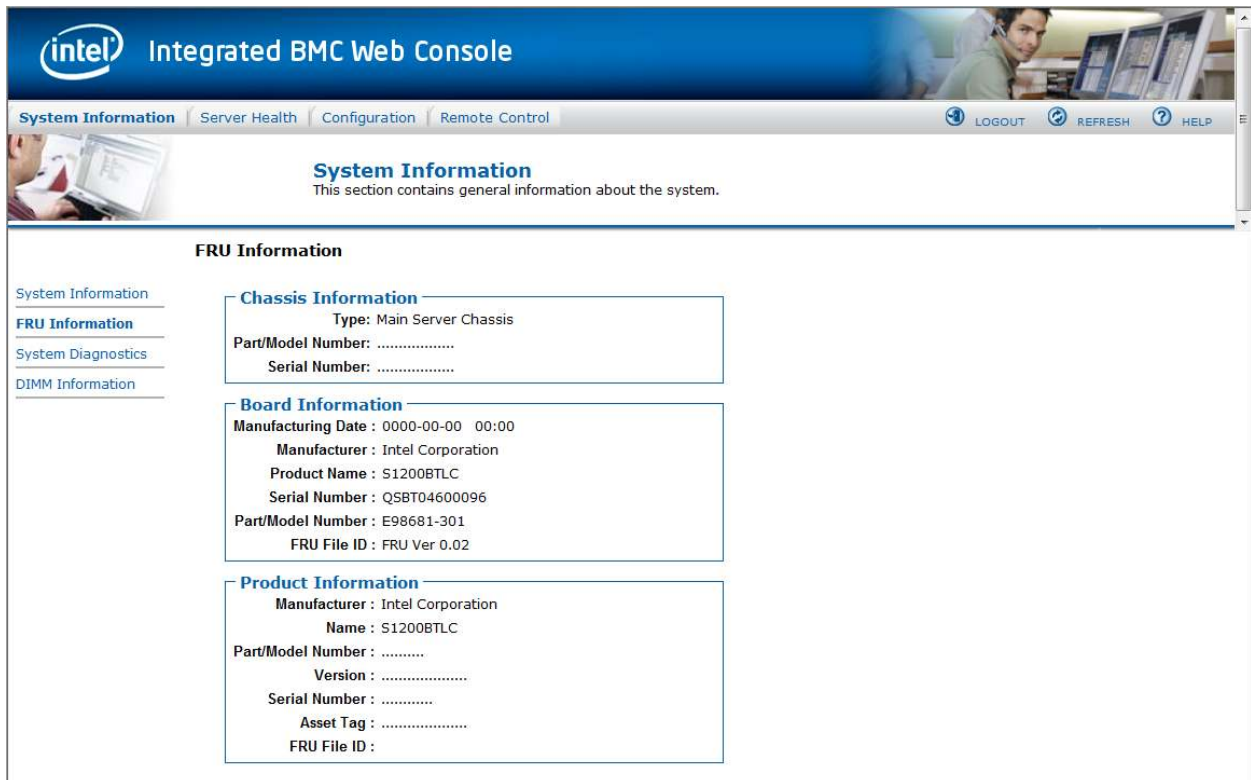


Figure 43: System Information FRU Information page

7.1.3 Viewing System Diagnostics Information

The System Diagnostics page displays information on System Diagnostics of the host system. Administrators can use this to run and collect data system-side. See Figure 44 for details:

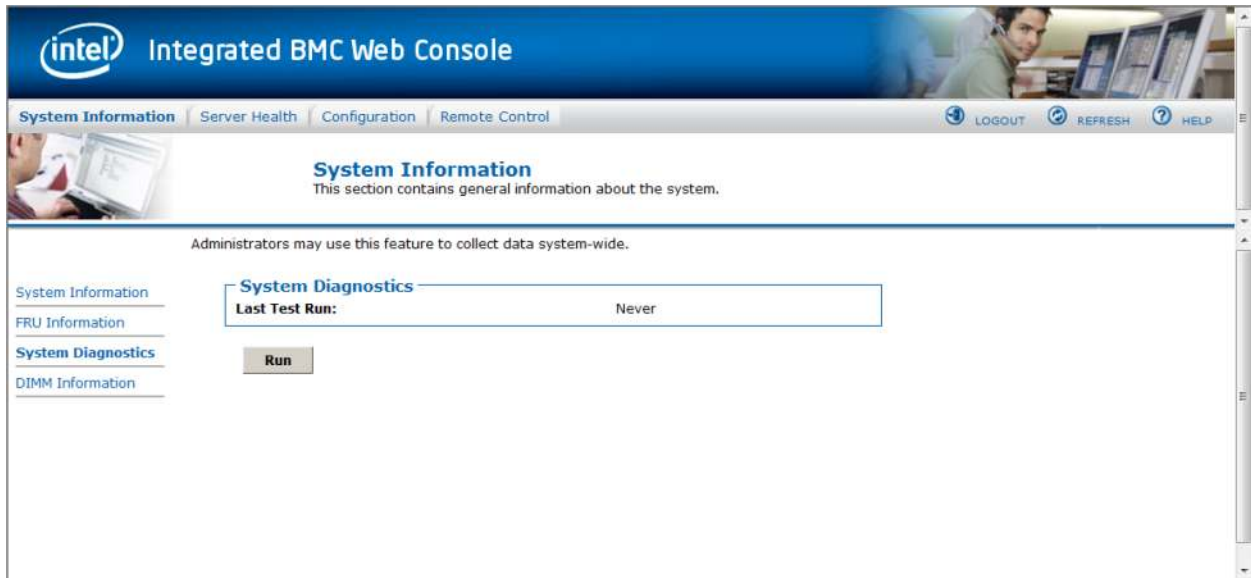


Figure 44: System Information System Diagnostics page

7.1.4 Viewing DIMM Information

The DIMM Information page displays information on DIMM modules installed on the host system. See Figure 45 for details:



Figure 45: System Information DIMM Information page

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. Click on the Server Health Tab to display the page. By default, this tab opens the sensor Readings page as shown in Figure 46.

7.2.1 Viewing Sensor Readings

The Sensor Readings page displays system sensor information including status, health, and reading.

