

Intel® Remote Management Module 3 User Guide

Revision 1.4
November, 2012

Revision History

Date	Revision Number	Modifications
August 2009	1.1	Updated document for feature updates (international keyboard support and soft keyboard) and review feedback.
September 2010	1.2	Added RMM3 variations –RMM3 Lite and RMM3 Lite-V.
June 2012	1.3	<ul style="list-style-type: none">• Corrections to SMASH section.• Added System Debug page.• Fixed minor typographical errors.
November 2012	1.4	<ul style="list-style-type: none">• Added note for About button.• Added note for F5 and page refresh not being supported.

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 3 Overview.....	7
2.1 Intel® RMM3 Features	7
2.1.1 RMM3 Lite and RMM3 Lite-V	8
2.2 Supported Operating Systems	8
2.2.1 Server System.....	9
2.2.2 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 on Intel® Server Boards S5500UR and S5500WB	11
3.3.2 Installation on Intel® Server Boards S5520HC, S5520BC, and S5520SC	12
3.3.3 Installation on Intel® Server Board S3420GPRX.....	13
3.3.4 Installation on Intel® Server System SR1640TH	13
4. Configuring Intel® RMM3.....	15
4.1 Configuring your Intel® RMM3 through BIOS setup	16
4.2 Configuring Your Intel® RMM3 Using the Intel® Deployment Assistant (IDA)	17
4.3 Configuring Your Server Using Intel System Configuration Utility (SysConfig)	24
4.3.1 Running the Sysconfig	24
4.3.2 Configuring IP address.....	24
4.3.3 Configuring Users	24
5. Getting Started with Intel® RMM3 Operation.....	25
5.1 Before You Begin	25
5.1.1 Client Browsers	25
5.2 Logging In	26
5.3 Navigation	27
5.4 Online Help	28
5.5 Logging Out	29
6. Remote Console (KVM) Operation	31
6.1 Launching the Redirection Console.....	31
6.2 Main Window.....	33

6.3	Remote Console Control Bar.....	34
6.3.1	Remote Console Video Menu.....	34
6.3.2	Remote Console Keyboard Menu.....	35
6.3.3	Remote Console Mouse Menu.....	38
6.3.4	Remote Console Options Menu.....	39
6.3.5	Remote Console Device Menu.....	39
6.4	Remote Console Status Line.....	40
7.	Intel® RMM3 Web Console Options.....	41
7.1	System Information.....	42
7.1.1	Viewing System Information.....	42
7.1.2	Viewing Field Replaceable Unit (FRU) Information.....	43
7.1.3	Viewing System Diagnostics.....	43
7.2	Server Health.....	45
7.2.1	Viewing Sensor Readings.....	45
7.2.2	Viewing Event Log.....	47
7.3	Configuring Settings.....	48
7.3.1	Configuring Network Settings.....	48
7.3.2	Managing Users.....	50
7.3.3	Login Security Settings.....	51
7.3.4	Configuring LDAP Settings.....	53
7.3.5	Configuring SSL Upload.....	54
7.4	Configuring Remote Session.....	55
7.4.1	Configuring Mouse Mode Setting.....	56
7.4.2	Configuring Keyboard Macros.....	57
7.5	Remote Control.....	58
7.5.1	Console Redirection.....	59
7.5.2	Server Power Control.....	60
8.	SMASH-Lite* Interface (System Management Architecture for Server Hardware* by AMI*).....	61
8.1	Logging into the SMASH* Session.....	61
8.2	SMASH* Targets.....	61
8.2.1	Supported Properties.....	61
8.2.2	Supported Verbs.....	62
8.3	System1.....	63
8.3.1	Supported Properties.....	63
8.3.2	Supported Verbs.....	64
8.4	Settings1.....	66
8.4.1	Supported Properties.....	66
8.4.2	Supported Verbs.....	67
8.5	SP1.....	68

8.5.1	Supported Properties	68
8.5.2	Supported Verbs	68
8.6	SOL1.....	69
8.6.1	Supported Properties	69
8.6.2	Supported Verbs	70
8.6.3	Terminating an SOL Session.....	71
8.7	Enetport1	71
8.7.1	Supported Properties	71
8.7.2	Supported Verbs	71
8.8	Lanendpt1	72
8.8.1	Supported Properties	72
8.8.2	Supported Verbs	73
8.9	Ipendpt1.....	73
8.9.1	Supported Properties	74
8.9.2	Supported Verbs	74
8.10	Remotesap1.....	75
8.10.1	Supported Properties	75
8.10.2	Supported Verbs	76
8.11	Dnsendpt1.....	76
8.11.1	Supported Properties	77
8.11.2	Supported Verbs	77
8.12	Remotesap1.....	78
8.12.1	Supported Properties	78
8.12.2	Supported Verbs	79
8.13	Remotesap2.....	80
8.13.1	Supported Properties	80
8.13.2	Supported Verbs	80
8.14	Account.....	81
8.14.1	Supported Properties	81
8.14.2	Supported Verbs	82
8.15	Logs1	83
8.15.1	Supported Properties	83
8.15.2	Supported Verbs	83
8.16	Record	85
8.16.1	Supported Properties	85
8.16.2	Supported Verbs	85
8.17	Sensor.....	86
8.17.1	Supported Properties	87
8.17.2	Supported Verbs	87
8.18	CreatingTargets	88

List of Figures

Figure 1: Intel® Remote Management Module 3.....	7
Figure 2: Intel® RMM3 Lite	8
Figure 3: Intel® RMM3 Lite-V.....	8
Figure 4: Installing Intel® RMM3 on Intel® Server Boards S5500UR and S5500WB	11
Figure 5: Installing Intel® RMM3 on Intel® Server Boards S5520HC, S5520BC, and S5520SC .	12
Figure 6: Installing Intel® RMM3 Lite to Intel® Server Board S3420GPRX	13
Figure 7: Installing Intel® RMM3 Lite-V to Intel® Server System SR1640TH	14
Figure 8: Server Management.....	16
Figure 9: IDA Configure Server: Communication Options Window	17
Figure 10: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) settings window	18
Figure 11: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Static IP Address window	19
Figure 12: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Set Up Users window	20
Figure 13: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Edit User Information window.....	21
Figure 14: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Apply Configuration window	22
Figure 15: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Applying Configuration progress window.....	23
Figure 16: Internet Explorer displaying encryption key length.....	25
Figure 17: Intel® RMM3 Login Page	26
Figure 18: Intel® RMM3 Home Page	27
Figure 19: Launching the Online Help	29
Figure 20: Logging Out of Intel® RMM3 – Step 1.....	29
Figure 21: Logging Out of Intel® RMM3 – Step 2.....	30
Figure 22: Remote Control Console Redirection window	31
Figure 23: Remote Console	32
Figure 24: Remote Console Main Window	33
Figure 25: Remote Console Control Bar.....	34
Figure 26: Remote Console Video Menu.....	34
Figure 27: Remote Console Keyboard Menu	35
Figure 28: Remote Console Keyboard Language Sub Menu.....	36
Figure 29: Remote Console Keyboard Soft Keyboard Sub Menu	37

Figure 30: RMM3 Soft Keyboard	37
Figure 31: Remote Console Mouse Menu	38
Figure 32: Remote Console Options Menu	39
Figure 33: Remote Console Device Menu	39
Figure 34: Status Line	40
Figure 35: Busy Indicator Bar	41
Figure 36: System Information page	42
Figure 37: System Information FRU Information page.....	43
Figure 38: System Diagnostics page.....	44
Figure 39: Server Health Sensor Readings window (Thresholds not displayed).....	45
Figure 40: Server Health Sensor Readings window (Thresholds displayed).....	46
Figure 41: Server Health Event Log	47
Figure 42: Configuration.....	48
Figure 43: Configuration Network Settings window	49
Figure 44: Configuring User List window	50
Figure 45: Configuring Users Modify User window	51
Figure 46: Configuring Login Security Settings window.....	52
Figure 47: Configuring LDAP Settings window	53
Figure 48: Configuring SSL Upload window	54
Figure 49: Configuring Remote Session window	55
Figure 50: Configuring Mouse Mode Setting window.....	56
Figure 51: Configuring Keyboard Macros window	57
Figure 52: Remote Control Console Redirection window	59
Figure 53: Server Power Control window	60
Figure 54: SMASH* Target.....	62
Figure 55: System Target.....	64
Figure 56: Example of System Target	65
Figure 57: Setting1 Target	67
Figure 58: SP1 Target.....	69
Figure 59: SOL1 Target	70
Figure 60: Enetport1 Target	72
Figure 61: LANENDPT1 Target.....	73
Figure 62: IPENDPT1 Target	75
Figure 63: REMOTESAP1 Target	76
Figure 64: DNSENDPT1 Target	78
Figure 65: REMOTESAP1 Target	79

Figure 66: REMOTESAP2 Target81

Figure 67: ACCOUNT1 Target.....83

Figure 68: LOGS1 Target.....84

Figure 69: RECORD1 Target86

Figure 70: SENSOR2 Target.....88

List of Tables

Table 1: Terminology	1
Table 2: Intel® RMM3 home page tabs.....	27
Table 3: Horizontal Toolbar Buttons.....	28
Table 4: System Information Details.....	42
Table 5: Server Health (Sensor Readings) Options.....	46
Table 6: Server Health (Event Log) Options.....	47
Table 7: Configuration (Network Settings) Options.....	49
Table 8: Configuration (LDAP Settings) Options	53
Table 9: Configuration (Remote Session) Options	55
Table 10: Macro Non-printable Key Names.....	58
Table 11: Remote Control (Power Control) Options	60
Table 12: SMASH* Targets - Supported Properties	61
Table 13: SMASH*Targets - Supported Verbs	62
Table 14: System1 - Supported Properties.....	63
Table 15: System1 - Supported Verbs	64
Table 16: Settings1 - Supported Properties.....	66
Table 17: Settings1 - Supported Verbs	67
Table 18: SP1 - Supported Properties.....	68
Table 19: SP1 - Supported Verbs	68
Table 20: SOL1 - Supported Properties	69
Table 21: SOL1 - Supported Verbs	70
Table 22: Enetport1 - Supported Properties	71
Table 23: Enetport1 - Supported Verbs.....	71
Table 24: Lanendpt1 - Supported Properties.....	72
Table 25: Lanendpt1 - Supported Verbs	73
Table 26: Ipendpt1 - Supported Properties.....	74
Table 27: Lanendpt1 - Supported Verbs	74
Table 28: Remotesap1 - Supported Properties	75
Table 29: Remotesap1 - Supported Verbs	76
Table 30: Dnsendpt1 - Supported Properties	77
Table 31: Dnsendpt1 - Supported Verbs	77
Table 32: Remotesap1 - Supported Properties	78
Table 33: Remotesap1 - Supported Verbs	79

Table 34: Remotesap2 - Supported Properties80

Table 35: Remotesap2 - Supported Verbs80

Table 36: Account - Supported Properties.....81

Table 37: Account - Supported Verbs82

Table 38: Logs1 - Supported Properties.....83

Table 39: Logs1 - Supported Verbs.....83

Table 40: Record - Supported Properties85

Table 41: Record - Supported Verbs.....85

Table 42: Sensor - Supported Properties87

Table 43: Sensor - Supported Verbs87

1. Introduction

The Intel® RMM3 works as an integrated solution on your server system. Based on an embedded operating system, the Intel® RMM3 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® RMM3 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 from a built-in Web Console from anywhere, anytime.

This User Guide describes how to use the Intel® Remote Management Module 3 (hereinafter referred to as Intel® RMM3). It provides an overview of the features of the module and instructions on how to set up and operate the Intel® RMM3.

1.1 Target Audience

This document is intended for system technicians who are responsible for installing, troubleshooting, upgrading, and repairing the Intel® RMM3. As a system administrator, you can use it to work on the Intel® RMM3 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
CLI	Command Line Interface
DDC	Display Data Channel
DHCP	Dynamic Host Configuration Protocol
DVC	Dambrackas* Video Compression
DVO	Dynamic Visual Output
EDID	Extended Display Identification Data
FML	Fast Management Link
FPGA	Field Programmable Gate Array
ICMP	Internet Control Message Protocol
Intel® ASMI	Intel® Advanced Server Management Interface
Intel® RMM3	Intel® Remote Management Module 3
IPMI	Intelligent Platform Management Interface
ITE	Information Technology Equipment
KVM	Keyboard, Video and Mouse
MAC	Media Access Controller
MII	Media Independent Interface

Word/Acronym	Definition
OOB	Out Of Band- No operating system interaction on Server
PBDE	Polybrominated Biphenyls Diphenyl Ethers
RMI	Reduced Media Independent Interface
RTC	Real-Time Clock
TCP/IP	Transmission Control Protocol/Internet Protocol
TPS	Technical Product Specification
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol

1.3 Safety Information

▲ **WARNING**

Before working with your Intel® RMM3 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.

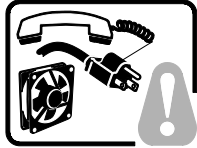
▲ **Warnings**

- ▲ **System power on/off:** The server power button DOES NOT turn off the system power or Intel® RMM3 power. To remove power from the Intel® RMM3 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® RMM3.
- ▲ **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.

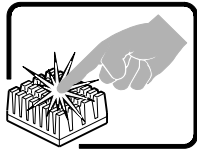
Safety Cautions

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:

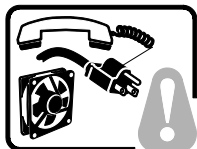
1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide some electrostatic 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.

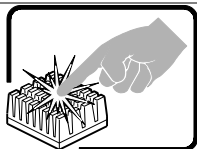
Wichtige Sicherheitshinweise

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 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.



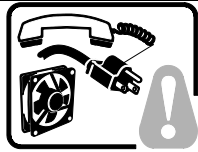
Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

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》）。

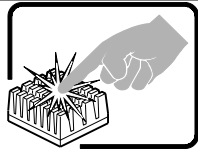
Consignes de sécurité

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:

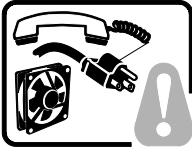
1. Mettez hors tension tous les périphériques connectés au système.
2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).
3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.
4. Identifiez et débranchez tous les câbles reliés 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.

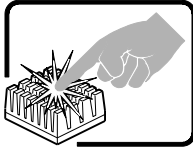
▲ Instrucciones de seguridad importantes

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 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.



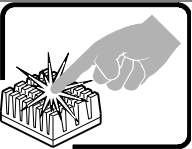
Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

▲ AVVERTENZA: Italiano



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

1. Spegner tutti i dispositivi periferici collegati al sistema.
2. Spegner 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® RMM3, 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 3 Overview

This section gives you an overview of the Intel® RMM3 and highlights significant benefits of its features.

The Intel® RMM3 is a 1.23-inch x 2.30-inch printed circuit board. When installed onto the Intel® RMM3 connector 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.