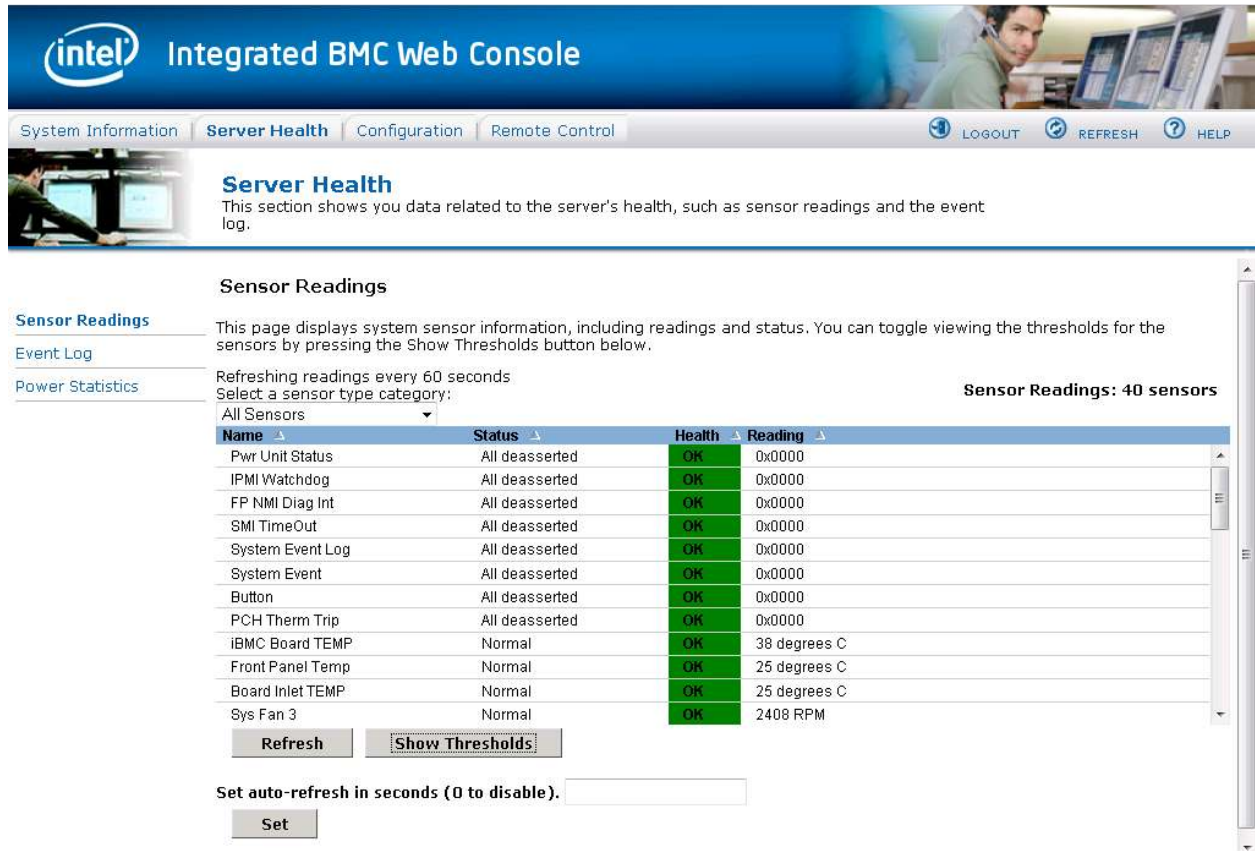


Figure 46: Server Health Sensor Reading's window (Thresholds not displayed)

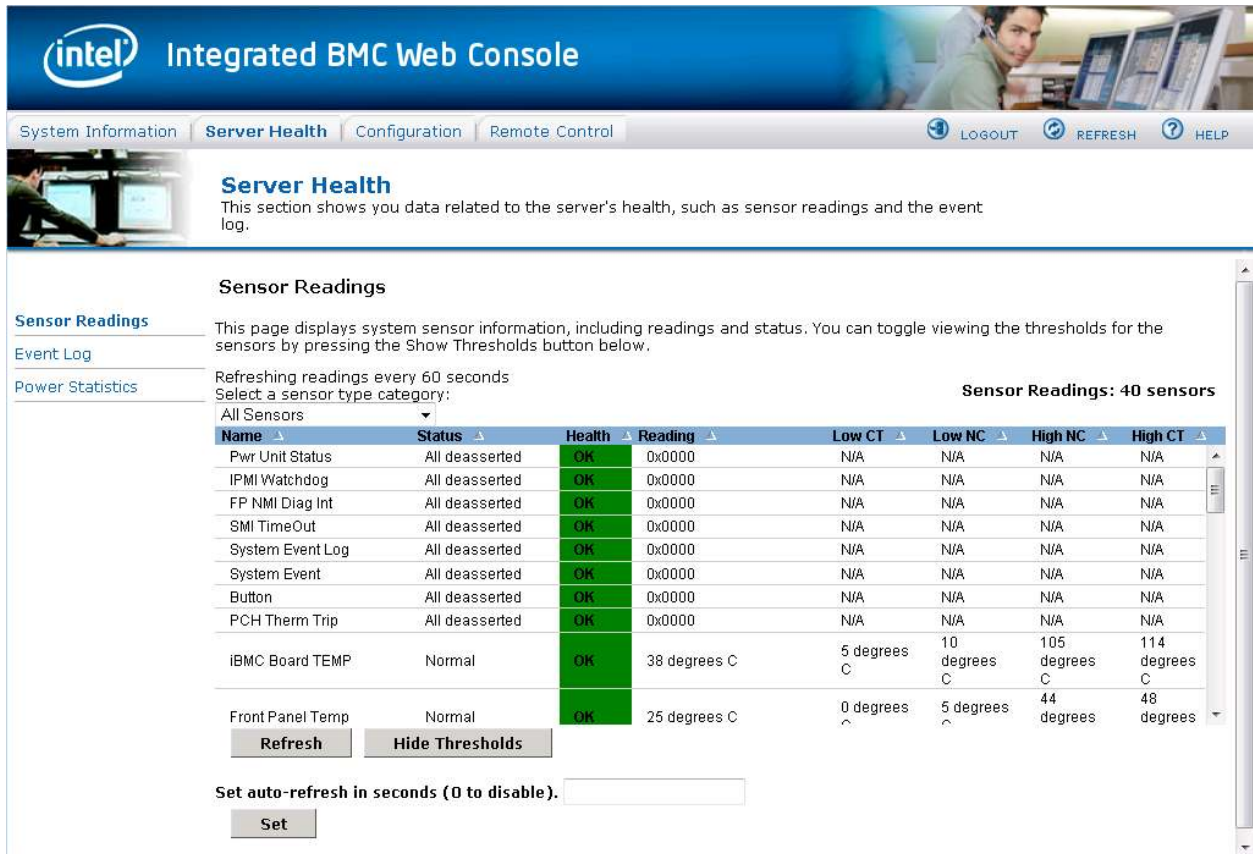


Figure 47: Server Health Sensor Reading's window (Thresholds displayed)

The following table lists the options available in this page:

Table 5: 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 see all sensors.
Sensor Readings list	Selected sensors shown with their name, status, health, and 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 display left and right.
Hide Thresholds button	Click to return to original display, hiding the threshold values
Refresh	Click to refresh the selected sensor readings

7.2.2 Viewing Event Log

The Event Log page displays the Event Log as shown in Figure 48.

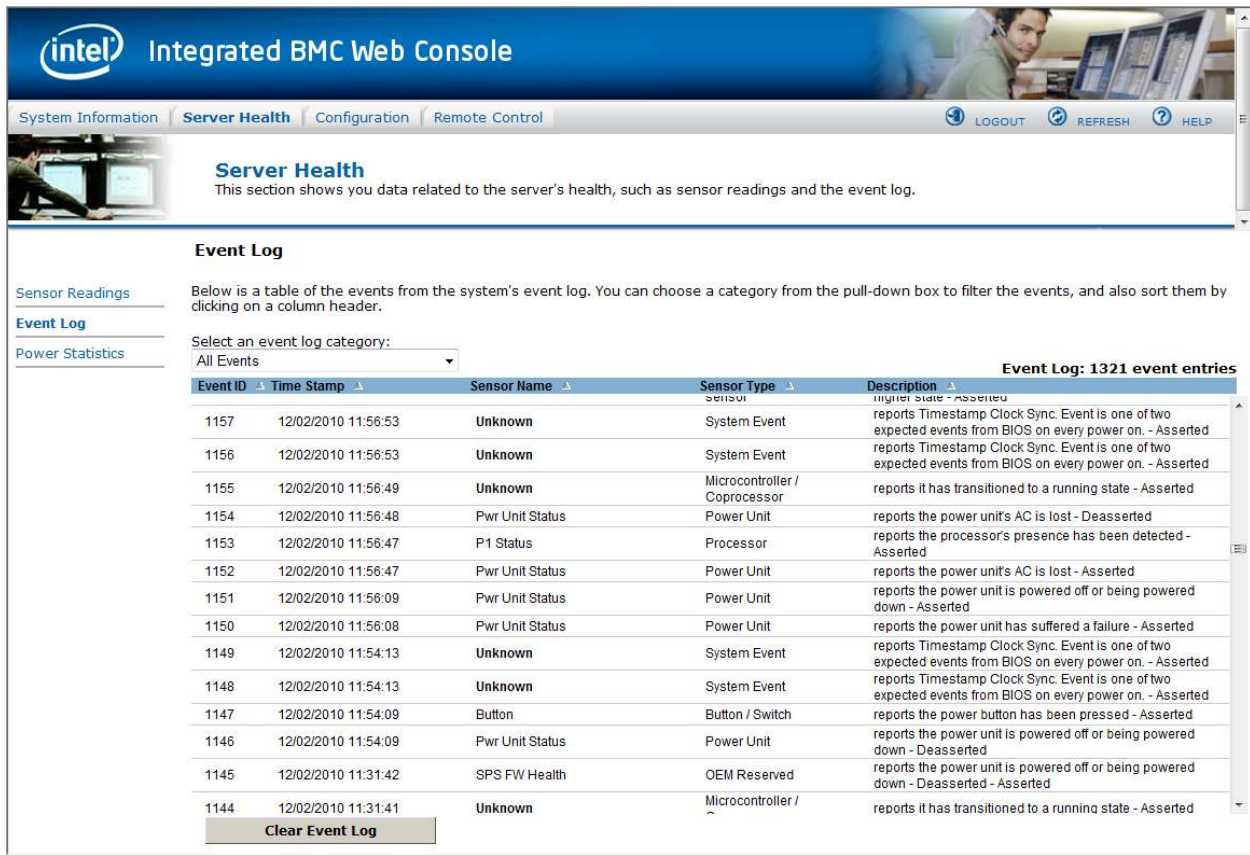


Figure 48: Server Health Event Log

The following table lists the options available in this page:

Table 6: Server Health (Event Log) Options

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.

7.2.3 Viewing Power Statistics

The Power Statistics page displays the systems power statistics in watts as shown in Figure 49.

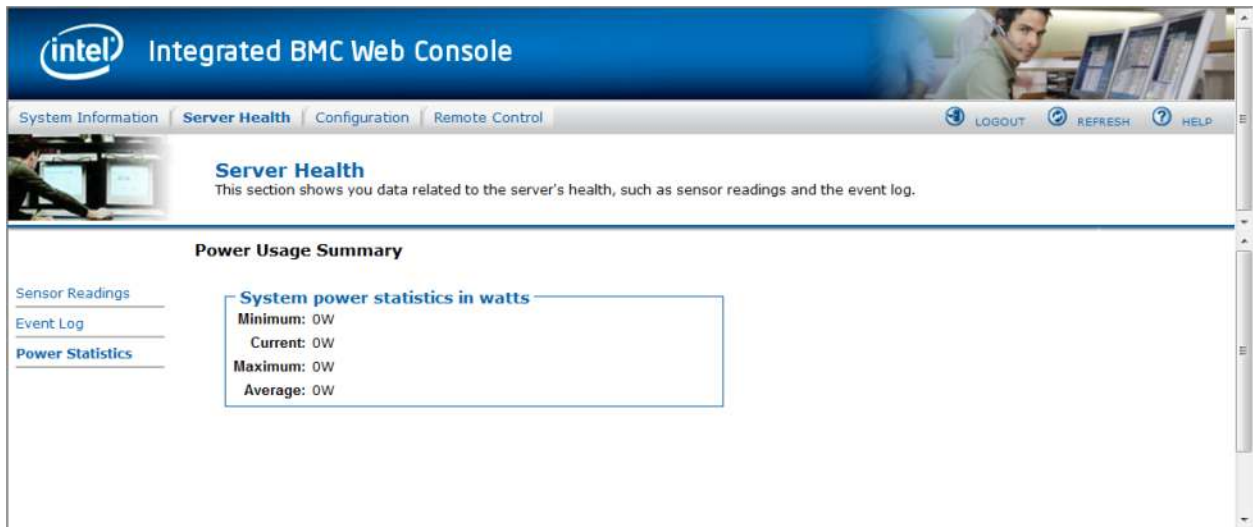


Figure 49: Server Health Power Statistics

7.3 Configuration Tab

The Configuration tab is used to configure various settings as shown in Figure 50. By default, it opens in the Network Settings window as shown in Figure 51.