2.1 Intel® RMM3 Features

The Intel® RMM3 add-on card offers convenient, remote KVM access and control from 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 provided by the Intel® RMM3 hardware.

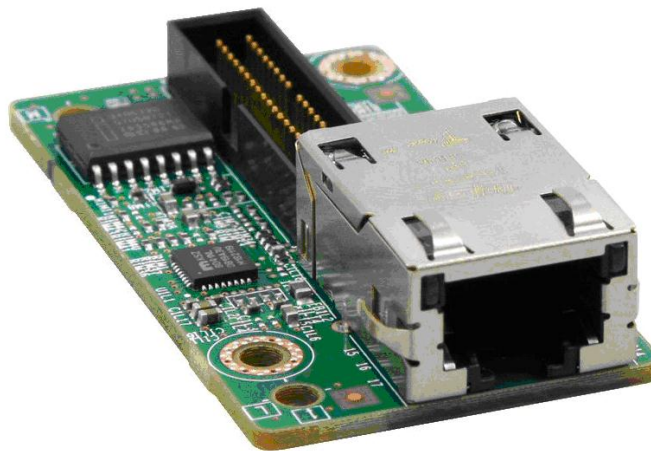


Figure 1: Intel® Remote Management Module 3

In addition, the Intel® RMM3 add-on card offers integrated remote power management using IPMI. Key features of the Intel® RMM3 add-on card are:

- Embedded Web Console UI supports Remote Power on/off, system health, system info, Event log.
- KVM redirection from either the RMM3 NIC or the baseboard NIC used for management traffic; high performance, up to two simultaneous KVM sessions.
- USB 2.0 media redirection - boot over remote media
- Security – open SSL, open LDAP
- OEM Customization of the Web Console.

- IPMI V2.0 Compliance
- 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.

2.1.1 RMM3 Lite and RMM3 Lite-V

RMM3 has two variations – RMM3 Lite and RMM3 Lite-V, which have the same functionality as RMM3. RMM3 Lite can be used only on Intel® Server Board S3420GPRX; it has no RMM3-dedicated NIC. The management traffic can only go through the onboard Integrated BMC-shared NIC (NIC5 on Intel® Server Board S3420GPRX) and share network bandwidth with the host system. RMM3 Lite-V module can be used only on Intel® Server System SR1640TH, with its RMM3-dedicated NIC separated and integrated on the server board.



Figure 2: Intel® RMM3 Lite



Figure 3: Intel® RMM3 Lite-V

2.2 Supported Operating Systems

The Intel® RMM3 runs independent of the host operating system on the server where it is installed except during Remote Console connections. During Remote Console connections the Keyboard, Video, and Mouse (KVM) of the console system operate just as if you were at the server where the Intel® RMM3 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.

2.2.1 Server System

The following operating systems are supported on the managed server:

- Microsoft Windows 2003 Server* with SP1
- Microsoft Windows 2003 Server* 32-bit
- Microsoft Windows 2003 Server* with SP2
- Microsoft Windows 2008 Server*
- Red Hat* Enterprise Linux 5
- SUSE* 10 SP1
- Red Hat* Enterprise Linux 5 U3
- Red Hat* Enterprise Linux 5 U4
- Microsoft Windows XP* with SP 2

2.2.2 Client System

The following client operating system and internet browser combinations have been tested:

- SUSE* 10.2/Firefox* 3.0.1
- Red Hat* Enterprise Linux 5.1/Firefox* 3.0.1
- Microsoft Windows XP Pro* with SP3/Firefox* 3.0.1
- Microsoft Windows XP Pro* with SP3/IE* 7.0
- Microsoft Windows XP Pro* with SP3 64-bit/IE* 7.0
- Microsoft Windows Vista* 32-bit/IE* 7.0
- Microsoft Windows XP Pro* with SP2/IE* 6.0
- Microsoft Windows XP Pro* with SP2/Firefox* 2.0.0.14

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 3 is currently supported on the following Intel® server boards:

- All SKUs of Intel® Server Board S5500BC
- All SKUs of Intel® Server Board S5520HC and S5520SC
- All SKUs of Intel® Server Board SC5520UR
- The Intel® RMM3 Lite is currently supported on all SKU of the Intel® Server Board S3420GPRX
- The Intel® RMM3 Lite-V is currently supported on Intel® Server System SR1640TH
- All SKUs of the Intel® Server Board S5500WB
- Intel® Storage System SR2612UR

The Intel® RMM3 box contains the following components:

- Intel® Remote Management Module
- Network Interface Card (NIC) module
- Plastic bag containing screws, slot bracket, three plastic standoffs, and cabling

The installation will vary between these server boards and their chassis configurations. The following sections detail installation instructions.

⚠ Caution: Intel® RMM3, RMM3 Lite, and RMM3 Lite-V 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, 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 on Intel® Server Boards S5500UR and S5500WB

The Intel® Server Board S5500UR and S5500WB install in rack mount 1U or 2U chassis. The same installation steps apply to both chassis types.

1. Attach the Intel® RMM3 to the metal fastening bracket.
2. Attach the cable from the baseboard to the RMM3 module.
3. Push out and remove the metal cover on the chassis where the NIC RJ-45 receptacle will align.
4. Mount the RMM3 module to the header on the baseboard and secure the metal fastening bracket to the back of the chassis as shown in Figure 2. This will align the RJ-45 with the opening in the chassis.
5. Make a note of the MAC address of the Intel® RMM3. It is written on a label attached to the module (not the NIC). Keeping a record now may eliminate the need to reopen the cover later.
6. Replace the chassis cover, attach AC power, and connect a network cable to the Intel® RMM NIC.

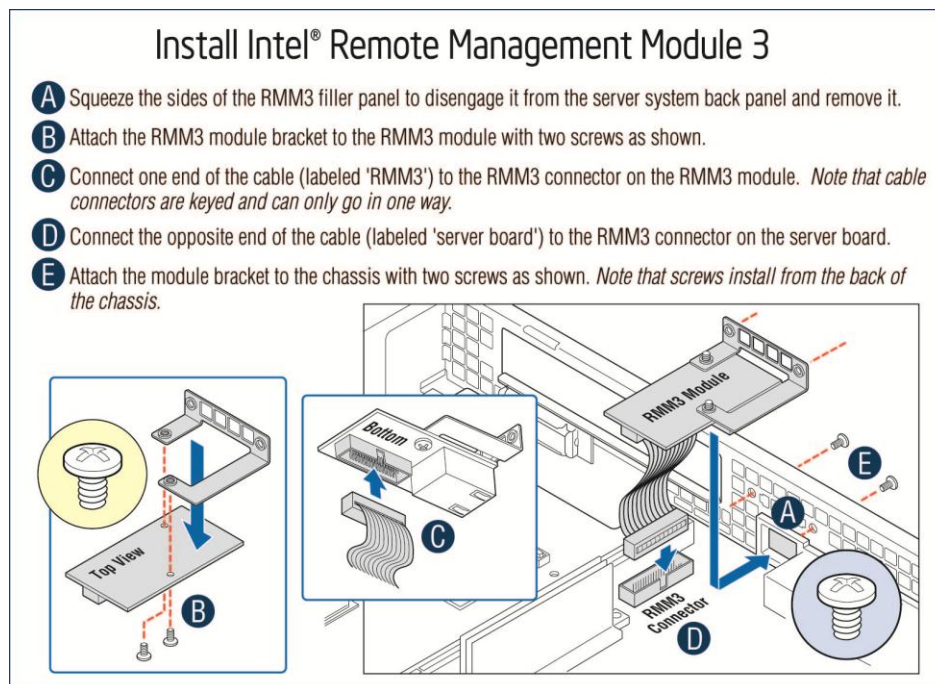


Figure 4: Installing Intel® RMM3 on Intel® Server Boards S5500UR and S5500WB

3.3.2 Installation on Intel® Server Boards S5520HC, S5520BC, and S5520SC

The Intel® Server Boards S5520HC, S5520BC, and S5520SC install in pedestal style chassis.

1. Attach the Intel® RMM3 to the connector on the server baseboard labeled “RMM”.
2. Mount the bracket with the RMM3 module in a chassis slot near the baseboard connector for the cable.
3. Attach the cable from the baseboard to the RMM3 module as shown.
4. Make a note of the MAC address of the Intel® RMM3. It is written on a label attached to the module (not the NIC). Keeping a record now may eliminate the need to reopen the cover later.
5. Replace the chassis cover, attach AC power, and connect a network cable to the Intel® RMM NIC

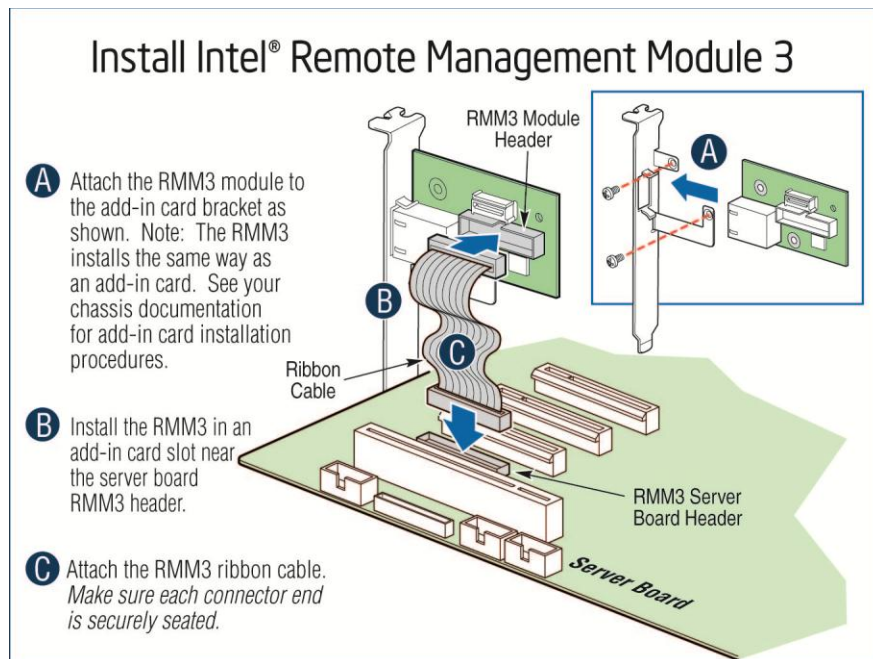


Figure 5: Installing Intel® RMM3 on Intel® Server Boards S5520HC, S5520BC, and S5520SC

3.3.3 Installation on Intel® Server Board S3420GPRX

Intel® Server Board S3420GPRX supports only Intel® RMM3 Lite. Position the RMM3 Lite over the server board RMM3 Lite connector (J2D1) as shown in Figure 6. Intel® RMM3 Lite has no dedicated NIC. The user can access only its Virtual Presence features (Web GUI, Virtual Media, and so on) from the Integrated BMC-shared NIC (NIC5 on Intel® S3420GPRX).

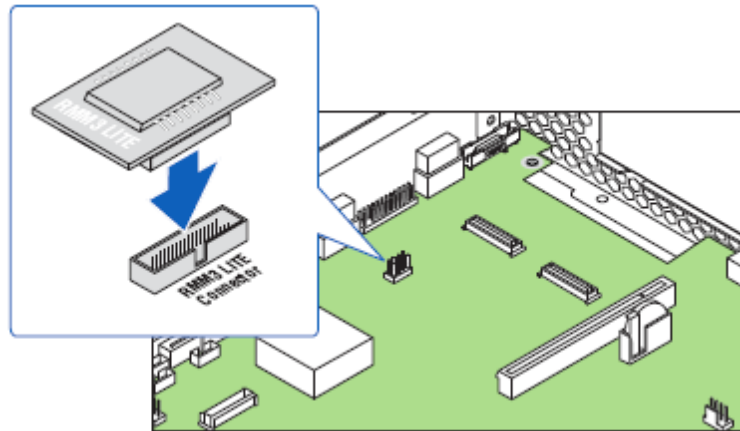


Figure 6: Installing Intel® RMM3 Lite to Intel® Server Board S3420GPRX

3.3.4 Installation on Intel® Server System SR1640TH

Intel® Server System SR1640TH supports only Intel® RMM3 Lite-V. Plug in RMM3 Lite-V module to the server board RMM3 Lite-V connector (J1G1 or J7E1) as shown in Figure 7.

Intel® RMM3 Lite-V dedicated NIC is separated and integrated on Intel® Server System SR1640TH server board. All Virtual Presence features (Web GUI, Virtual Media, and so on) are supported on Integrated BMC-shared NIC and RMM3 Lite-V dedicated NIC. IPMI traffic to those two network paths is supported only if the Integrated BMC-shared NIC and the Intel® RMM3 Lite-V dedicated NIC are on separate subnets.

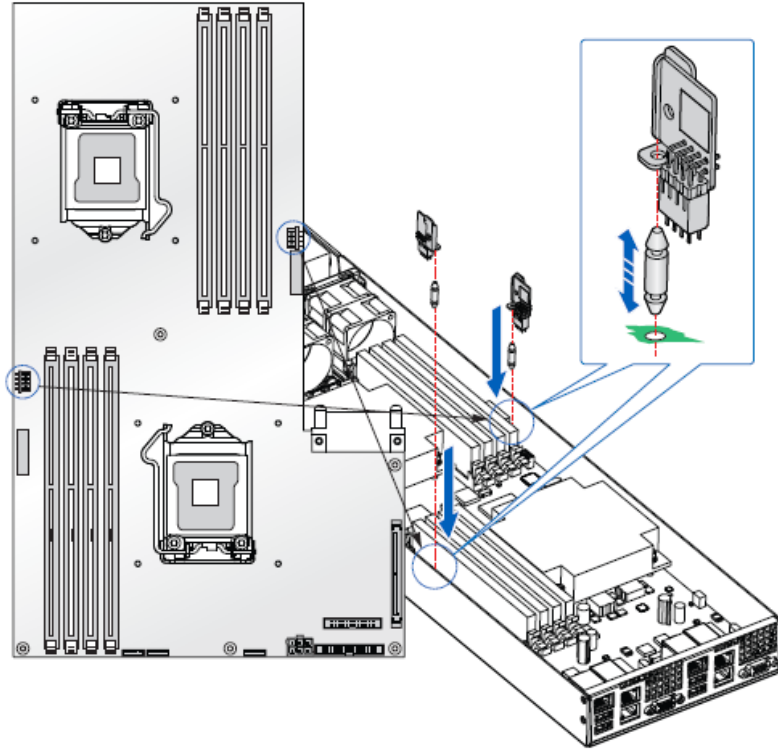


Figure 7: Installing Intel® RMM3 Lite-V to Intel® Server System SR1640TH

4. Configuring Intel® RMM3

This section discusses using the Server Utilities to enable an Intel® RMM3, includes RMM3 Lite and RMM3 Lite-V, from a new unconfigured state to an operational one.