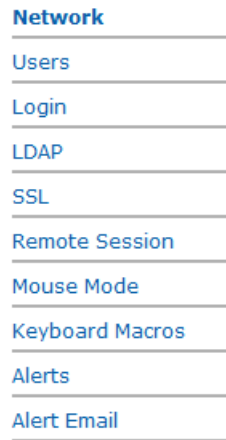


Figure 50: Configuration

7.3.1 Configuring Network Settings

The Network settings page is used to configure the network settings. It provides options to do either of the following:

⚠ WARNING

The RMM4 IP address must be on a different subnet than the baseboard IP address used for management traffic.

- **Automatic:** Obtain an IP address automatically (using DHCP)
- OR
- **Manual:** Manually configure the IP address.

Figure 51: Configuration Network Settings window

The following table lists the options available in this page:

Table 7: Configuration (Network Settings) Options

Option	Task
LAN Channel Number drop-down box	It lists the LAN Channel(s) available for server management. The LAN channels describe the physical NIC connection on the server. Intel® RMM4 channel is the add-in RMM4 NIC. The Baseboard Mgmt channel (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system.
MAC Address	The MAC address of the device (read only)

Option	Task
IP Address	Select the type of IP assignment with the radio buttons. If configuring a static IP, enter the requested address, subnet mask, and gateway in the given fields. <ul style="list-style-type: none"> • IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". <ul style="list-style-type: none"> — 'xxx' ranges from 0 to 255 — First 'xxx' must not be 0
Save button	Click to save any changes made

7.3.2 Managing Users

The User List page lists the configured users, along with their status and network privilege.

User List

The list below shows the current list of configured users.

If you would like to modify or delete a user, select their name in the list and click Modify User or Delete User. To add a new user, select an unconfigured slot and click Add User.

Number of configured users: 5

UserID	User Name	User Status	Network Privilege
1	anonymous	disabled	Administrator
2	root	disabled	Administrator
3	admin	ENABLED	Administrator
4	test2	disabled	Administrator
5	test3	disabled	Administrator
6	~	~	~
7	~	~	~
8	~	~	~
9	~	~	~
10	~	~	~
11	~	~	~
12	~	~	~
13	~	~	~
14	~	~	~
15	~	~	~

Figure 52: Configuring User List window

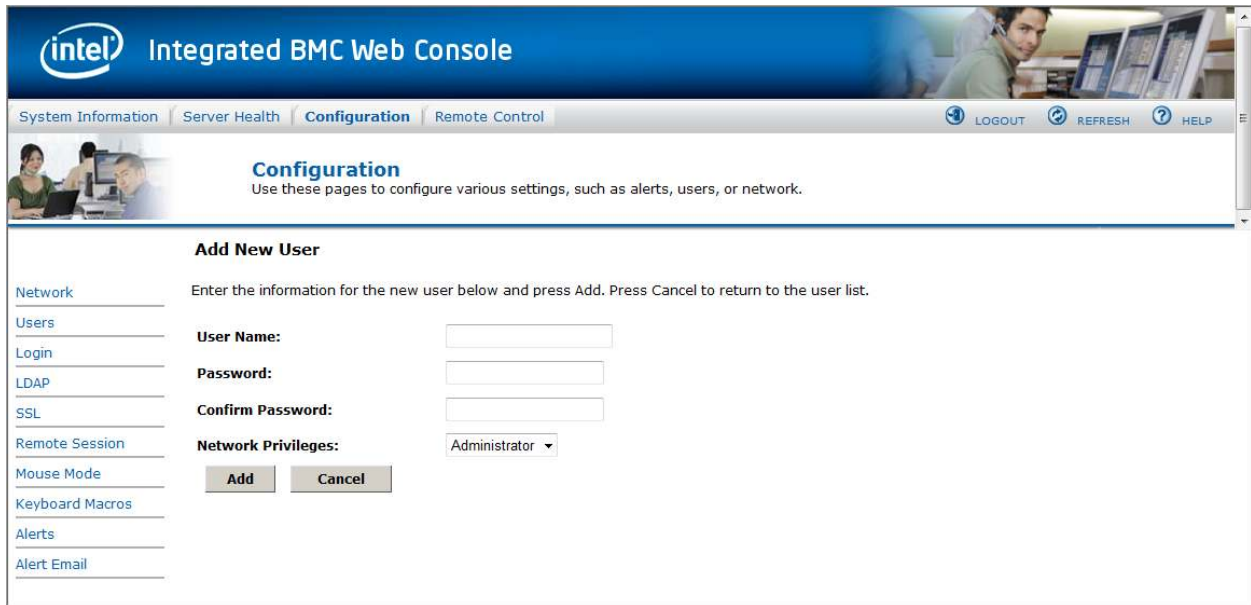
This page has options to configure the IPMI users and privileges for this server.

Notes:

- 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 user, select a user in the list and click Delete User.

To add 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 53.



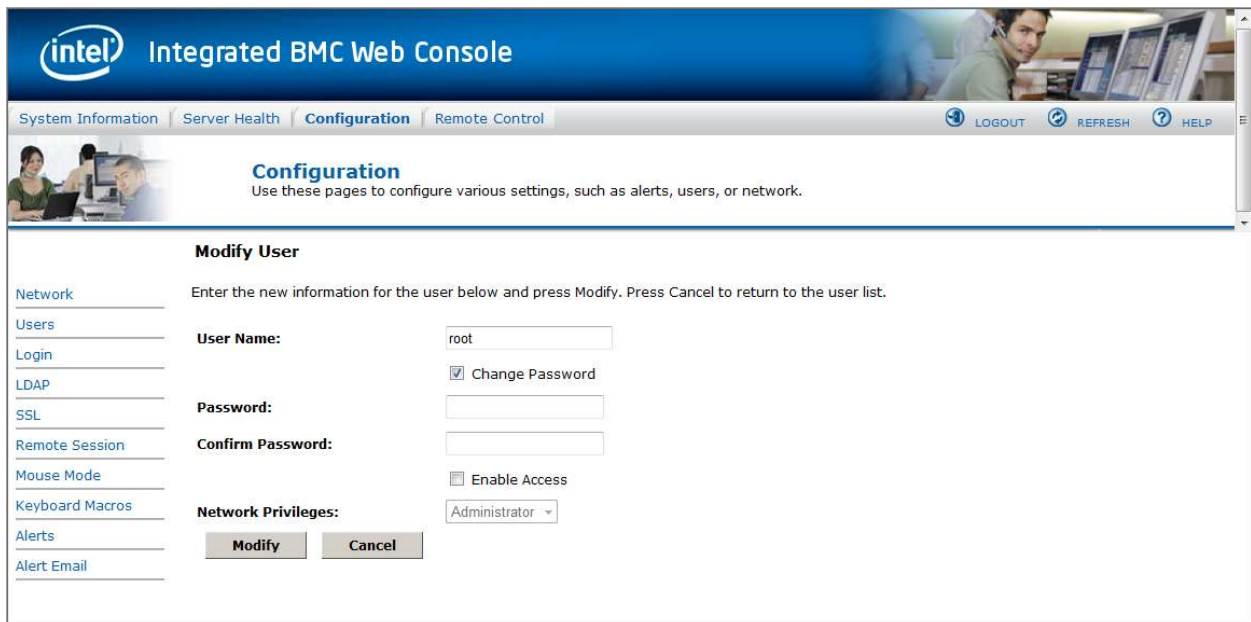
The screenshot shows the 'Add New User' window in the Intel Integrated BMC Web Console. The interface includes a navigation bar with 'System Information', 'Server Health', 'Configuration', and 'Remote Control'. The 'Configuration' section is active, and the 'Add New User' form is displayed. The form contains the following fields and options:

- User Name:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Network Privileges:** A dropdown menu set to 'Administrator'.
- Buttons:** 'Add' and 'Cancel' buttons.

On the left side, there is a sidebar menu with options: Network, Users, Login, LDAP, SSL, Remote Session, Mouse Mode, Keyboard Macros, Alerts, and Alert Email.

Figure 53: Configuring Users Add User window

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 54.



The screenshot shows the 'Modify User' window in the Intel Integrated BMC Web Console. The interface is similar to the 'Add New User' window, but with the following differences:

- User Name:** The text input field contains 'root'.
- Change Password:** A checked checkbox.
- Enable Access:** An unchecked checkbox.
- Buttons:** 'Modify' and 'Cancel' buttons.

The sidebar menu on the left is identical to the 'Add New User' window.

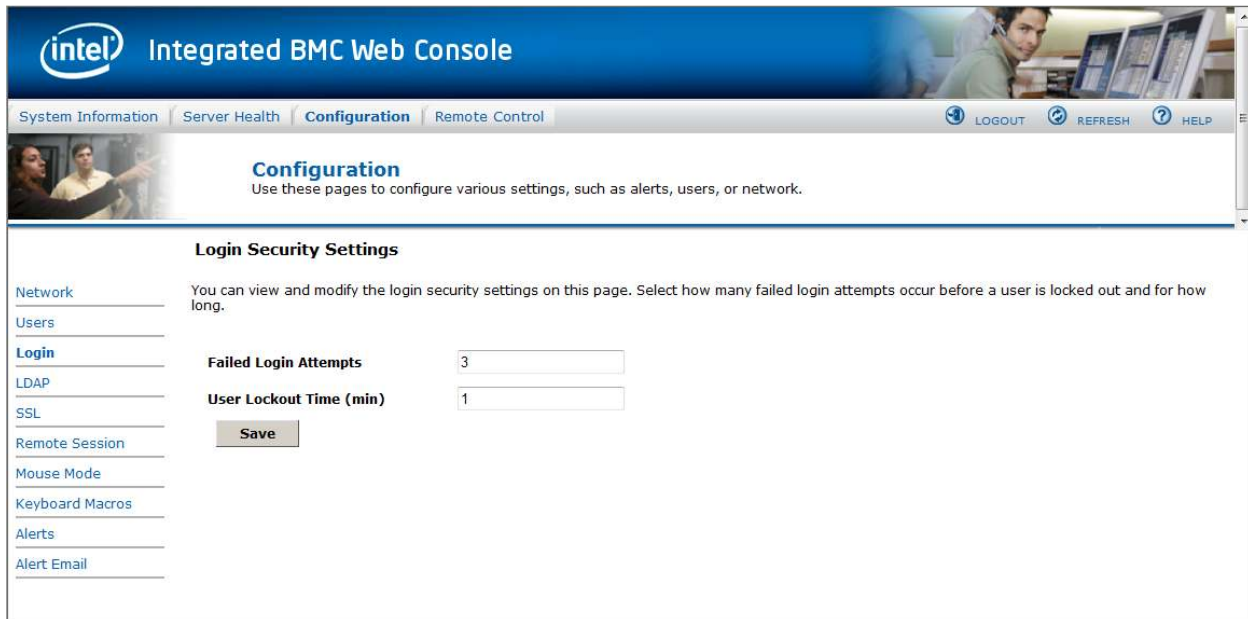
Figure 54: Configuring Users Modify User window

7.3.3 Login Security Settings

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. Default is 3 failures will lockout a user for 1 minute.



The screenshot displays the Intel Integrated BMC Web Console interface. At the top, there is a blue header with the Intel logo and the text "Integrated BMC Web Console". Below the header, a navigation bar contains tabs for "System Information", "Server Health", "Configuration" (which is active), and "Remote Control". To the right of the navigation bar are buttons for "LOGOUT", "REFRESH", and "HELP".

The main content area is titled "Configuration" and includes a sub-header "Login Security Settings". Below this, there is a sidebar with a list of configuration categories: Network, Users, Login (highlighted), LDAP, SSL, Remote Session, Mouse Mode, Keyboard Macros, Alerts, and Alert Email. The main content area contains the following text and form fields:

Login Security Settings

You can view and modify the login security settings on this page. Select how many failed login attempts occur before a user is locked out and for how long.

Failed Login Attempts

User Lockout Time (min)

Figure 55: Configuring Login Security Settings window

7.3.4 Configuring LDAP Settings

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

The screenshot shows the Intel Integrated BMC Web Console interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration', and 'Remote Control'. The 'Configuration' section is active, with a sub-header 'LDAP Settings'. Below this, there is a 'Save' button and a list of configuration options: 'Enable LDAP Authentication' (checkbox), 'Port' (text input with '389'), 'IP Address' (text input), 'Searchbase' (text input), 'Bind DN' (text input), and 'Bind Password' (text input). A 'Save' button is located at the bottom left of the configuration area.