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
- SYSCFG - <http://downloadcenter.intel.com/default.aspx> > relevant server platforms page
- Through BIOS Setup

When first powered on, by default, the Intel® RMM3 uses a static IP address of 0.0.0.0.

The Intel® RMM3 can be configured in many ways: using the Intel® Deployment Assistant (IDA), Sysconfig, and IPMI commands.

The following two steps are necessary before Intel® RMM3 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® RMM3 through BIOS setup

1. During POST, press **F2** to go to BIOS setup.
2. Navigate to the menu **Server Management** and scroll down to Baseboard LAN configuration.
3. Go to the Intel® RMM3 sub-menu and configure the IP source, IP address, Subnet mask, and Gateway IP.

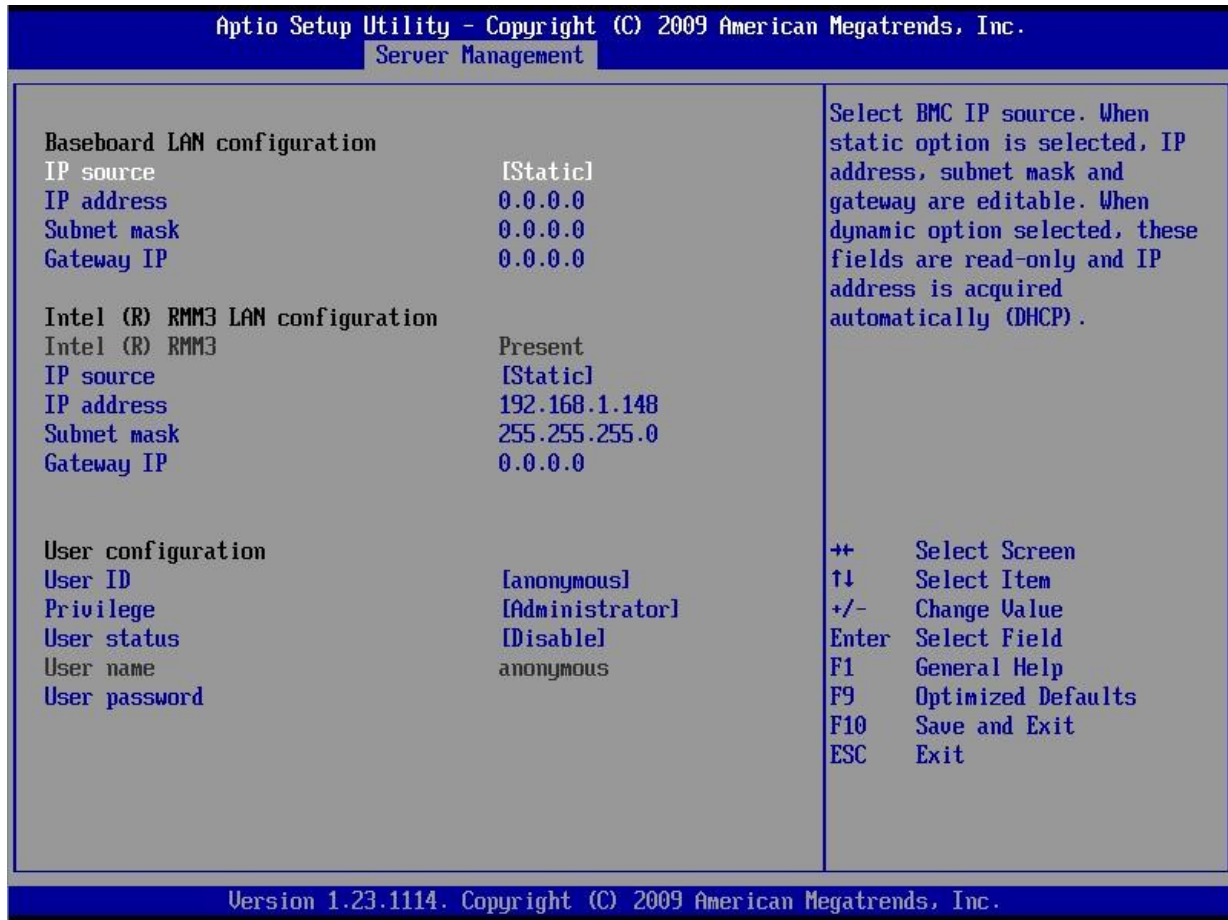


Figure 8: Server Management

4.2 Configuring your Intel® RMM3 using the Intel® Deployment Assistant (IDA)

The following section explains the RMM3 configuration using the IDA.

⚠ WARNING

If you need to configure both channel 1 and RMM3, ensure that they are connected to different subnets.

Note: When using IDA to setup Intel® RMM3 Lite on Intel® S3420GPRX user can only configure BMC channel1. Since Intel® RMM3 Lite has no dedicated NIC, the BMC channel 3 configuration with IDA is disabled. The user can access Intel® RMM3 Lite advance features from onboard NIC 5 (BMC channel 1).

1. After selecting Server Management settings, you should get a window as shown in Figure 9. Select which channel you would like to configure.

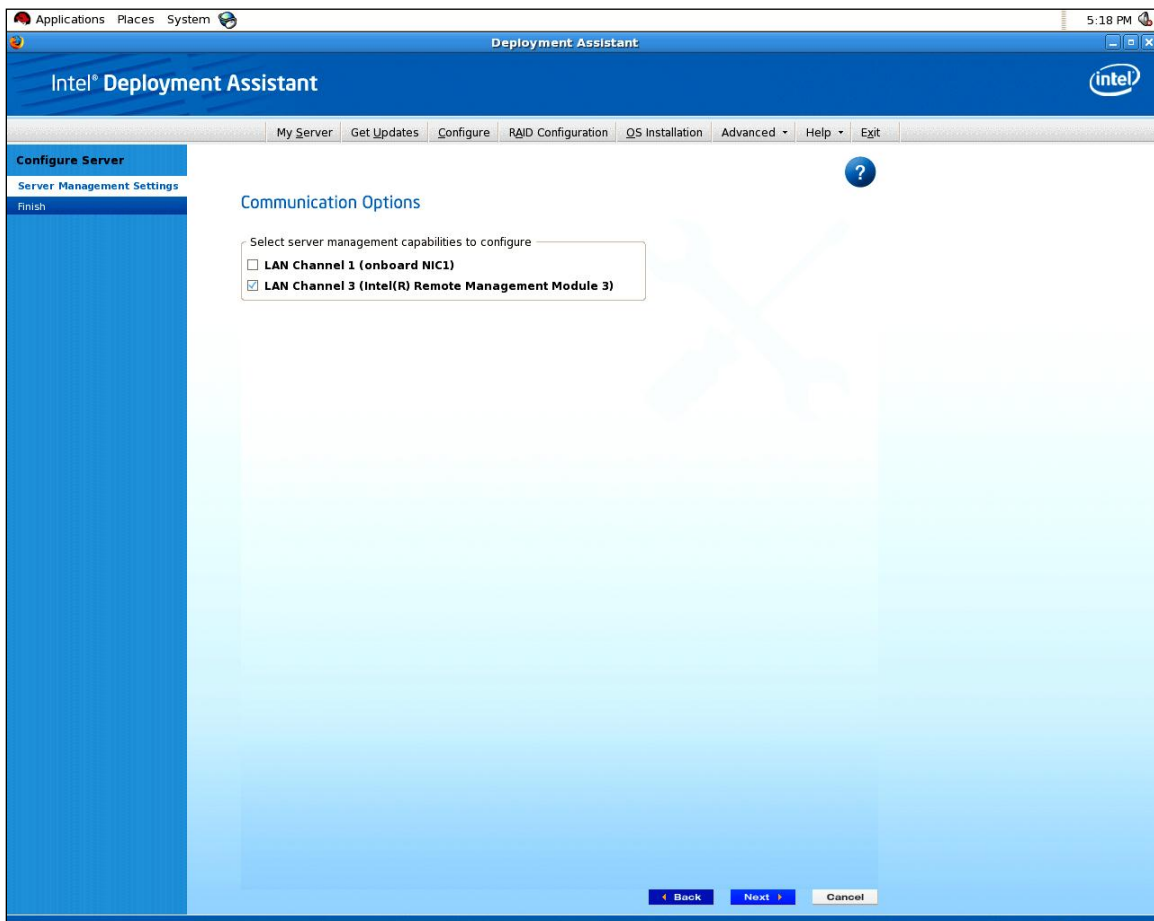


Figure 9: IDA Configure Server: Communication Options Window

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 11.
- b. If **Static IP Address** is selected, configure the **IP address**, **Subnet Mask**, and **Gateway** as shown in Figure 10.

3. You can also select **Enable Serial Over LAN** on these screens.

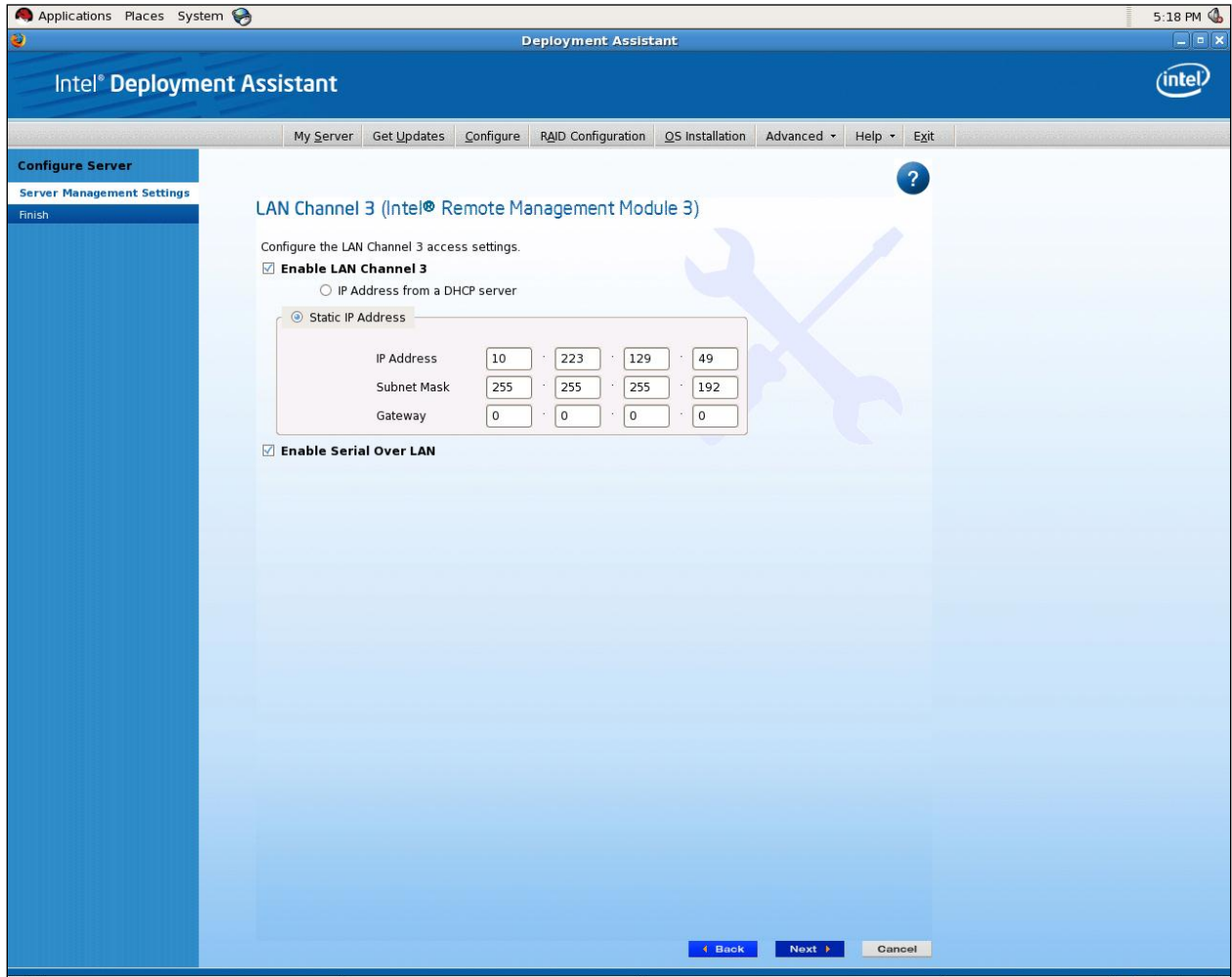


Figure 10: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) settings window

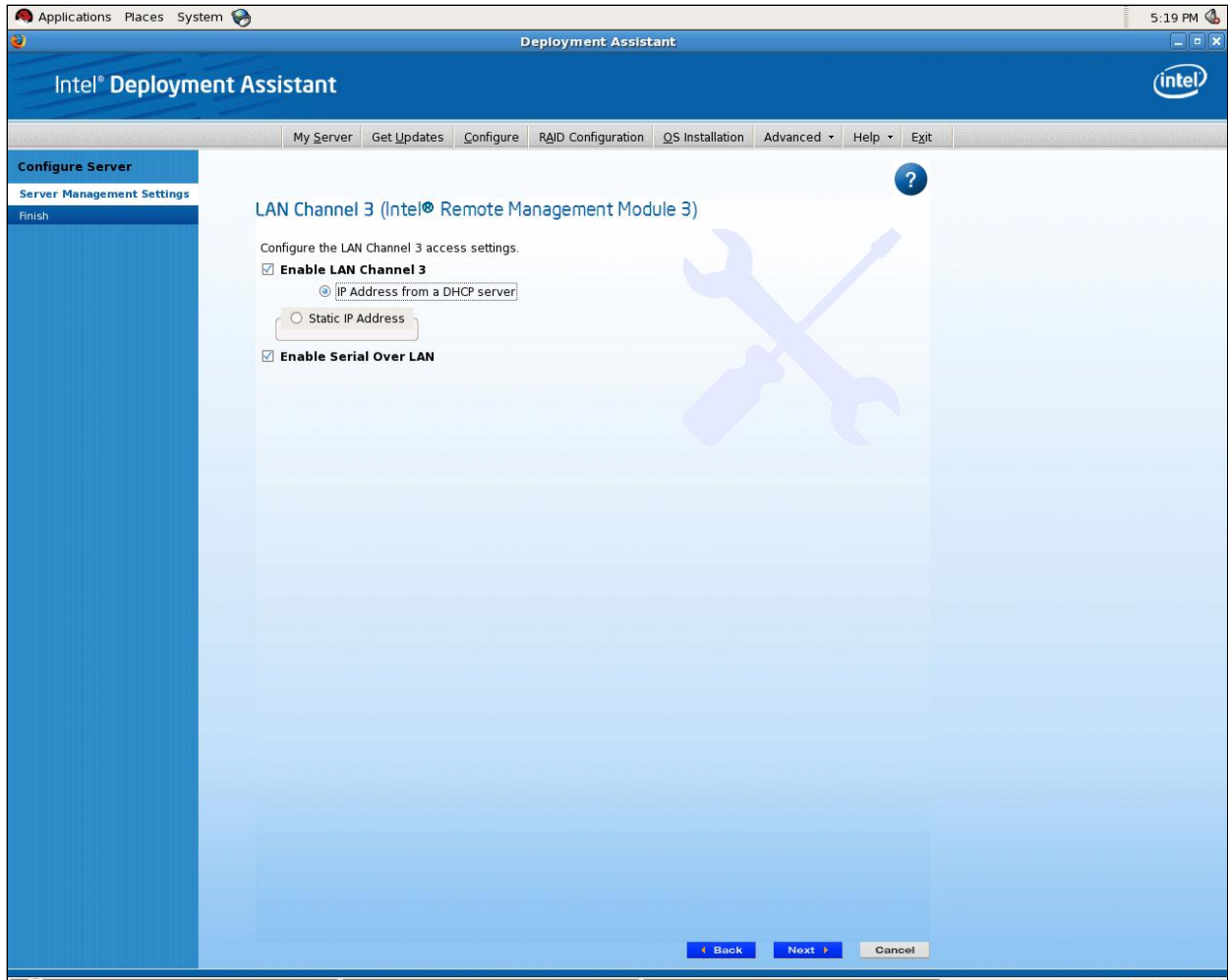


Figure 11: IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Static IP Address window

4. [Optional] You have the option to edit user information data. Click **Edit**.
The Edit User Data window opens.