Figure 56: Configuring LDAP Settings window

The following table lists the options available in this page:

Table 8: Configuration (LDAP Settings) Options

Option	Task
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 <ul style="list-style-type: none"> IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx" 'xxx' ranges from 0 to 255 First 'xxx' must not be 0
Bind Password	Authentication password for LDAP server; the password must be at least 4 characters long
Bind DN	The Distinguished Name of the LDAP server, e.g. "cn=Manager, dc=my-domain, dc=com"
Searchbase	The searchbase of the LDAP server, for example, "dc=my-domain, dc=com"
Save button	Click to save the current settings

7.3.5 Configuring SSL Upload

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

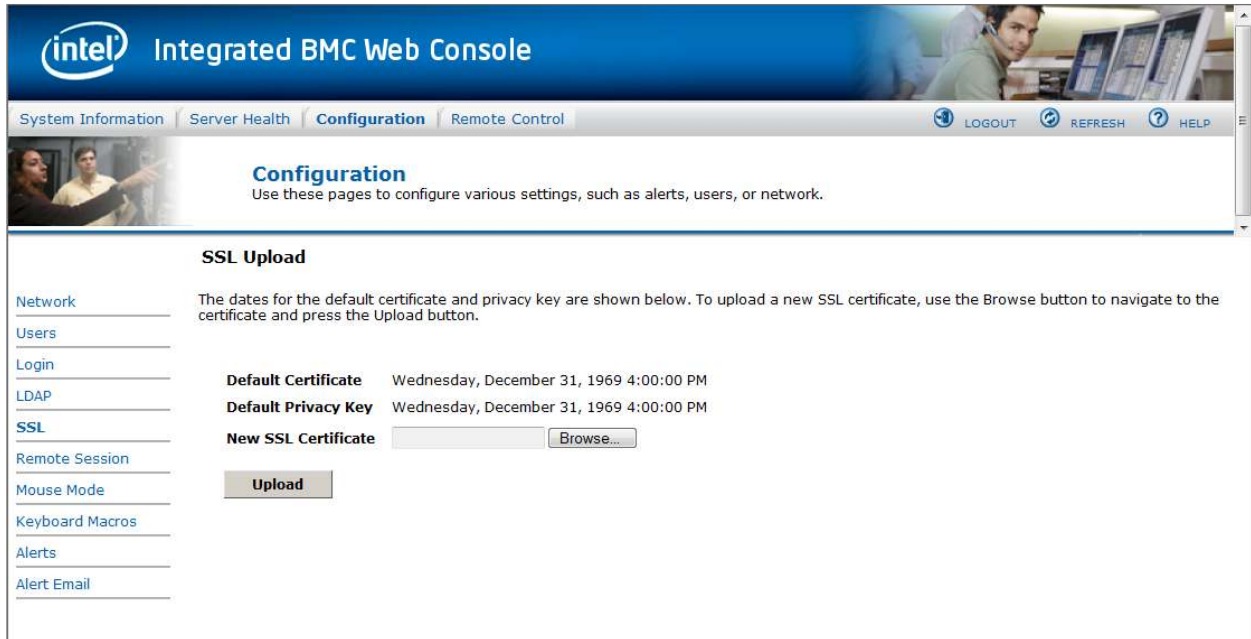


Figure 57: Configuring SSL Upload window

First upload the SSL certificate and then the device will prompt to upload privacy key. If either of the files is invalid the device will notify. The device will give notification on Successful upload. On successful upload, device will prompt to reboot the device. 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.

7.3.6 Configuring Remote Session

Use this page to enable/disable encryption on KVM or Media during a redirection session.



Figure 58: Configuring Remote Session window

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 9: Configuration (Remote Session) Options

Option	Task
Enable/Disable Encryption mode	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.
Save button	Click to use selected modes.

7.3.7 Configuring Mouse Mode

Click the **Mouse Mode** tab to view the Mouse Mode Setting window as shown in Figure 59.

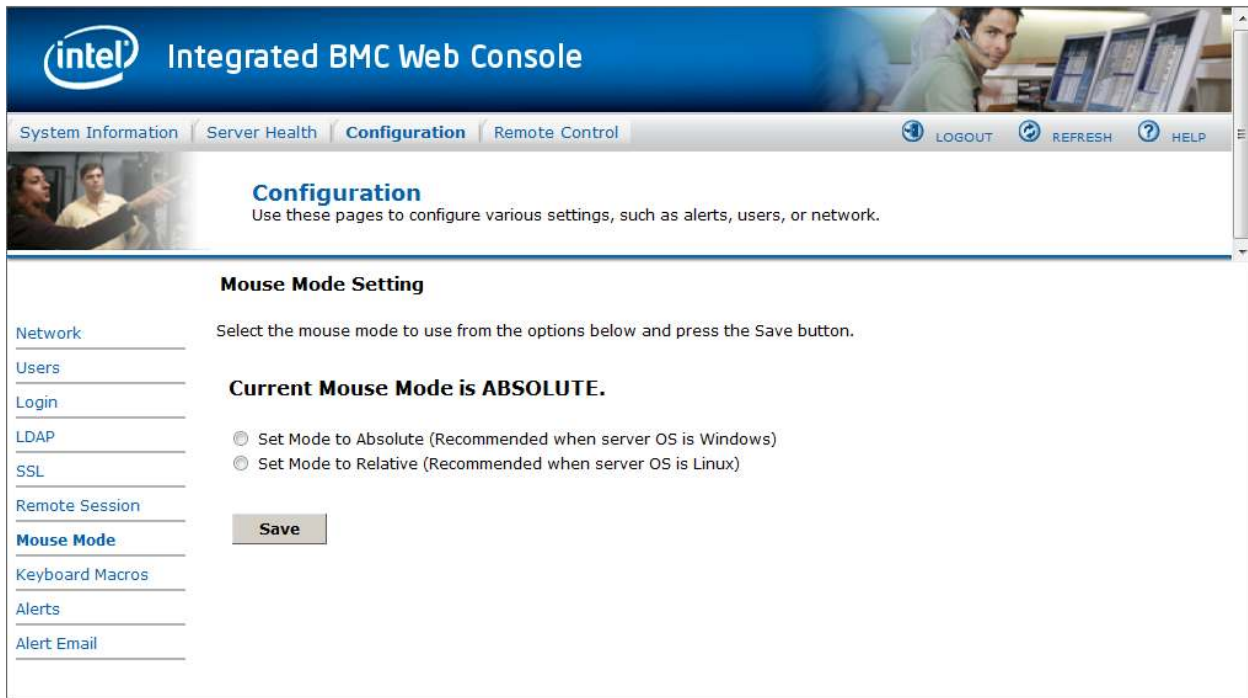


Figure 59: Configuring Mouse Mode Setting window

The Redirection Console handles mouse emulation from local window to remote screen in either of two methods:

- **Absolute Mode.** Select to have the absolute position of the local mouse sent to the server. Use this mode for 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.