Note:

- You cannot login to the Intel® RMM3 as an anonymous user. You must modify existing users. “root” user is the default.
- To connect remotely to LAN Channel 3, you will need to configure users. Edit username/passwords, and set privilege for the users as shown below.

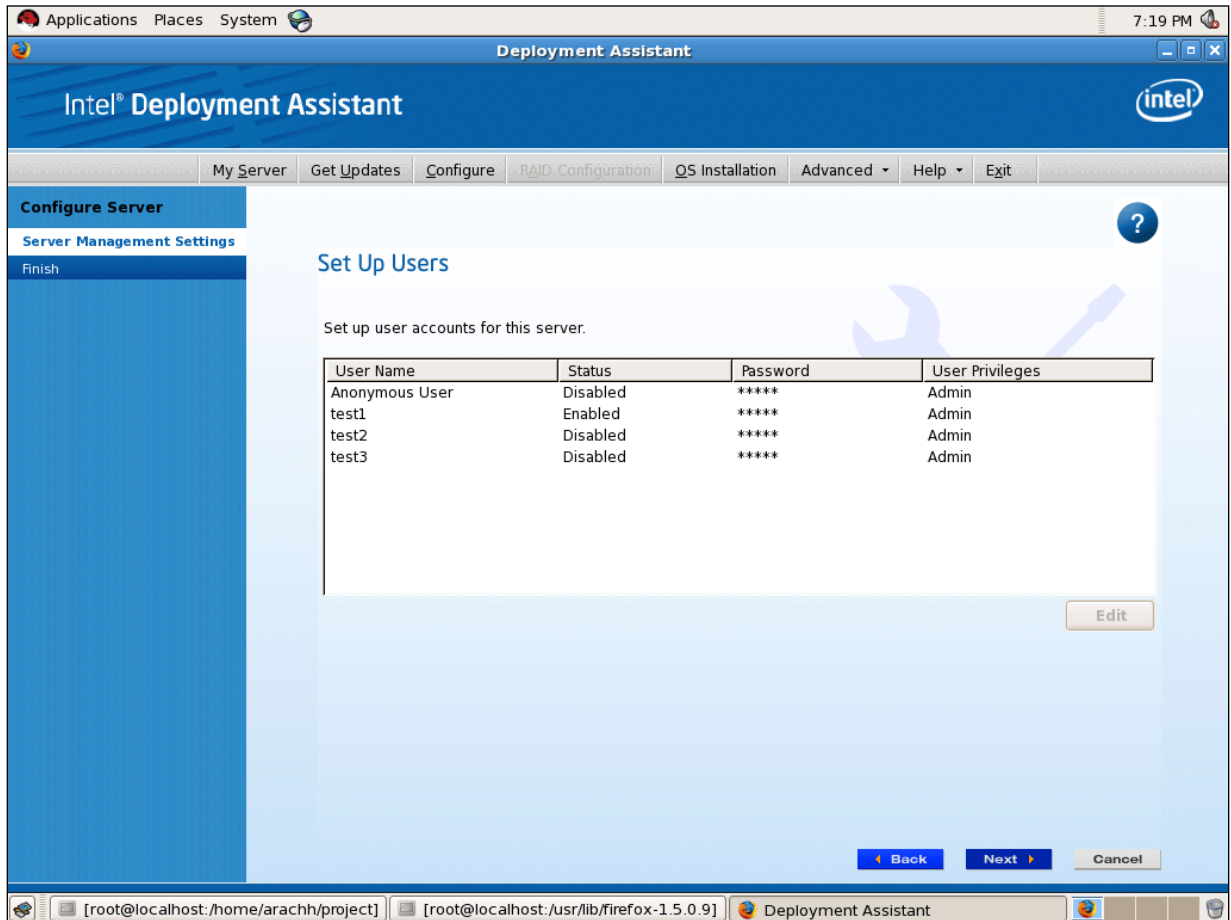
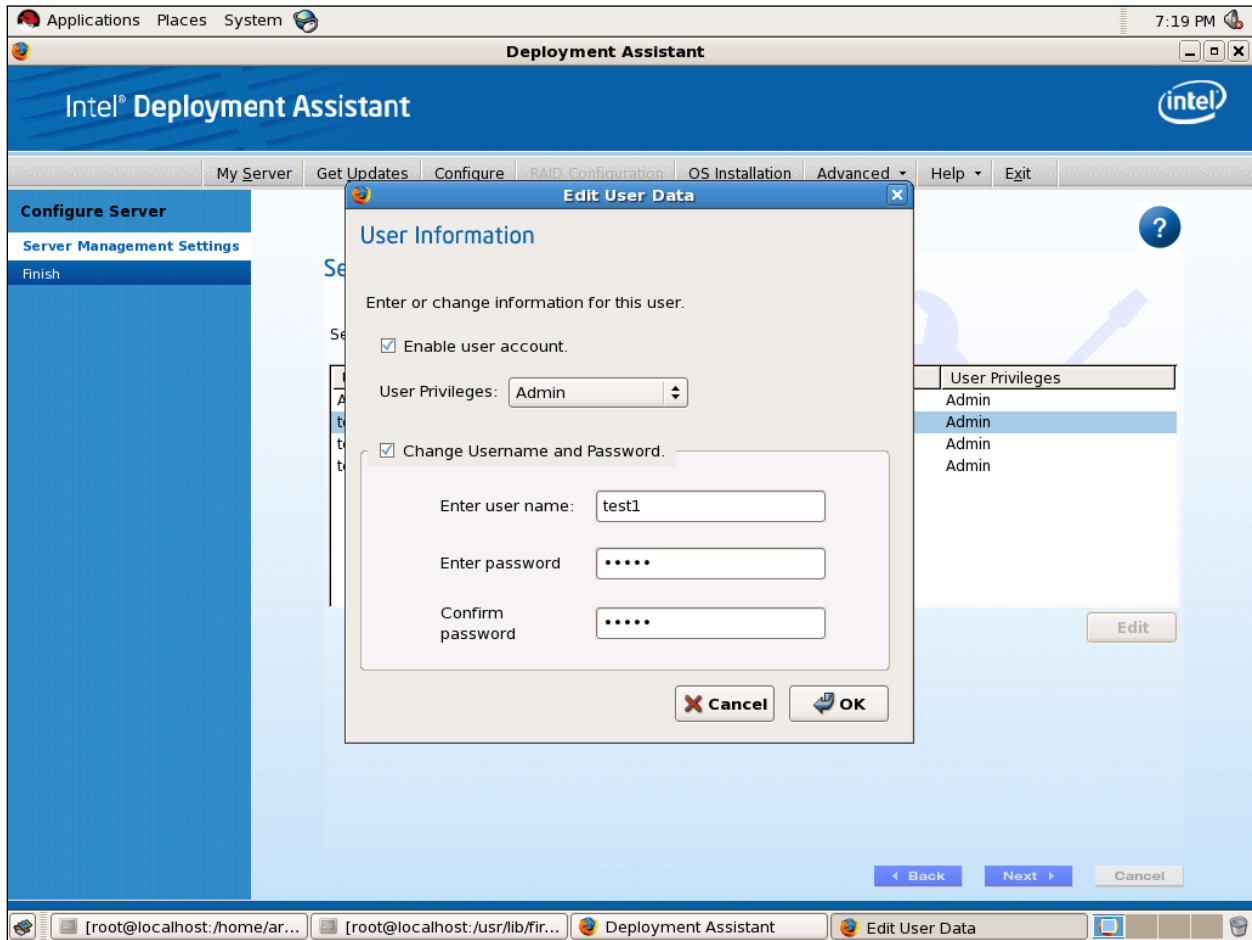


Figure 12: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Set Up Users window

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



**Figure 13: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3)
Edit User Information window**

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

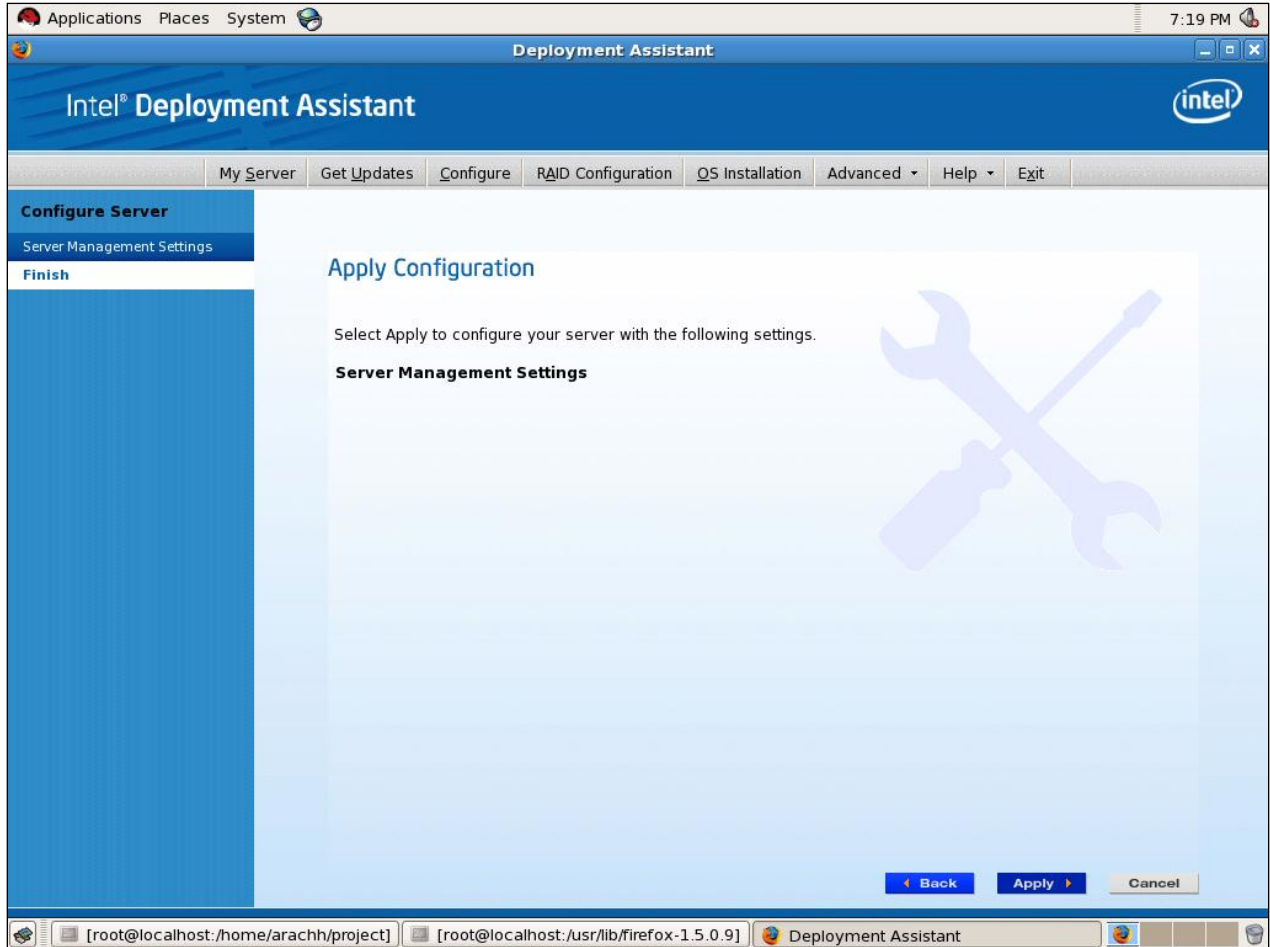
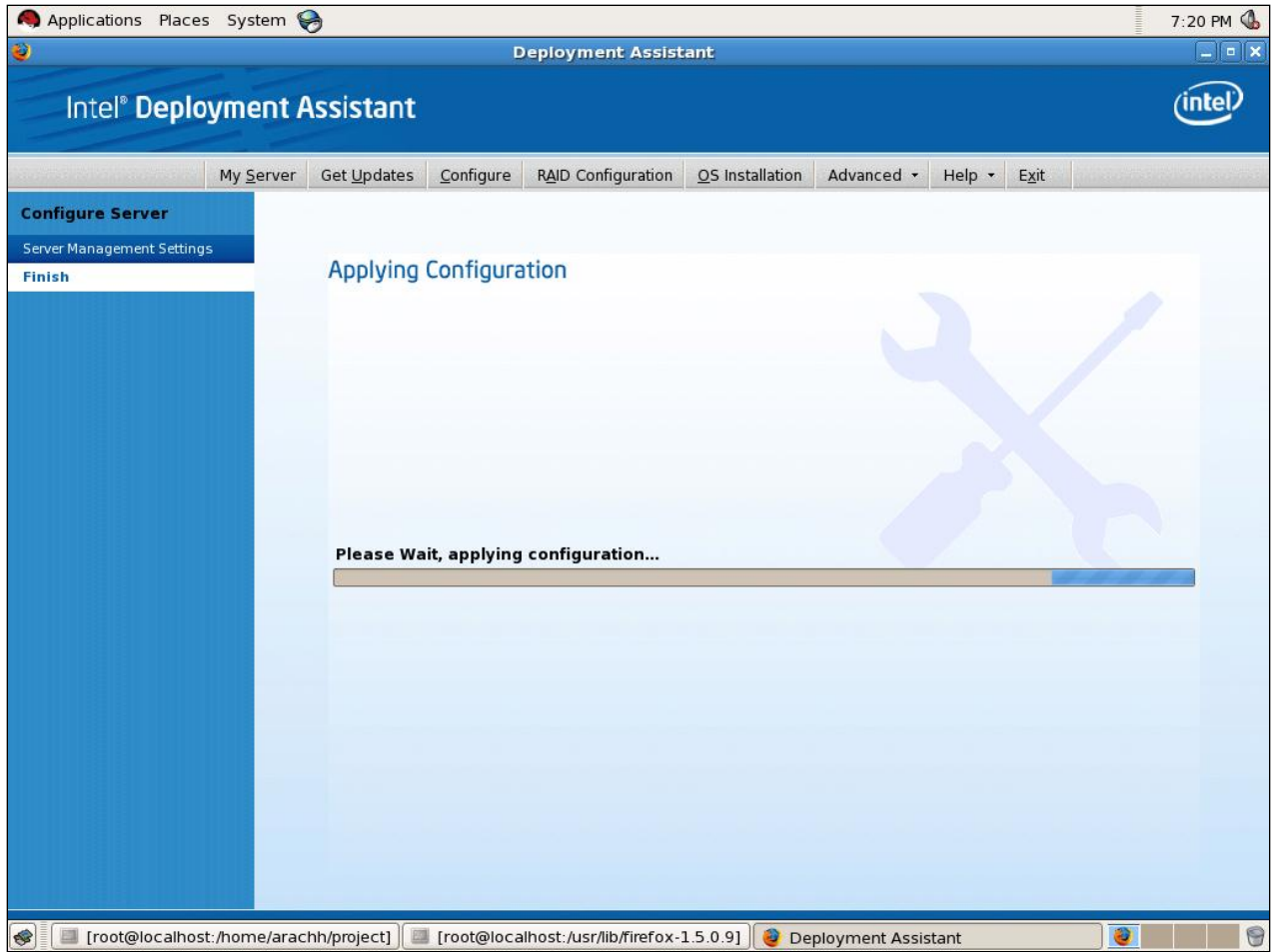


Figure 14: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3) Apply Configuration window



**Figure 15: IDA Configure Server: Configure LAN Channel 2 (Intel® RMM3)
Applying Configuration progress window**

4.3 Configuring your Server using Intel® System Configuration Utility (SysConfig)

This section explains how to configure using Sysconfig commands.

4.3.1 Running the Sysconfig

To run Sysconfig, enter the Sysconfig directory using this command:

```
cd /usr/local/syscfg
```

4.3.2 Configuring IP address

- To set static IP address:
`syscfg -le 3 static <STATIC_IP> <SUBNET_MASK> -lc 3 12 <DEFAULT_GATEWAY_IP>`
- To set dhcp IP address:
`syscfg -le 1 dhcp`
- Additionally, to enable SOL (can be used for either static or DHCP)
To enable Serial Over LAN (SOL):
`syscfg -sole 3 Enable Admin BAUD_RATE RETRY_COUNT RETRY_INTERVAL_IN_MILLISECONDS`

4.3.3 Configuring Users

- To enable a user for RMM3 channel:
`syscfg -up 3 3 Admin sol -ue 3 Enable 3`

5. Getting Started with Intel® RMM3 Operation

The Intel® RMM3 module, including Intel® RMM3 Lite and RMM3 Lite-V, features an embedded web server and applications offering a variety of standardized interfaces. 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 will use user “root”, but other usernames and passwords could be used.

The Intel® RMM3 add-on card may be accessed using a standard Java* enabled web browser. You may use the HTTP protocol or a secure encrypted connection from HTTPS.

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 6.0* or higher, you can verify strong encryption by opening the “Help/About” menu to read about the key length that is currently activated. Figure 16 shows the dialog box presented by the Internet Explorer 6.0*.



Figure 16: Internet Explorer displaying encryption key length

In order to use the Remote Console (KVM) window of your managed server, Java Runtime Environment* (JRE*) version 1.6 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® RMM3 add-on card into your web browser. In order to use a secure connection, type `https://<IPaddress of RMM3>/`. This will take you to the Intel® RMM3 module login page as shown in Figure 17.

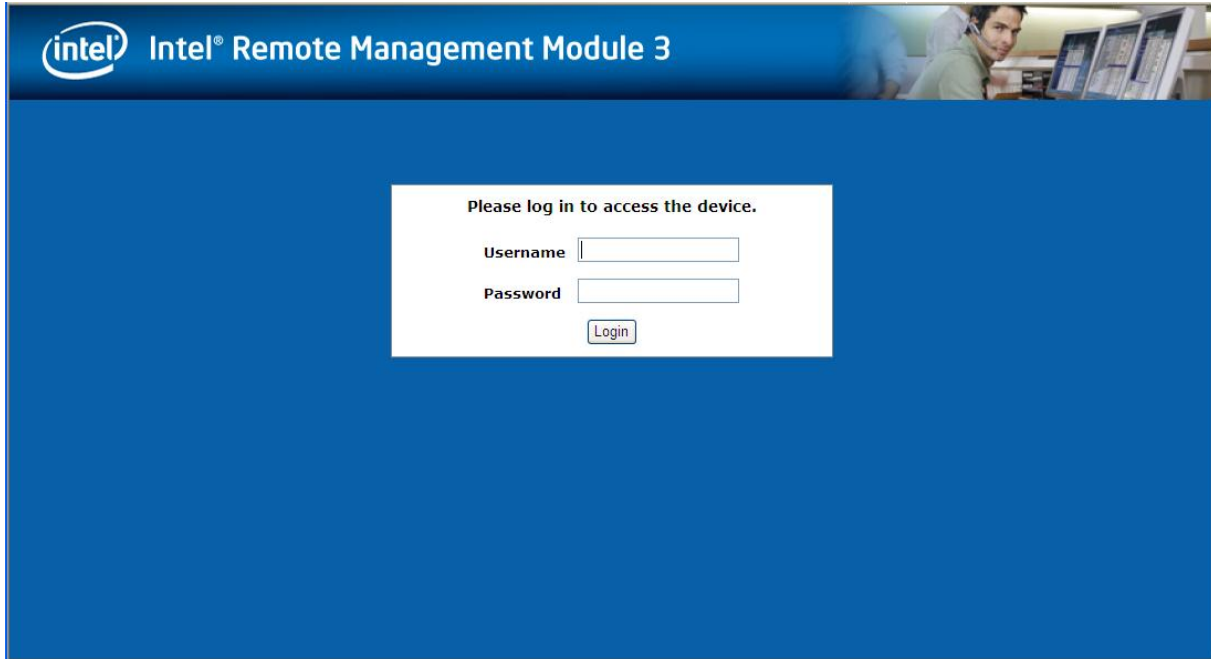


Figure 17: Intel® RMM3 Login Page

Log in by entering the username and password.

For example:

- Username = root
- Password = superuser

Click the **Login** button to view the RMM3 home page as shown in Figure 17.

After the initial log in, System Administrators may change passwords, create new users, and have full control over access to the Intel® RMM3.

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 Intel® RMM3 module, the Intel® RMM3 home page appears as shown in Figure 18:

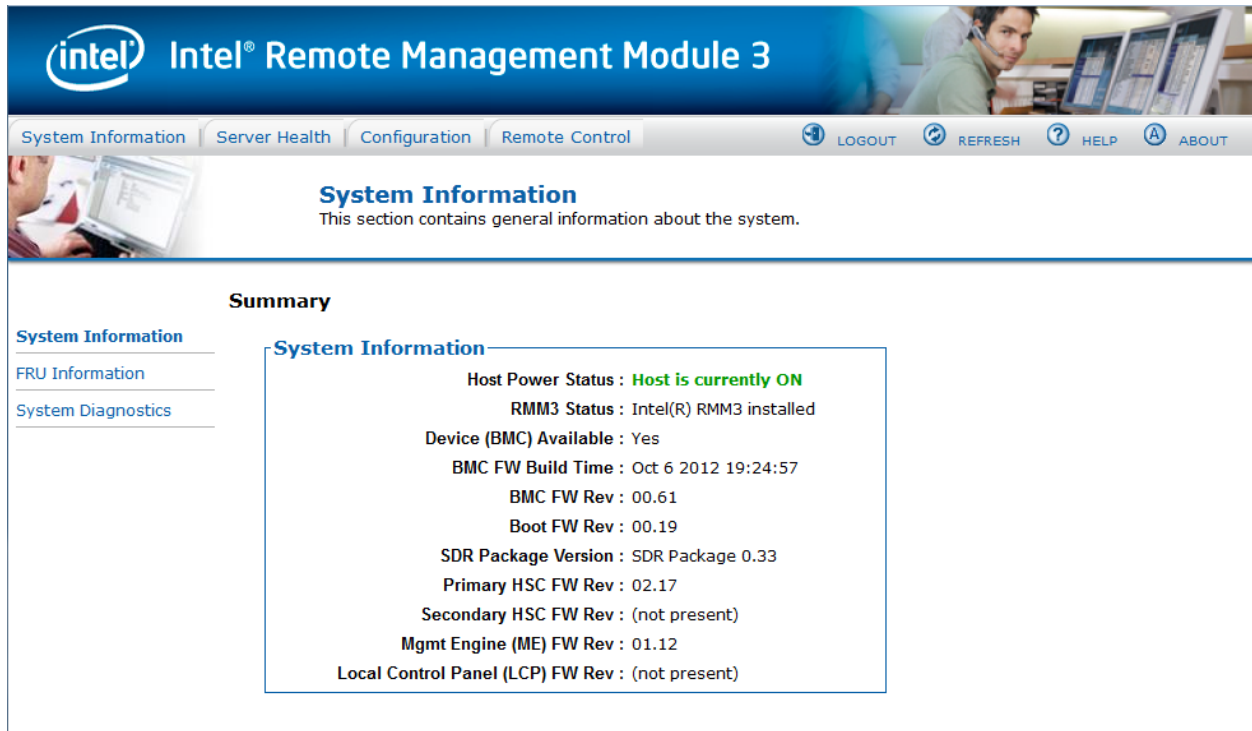

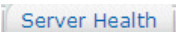




Figure 18: Intel® RMM3 Home Page

The top horizontal toolbar within the Intel® RMM3 home page has four tabs. Click these tabs to get specific system information and perform tasks as shown in the following table:




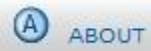
Table 2: Intel® RMM3 home page tabs

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
	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


Tab	Function
	<ul style="list-style-type: none"> • 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 RMM3 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 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. <p>Note: Using the web browsers refresh/reload button or pressing the function key F5 to do a refresh/reload are not supported for reloading the Web Console pages. Using either of them can cause unexpected results.</p>
	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.
	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 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 19. The right **Help** frame is visible only when the online help is being accessed.

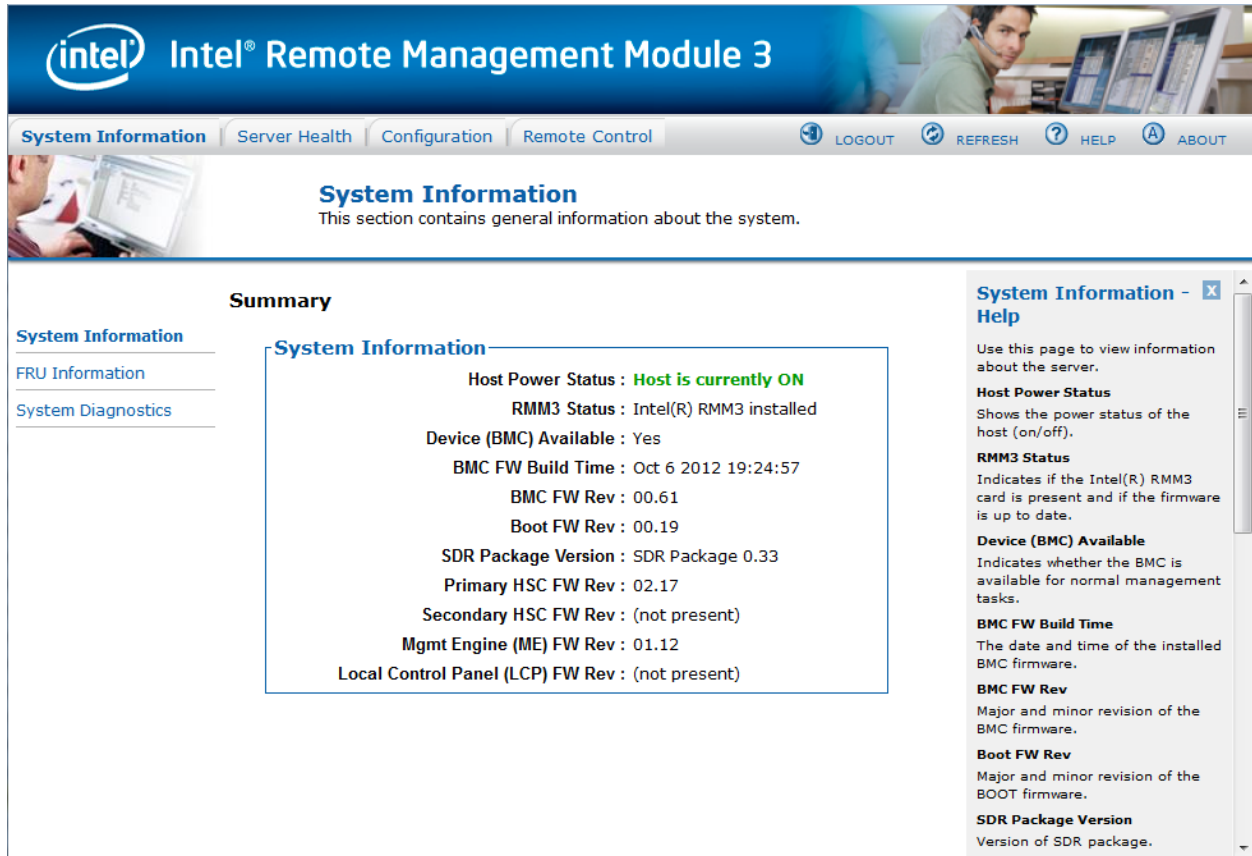



Figure 19: Launching the Online Help

5.5 Logging Out

Click the  button to log out the current user and revert to a new login screen as shown in Figure 20 and Figure 21.