7.3.8 Configuring Keyboard Macros

Macro buttons can be defined on this page that will 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.

The screenshot shows the 'Configuration' page of the Intel Integrated BMC Web Console. The 'Keyboard Macros' section is active, displaying a table for defining macros. The table has two columns: 'Key Sequence' and 'Button Name'. There are 10 rows, numbered #1 to #10. The first two rows are pre-filled with 'Ctrl+Alt+Del' and 'Alt+Tab' respectively. A 'Save' button is located at the bottom of the table.

	Key Sequence	Button Name
#1	Ctrl+Alt+Del	Ctrl Alt Del
#2	Alt+Tab	Alt Tab
#3		
#4		
#5		
#6		
#7		
#8		
#9		
#10		

Figure 60: Configuring Keyboard Macros window

This makes it convenient to quickly do oft repeated typing as well as execute key combos that aren't possible directly from the local client keyboard. Alt and Win key combos such as Ctrl+Alt+Del get interpreted by the local client OS and aren't 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, and then only the next time the Remote Console is launched – changes will not affect a Remote Console already running.

7.3.8.1 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 scancodes that get interpreted by the target OS, so they will be affected by modifiers such as Numlock as well as the target OS keyboard language setting.

Table 10: 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)	

7.3.9 Configuring Alerts

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.

Alerts

Configure which system events generate Alerts and the external network destinations they should be sent to.

Select the events that will trigger alerts:

<input type="checkbox"/> Temperature Sensor Out of Range	<input type="checkbox"/> Watchdog Timer
<input type="checkbox"/> System Restart	<input type="checkbox"/> Voltage Sensor Out of Range
<input type="checkbox"/> Fan Failure	<input type="checkbox"/> Chassis Intrusion
<input type="checkbox"/> Power Supply Failure	<input type="checkbox"/> Memory Error
<input type="checkbox"/> BIOS: Post Error Code	<input type="checkbox"/> FRB Failure
<input type="checkbox"/> Node Manager Exception	<input type="checkbox"/> Hard Drive Failure

LAN Channel to Configure: Baseboard Mgmt

Alert Destination #1:

SNMP Send SNMP Alerts to IP: 0.0.0.0

Email Send Email to:

Alert Destination #2:

SNMP Send SNMP Alerts to IP: 0.0.0.0

Email Send Email to:

Figure 61: Configuring Alerts window

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 11: 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 destination for.
Alert Destination #1/#2	Select either SNMP along with the IP address or email address that the alert should be sent to. Up to 2 destinations can be selected for each LAN channel.
Save button	Click to use selected setup.
Send Test Alerts	After configuring select this to send a test alert.

7.3.10 Configuring Alert Email

Use this page to configure the parameter for Alert Emails.

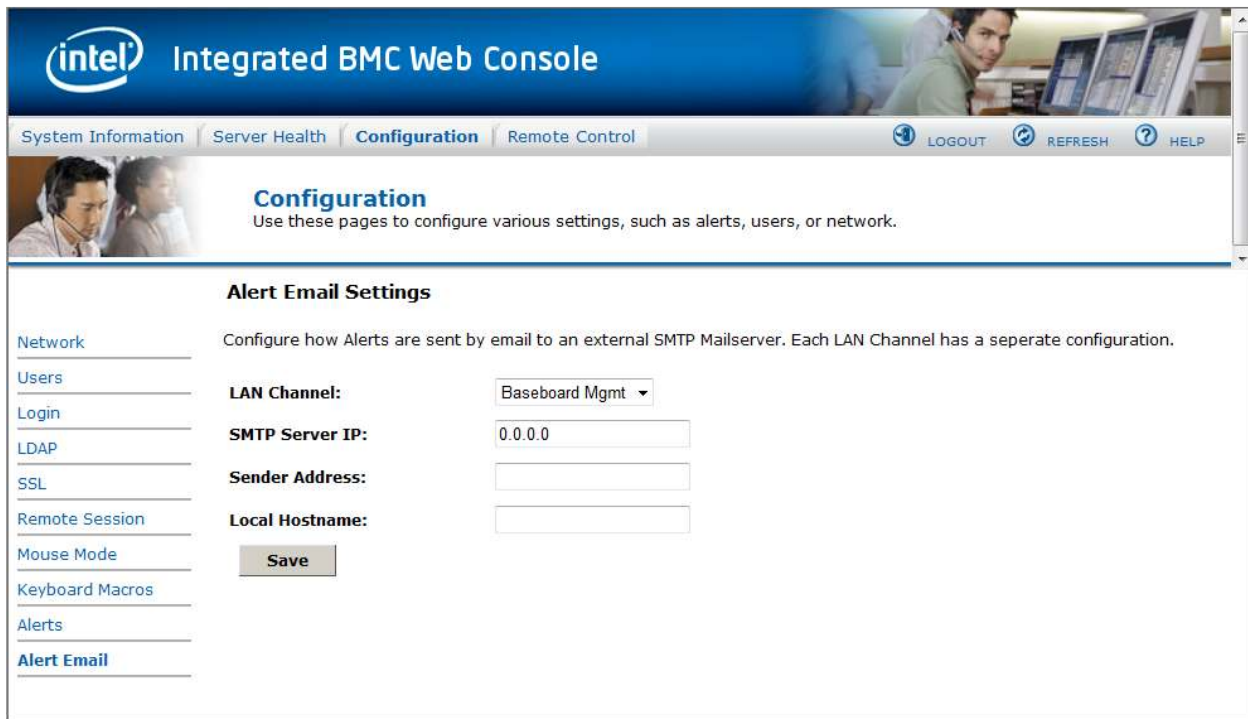


Figure 62: Configuring Alert Email window

Table 12: Configuration (Alert Email) Options

Option	Task
LAN Channel	Select either the BMC or RMM4 to configure destination for.
SMTP Server IP.	<p>The IP address of the remote SMTP Mailserver that Alert email should be sent to.</p> <ul style="list-style-type: none"> IP Address is made of 4 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	<p>The hostname of the local machine that is generating the alert. It is put into the outgoing Alert email.</p> <ul style="list-style-type: none"> The Local Hostname is a string of maximum 31 alpha-numeric characters. Space, Special Characters are not allowed.
Save button	Click to use selected setup.