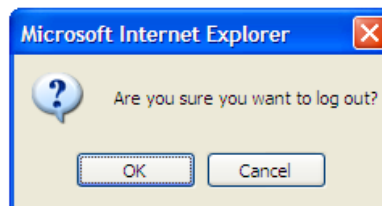


Figure 20: Logging Out of Intel® RMM3 – Step 1

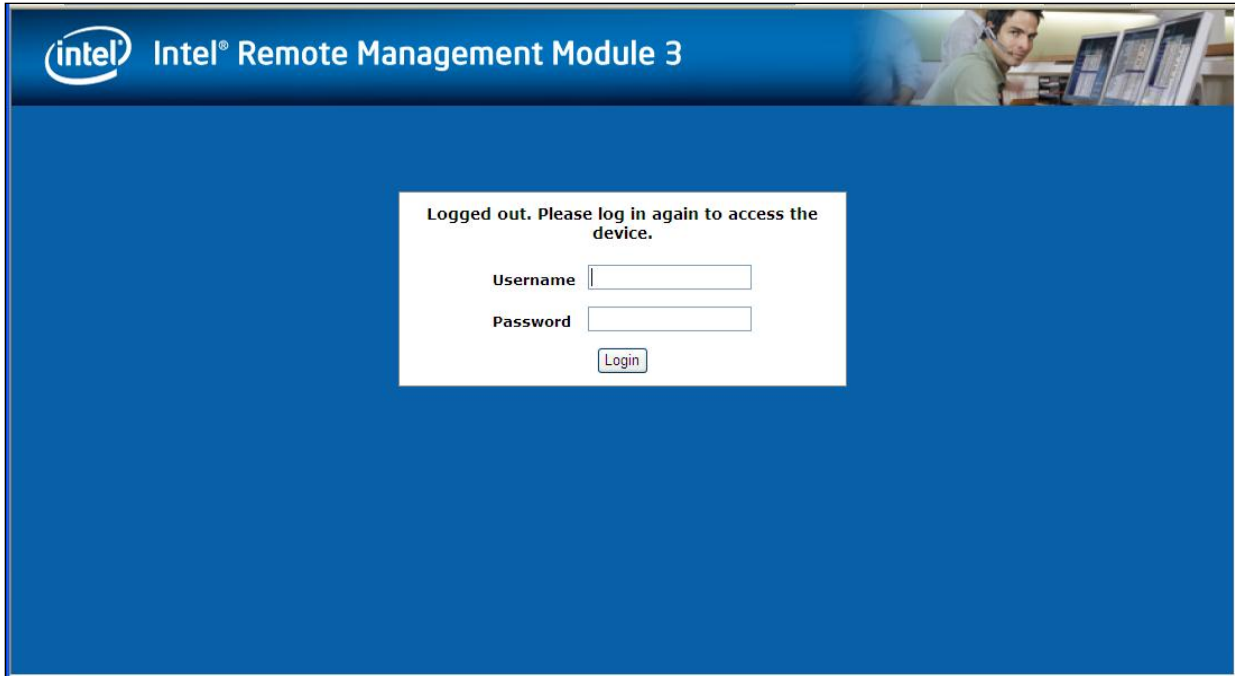


Figure 21: Logging Out of Intel® RMM3 – Step 2

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® RMM3 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® RMM3 module is installed. Launch the remote console KVM redirection window from this page.



Figure 22: Remote Control Console Redirection window

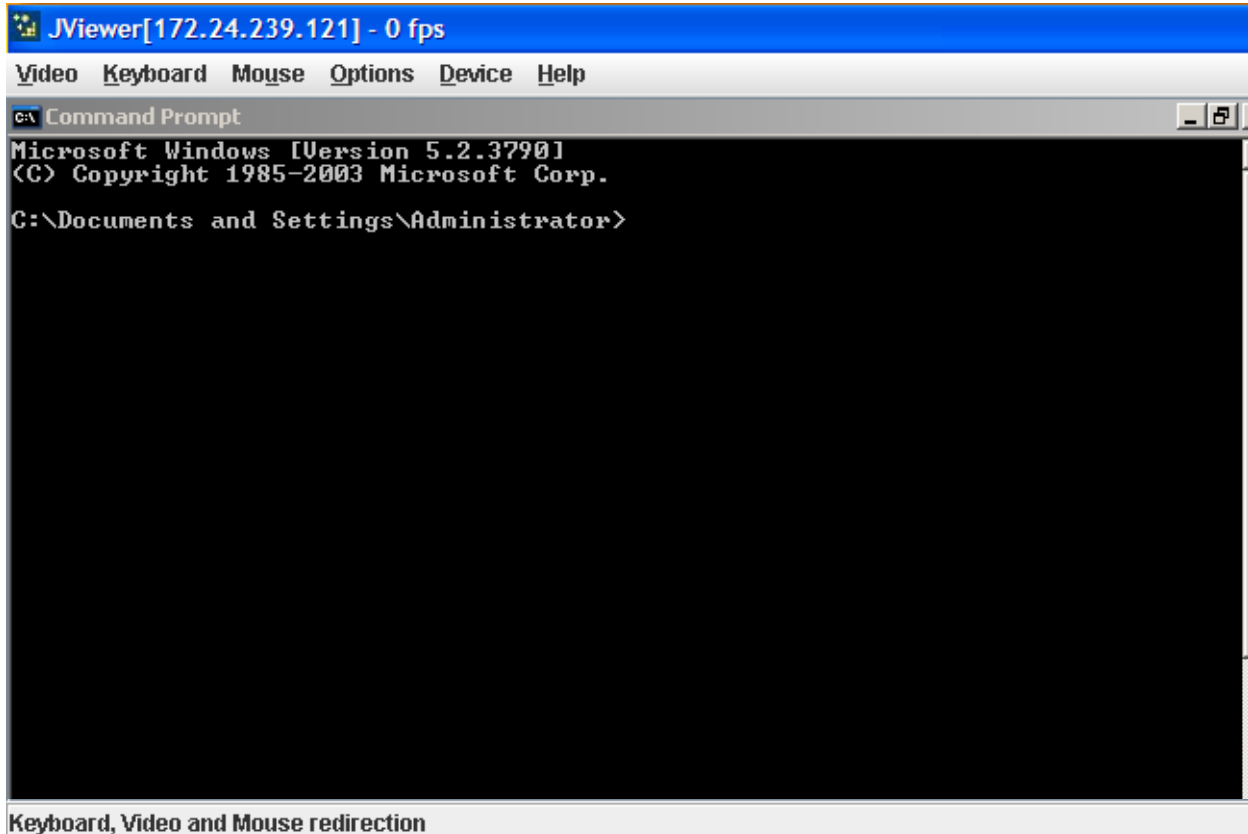
Click the **Launch Console** button to launch the redirection console and manage the server remotely.

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.

Note:

- Java Run-Time Environment* (JRE*, version 6 update 10 or later) must be installed on the client prior to the launch of a JNLP file.
- The client browser must allow pop-up windows from the Intel® RMM3 IP address.

**Figure 23: Remote Console**

The Remote Console window is a Java Applet* that establishes TCP connections to the Intel® RMM3 module. 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 24.

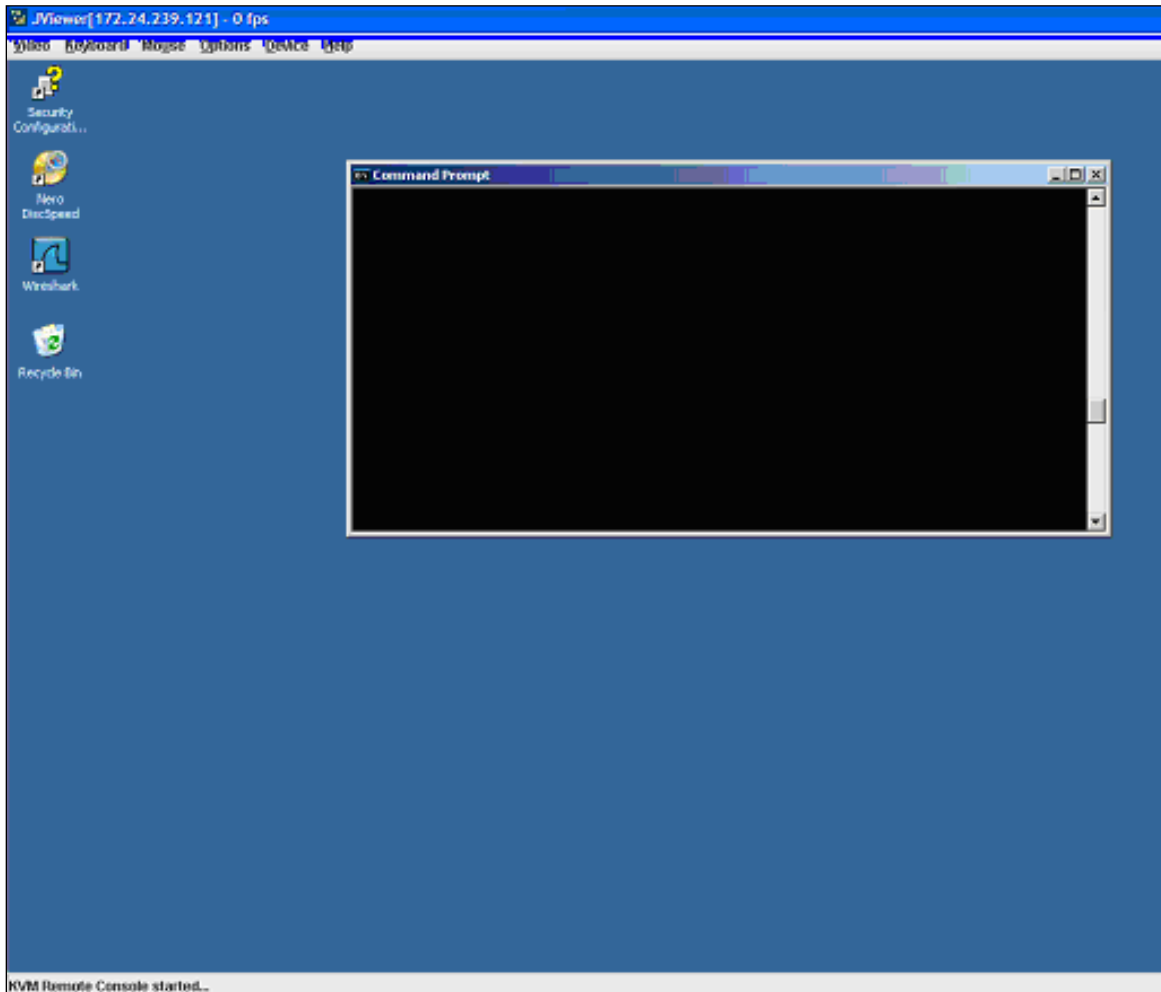


Figure 24: Remote Console Main Window

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 the Intel® RMM3 module 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 25: 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 26.

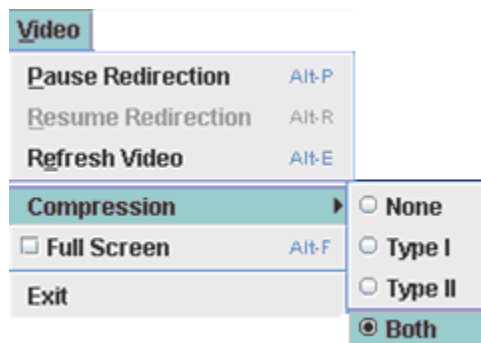


Figure 26: Remote Console Video Menu

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 27.

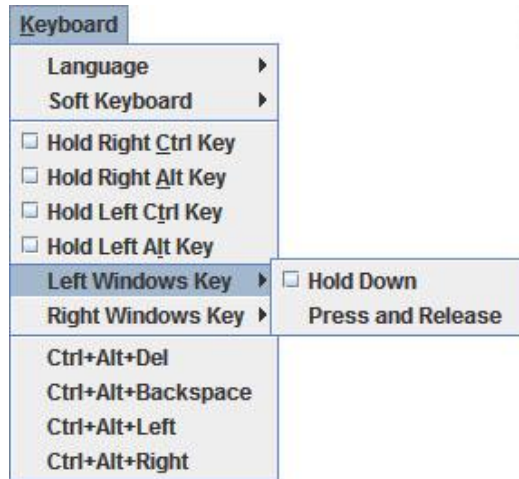


Figure 27: Remote Console Keyboard Menu

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.

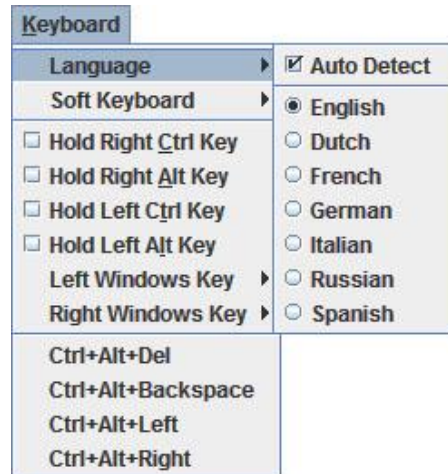


Figure 28: Remote Console Keyboard Language Sub Menu

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 Microsoft 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 do not 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* and 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 29.



Figure 29: 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 30: RMM3 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 31.



Figure 31: 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.

6.3.3.1 Relative Mode Mouse Calibration Procedure

1. If the remote mouse and local mouse cursor are not in synch, 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 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

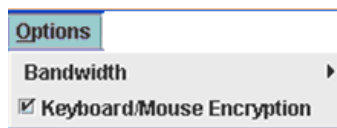


Figure 32: Remote Console Options Menu

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 33: 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 appear 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 34. As you navigate the menu options, the status line gives a more detailed definition of each option.



Keyboard, Video and Mouse redirection

Figure 34: Status Line

7. Intel® RMM3 Web Console Options

This chapter gives you a detailed description of each 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.

Note:

- 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 35.



Figure 35: Busy Indicator Bar

7.1 System Information

By default, the RMM3 home page opens in the System Information page. 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 36.

System Information
This section contains general information about the system.

Summary

System Information

- Host Power Status : **Host is currently ON**
- RMM3 Status : Intel(R) RMM3 installed
- Device (BMC) Available : Yes
- BMC FW Build Time : Oct 6 2012 19:24:57
- BMC FW Rev : 00.61
- Boot FW Rev : 00.19
- SDR Package Version : SDR Package 0.33
- Primary HSC FW Rev : 02.17
- Secondary HSC FW Rev : (not present)
- Mgmt Engine (ME) FW Rev : 01.12
- Local Control Panel (LCP) FW Rev : (not present)

Figure 36: 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).
RMM3 Status	Indicates if the Intel® RMM3 card is present and if the firmware is up to date.
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.

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 37 for details.

The screenshot shows the Intel Remote Management Module 3 web console interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration', and 'Remote Control'. The main content area is titled 'System Information' and contains a section for 'FRU Information'. On the left, there is a sidebar with links for 'System Information', 'FRU Information', and 'System Diagnostics'. The 'FRU Information' section is divided into three sub-sections: 'Chassis Information', 'Board Information', and 'Product Information'. Each sub-section displays various system details.

FRU Information	
System Information	
FRU Information	
System Diagnostics	
Chassis Information	
Type:	Main Server Chassis
Part/Model Number:
Serial Number:
Board Information	
Manufacturing Date :	2010-05-05 23:38
Manufacturer :	Intel Corporation
Product Name :	S5520HC
Serial Number :	QSHZ01700018
Part/Model Number :	E80888-553
FRU File ID :	FRU Ver 0.05
Product Information	
Manufacturer :	Intel Corporation
Name :	S5520HC
Part/Model Number :
Version :
Serial Number :
Asset Tag :
FRU File ID :	

Figure 37: System Information FRU Information page

7.1.3 Viewing System Diagnostics

The System Diagnostic page can be used to download a file that contains data that was collected when a Catastrophic Error (CATERR) occurred on the system. When the BMC firmware sees CATERR asserted, it will try to collect Global error registers data from the chipset on the board. This data can be used to help diagnose what could have caused the CATERR.

To create the log file, press the **Run Diagnostics** button. It may take some time for the file to be created.

Once the diagnostic log dump is finished, you can click the diagnostic 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.

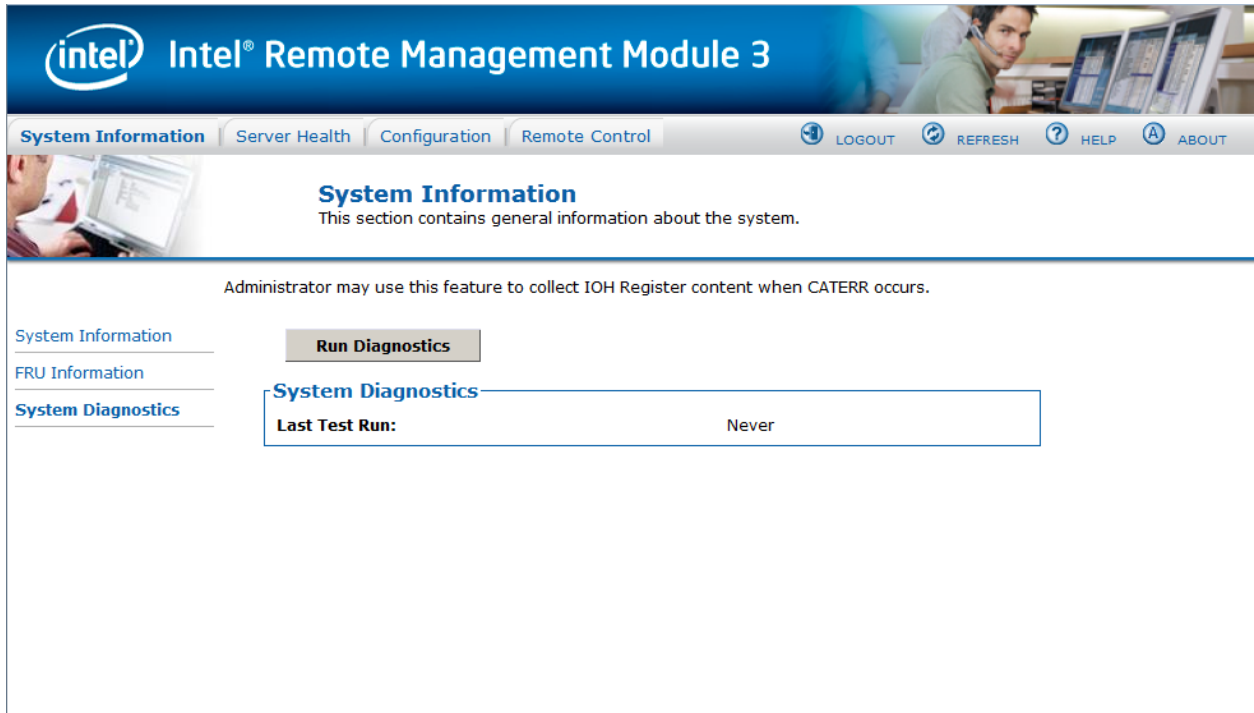


Figure 38: System Diagnostics page

7.2 Server Health

The Server Health page shows you data related to the server's health, such as sensor readings and the event log. Click on the **Server Health** tab to display the page. By default, this tab opens the Sensor Readings page as shown in Figure 40.

7.2.1 Viewing Sensor Readings

The Sensor Readings page displays system sensor information including readings and status.

Server Health
This section shows you data related to the server's health, such as sensor readings and the event log.

Sensor Readings
This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.

Select a sensor type category:
All Sensors

Sensor Readings: 58 sensors

Name	Status	Reading
BB +1.1V IOH	Normal	1.093 Volts
BB +1.1V P1 Vccp	Normal	1.061 Volts
BB +1.1V P2 Vccp	Normal	0.951 Volts
BB +1.5V P1 DDR3	Normal	Not Available
BB +1.5V P2 DDR3	Normal	Not Available
BB +1.8V AUX	Normal	1.773 Volts
BB +3.3V	Normal	3.324 Volts
BB +3.3V STBY	Normal	3.31 Volts
BB Vbat	Normal	3.022 Volts
BB +5.0V	Normal	5.061 Volts
BB +5.0V STBY	Normal	5.061 Volts
BB +12.0V	Normal	12.039 Volts
RR -12.0V	Normal	-11.802 Volts

Refresh Show Thresholds

Figure 39: Server Health Sensor Readings window (Thresholds not displayed)

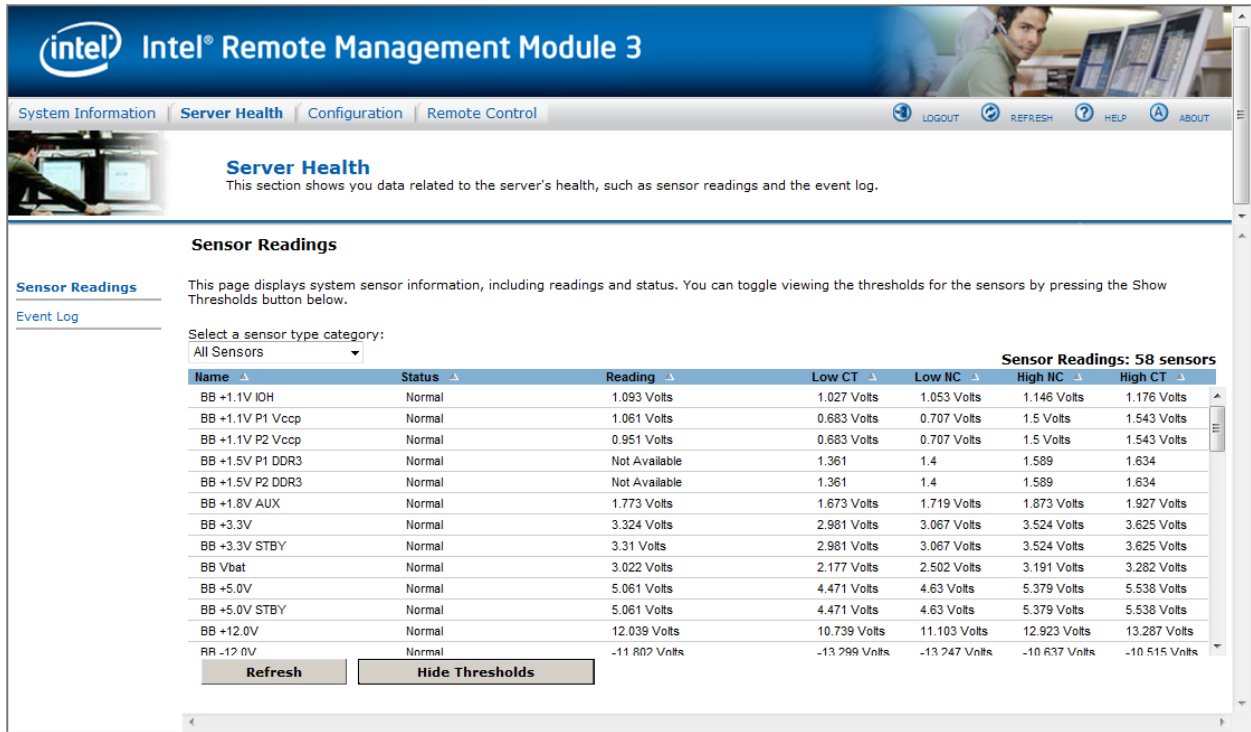


Figure 40: Server Health Sensor Readings window (Thresholds displayed)

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, and readings.
Show Thresholds button	Click to expand the list, showing low and high threshold assignments. See 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 41.

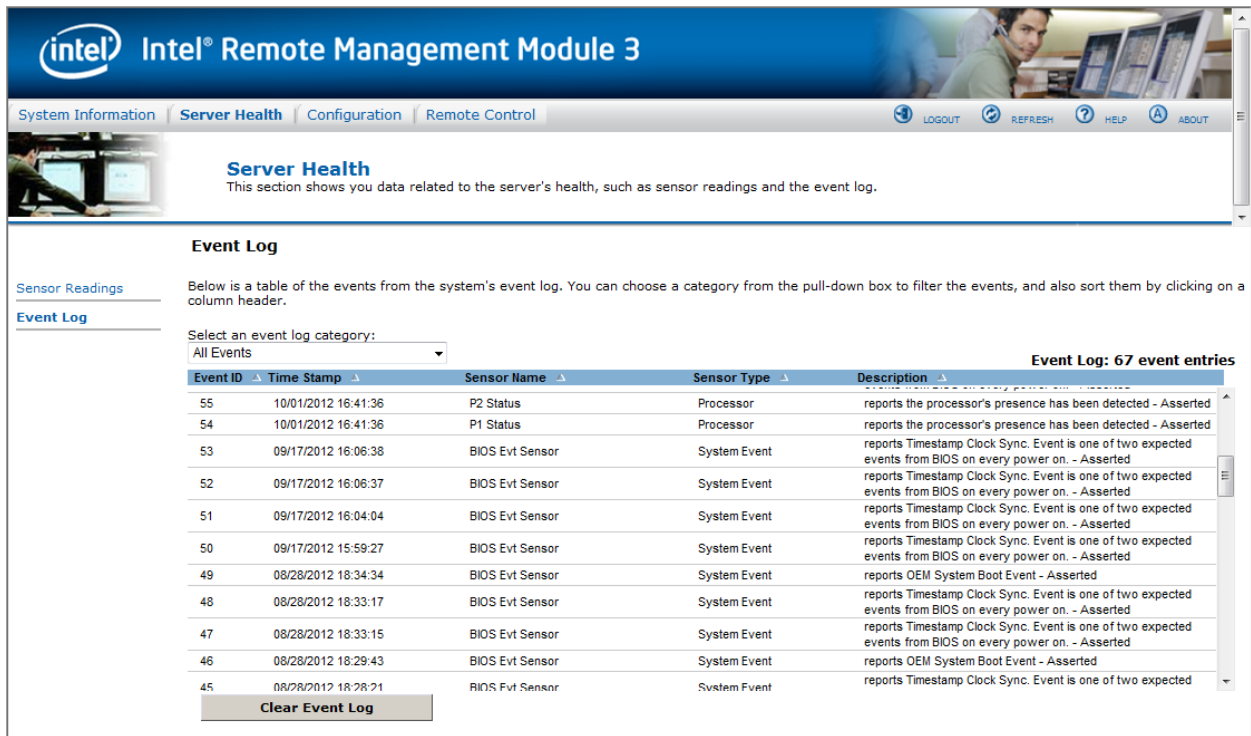


Figure 41: Server Health Event Log

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.

7.3 Configuring Settings

The **Configure** page is used to configure the settings shown in Figure 42. By default, it opens in the **Network Settings** window as shown in Figure 44.

⚠ WARNING

The RMM3 IP address must be on a different subnet than the baseboard IP address used for management traffic.



Figure 42: 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:

- **Automatic:** Obtain an IP address automatically (using DHCP), or
- **Manual:** Manually configure

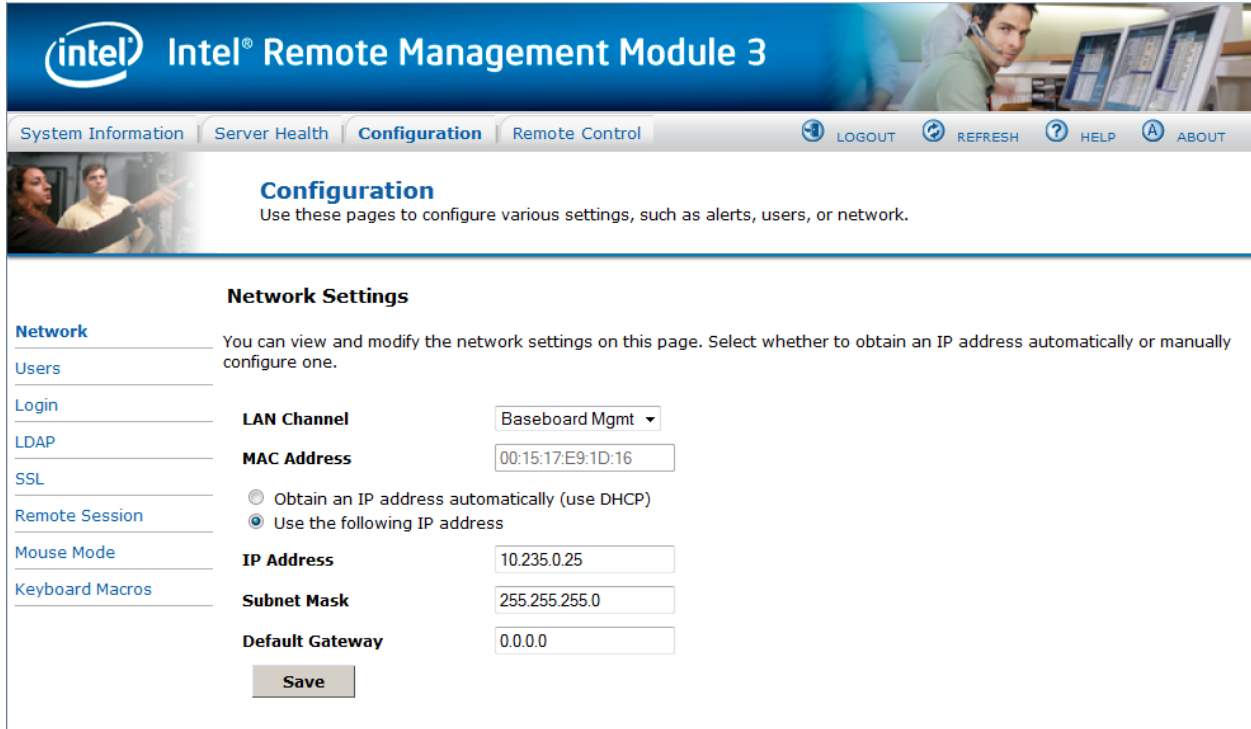


Figure 43: Configuration Network Settings window

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® RMM3 channel is the add-in RMM3 NIC. The Baseboard Management channel (BMC LAN Channel 1) is the 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	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.

Configuration
Use these pages to configure various settings, such as alerts, users, or network.