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

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

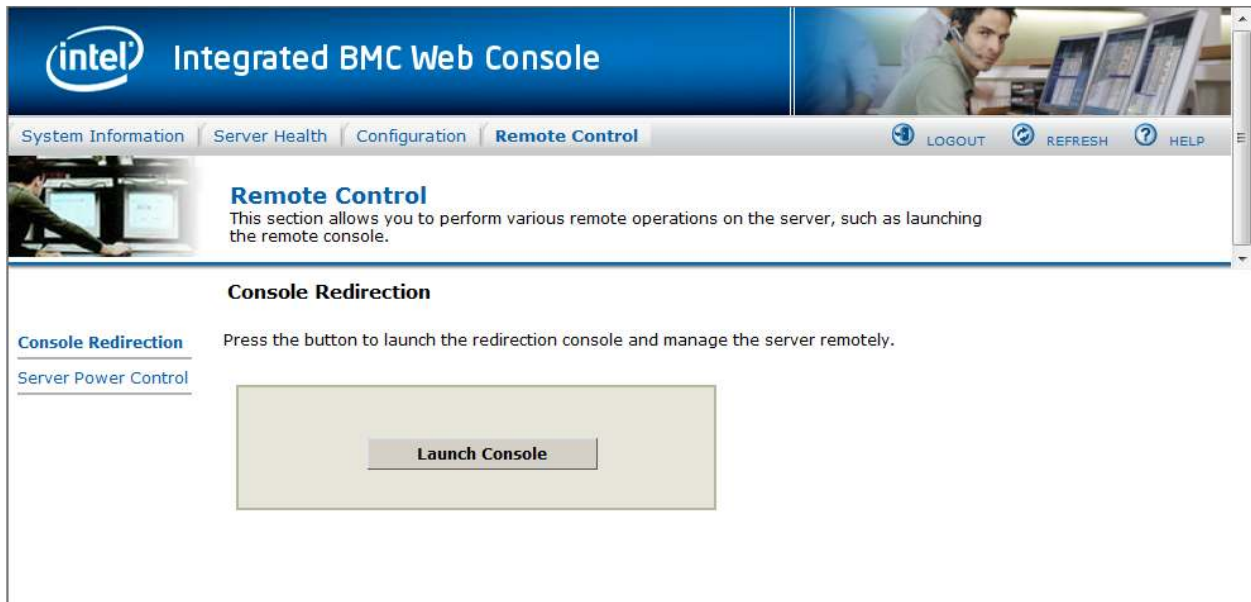


Figure 63: Remote Control Console Redirection window

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

Note: Java Run-Time Environment (JRE, Version 6 Update 22 or higher) must be installed on the client prior to launch of JNLP file.

7.4.2 Server Power Control

The Server Power Control page shows the power status of the server.

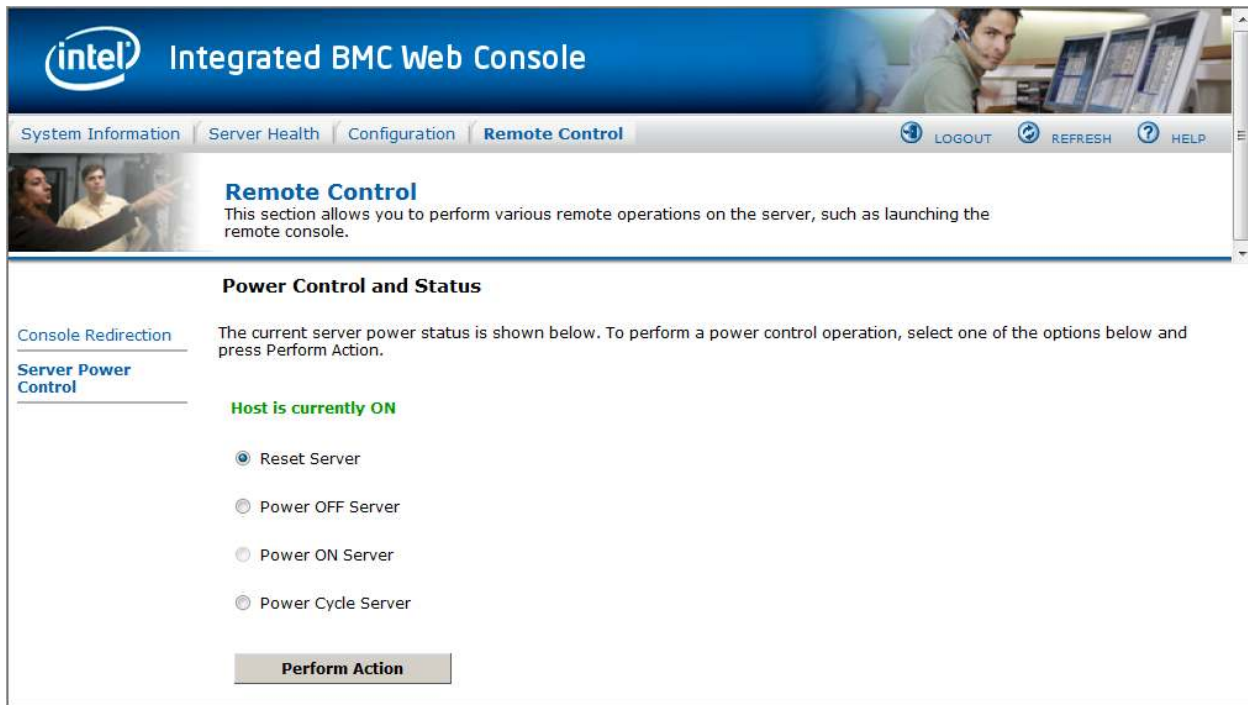


Figure 64: Server Power Control window

The following power control operations can be performed:

Table 13: Remote Control (Power Control) Options

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
Power ON Server	Select option to power on the host
Power Cycle Server	Select option to immediately power off the host, 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 via the KVM interface or other interface before initiating power actions.	