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	ENABLED	Administrator
3	test1	ENABLED	Administrator
4	test2	ENABLED	Administrator
5	test3	ENABLED	Administrator
6	~	~	~
7	~	~	~
8	~	~	~
9	~	~	~
10	~	~	~
11	~	~	~
12	~	~	~
13	~	~	~
14	~	~	~
15	~	~	~

Figure 44: Configuring User List window

Modify User

Enter the new information for the user below and press Modify. Press Cancel to return to the user list.

User Name:

Change Password

Password:

Confirm Password:

Enable Access

Network Privileges: Administrator ▾

Figure 45: Configuring Users Modify User window

This page has options to configure the IPMI users and privileges for this server. To modify or delete a user, select user name in the list and click **Modify User** or **Delete User**.

Note:

- 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 add user, select an empty slot in the list and click to add a new user.
- To modify user, select a user in the list and click to modify their settings.
- To delete user, select a user in the list and click to delete.

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.



The screenshot displays the Intel Remote Management Module 3 web console interface. At the top, there is a blue header with the Intel logo and the text "Intel® Remote Management Module 3". Below the header is a navigation bar with tabs for "System Information", "Server Health", "Configuration" (which is active), and "Remote Control". To the right of the navigation bar are icons for "LOGOUT", "REFRESH", "HELP", and "ABOUT".

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" (which is selected and highlighted in blue), "LDAP", "SSL", "Remote Session", "Mouse Mode", and "Keyboard Macros".

The "Login Security Settings" section contains the following text: "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." Below this text are two input fields: "Failed Login Attempts" with a value of "3" and "User Lockout Time (min)" with a value of "1". A "Save" button is located below these fields.

Figure 46: Configuring Login Security Settings window

To turn the feature off, set the lockout time to zero. Default is three; failures will lockout a user for one minute.

7.3.4 Configuring LDAP Settings

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

The screenshot shows the Intel Remote Management Module 3 web console interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration', and 'Remote Control'. The 'Configuration' tab is active. Below the navigation bar, there is a 'Logout', 'Refresh', 'Help', and 'About' section. The main content area is titled 'Configuration' and contains a sub-section for 'LDAP Settings'. A sidebar on the left lists various configuration options: Network, Users, Login, LDAP (selected), SSL, Remote Session, Mouse Mode, and Keyboard Macros. The 'LDAP Settings' section includes a checkbox for 'Enable LDAP Authentication', which is currently unchecked. Below this are input fields for 'Port' (389), 'IP Address', 'Bind Password', 'Bind DN', and 'Searchbase'. A 'Save' button is located at the bottom of the form.

Figure 47: 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, for example, "cn=Manager, dc=my-domain, dc=com"
Searchbase	The searchbase of the LDAP server, for example,

Option	Task
	"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.

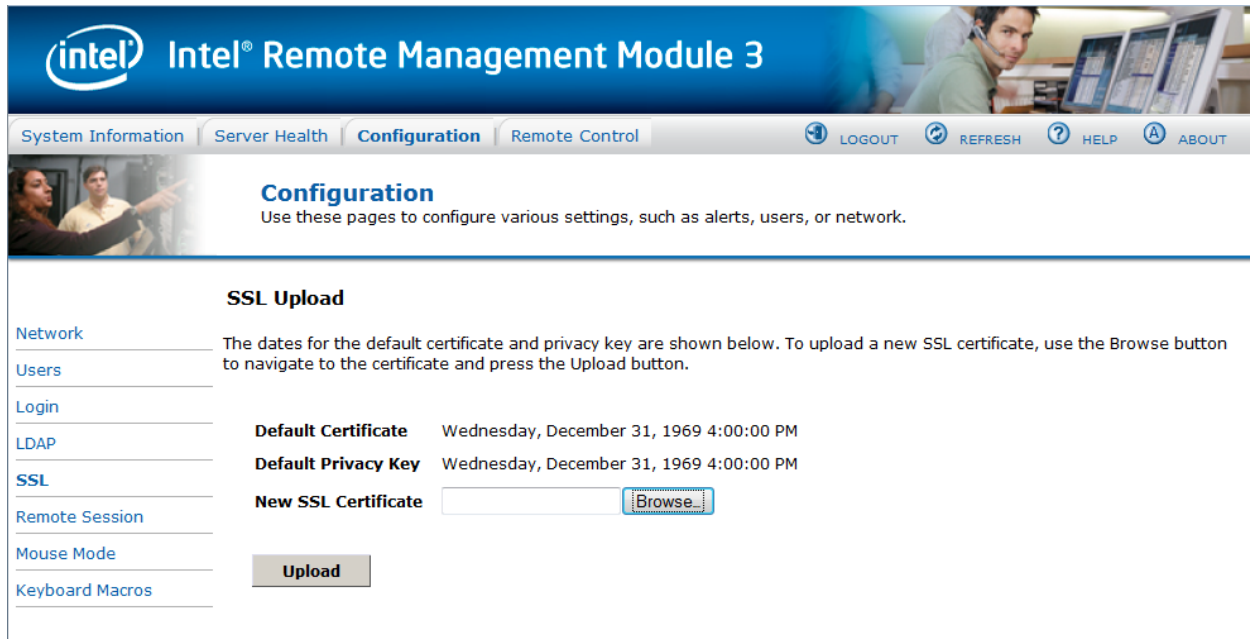


Figure 48: Configuring SSL Upload window

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.

7.4 Configuring Remote Session

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

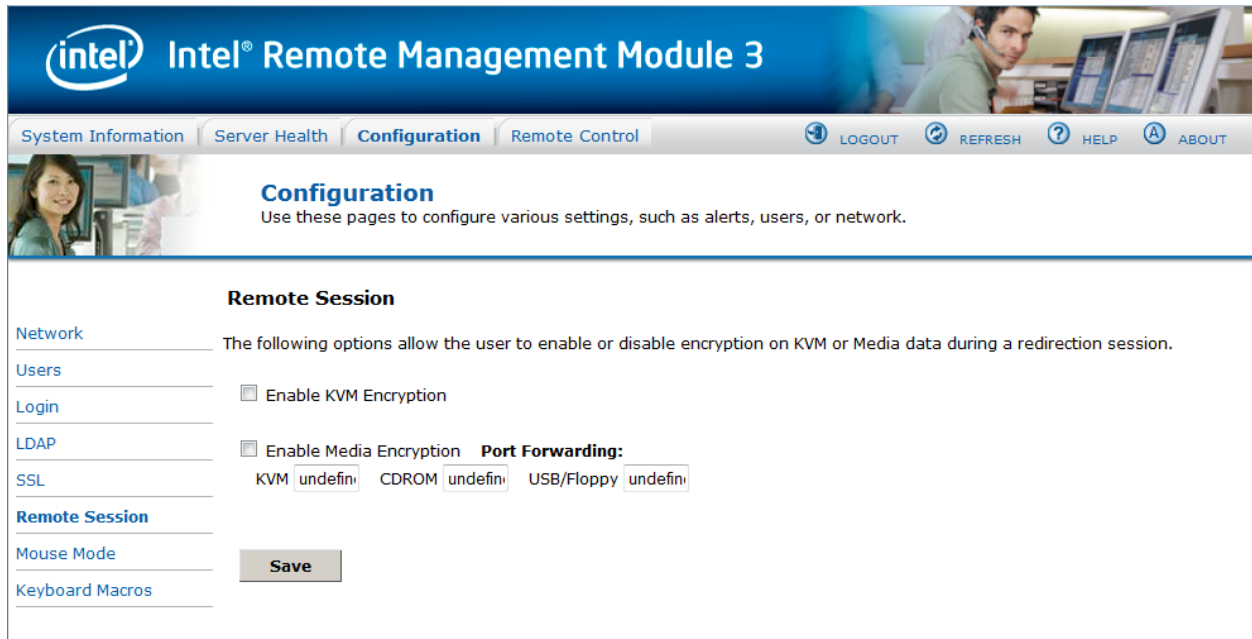


Figure 49: Configuring Remote Session window

The following table lists the options allowing you to enable or disable encryption on KVM or media data 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.
Save button	Click to use selected modes.

7.4.1 Configuring Mouse Mode Setting

Click the **Mouse Mode** tab to view the Mouse Mode Setting window as shown in Figure 50.

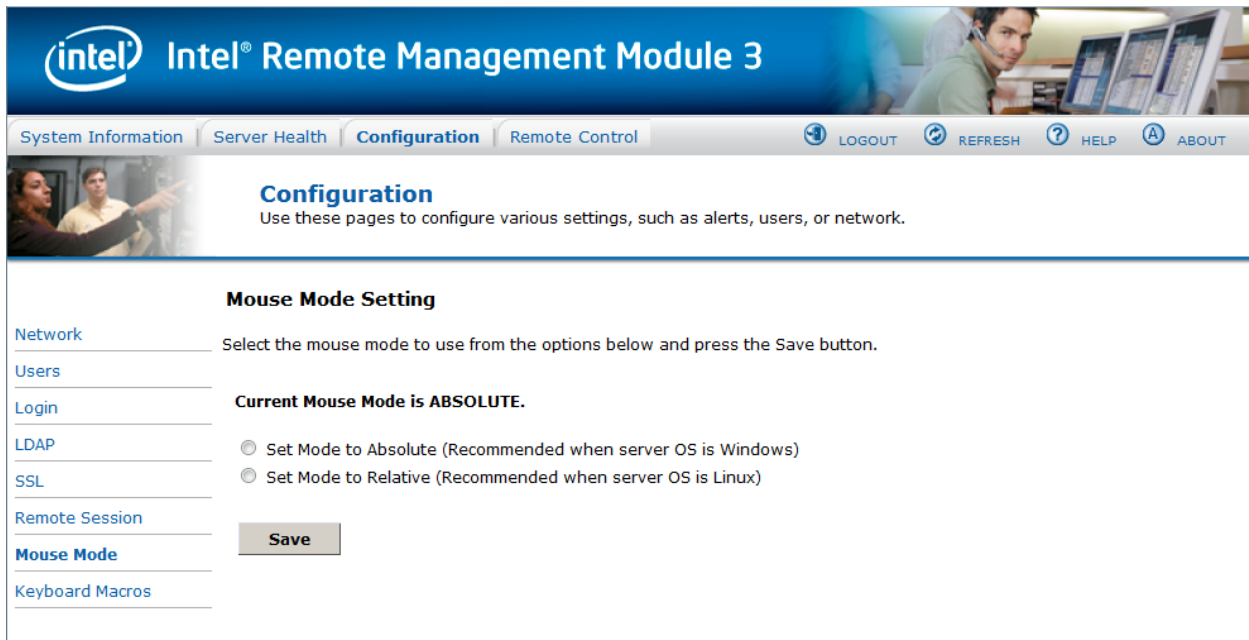


Figure 50: Configuring Mouse Mode Setting window

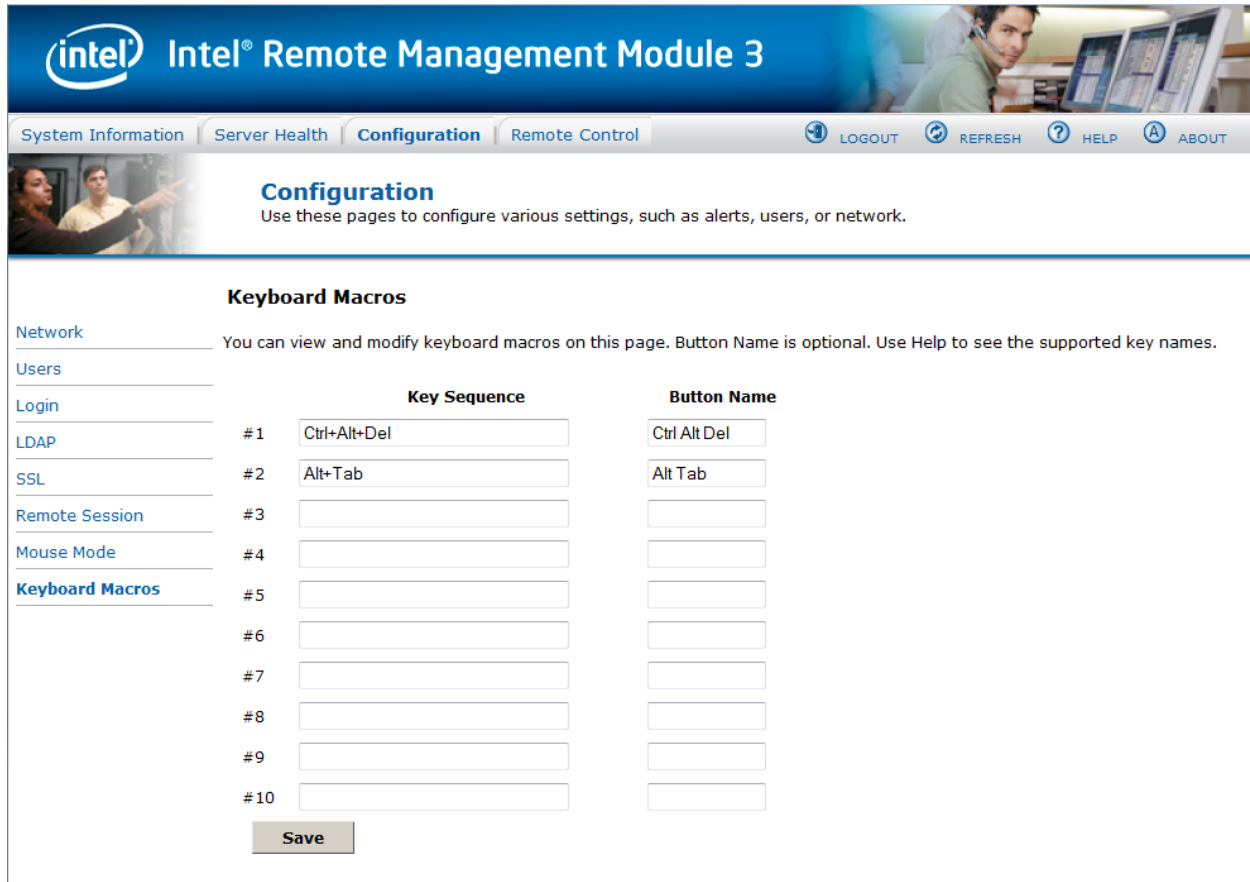
The Redirection Console handles mouse emulation from local window to remote screen in either of two methods:

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

7.4.2 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 Intel Remote Management Module 3 web console interface. The top navigation bar includes 'System Information', 'Server Health', 'Configuration', and 'Remote Control'. The 'Configuration' section is active, displaying a sidebar with links for Network, Users, Login, LDAP, SSL, Remote Session, Mouse Mode, and Keyboard Macros. The main content area is titled 'Keyboard Macros' and contains a table for configuring macros. The table has two columns: 'Key Sequence' and 'Button Name'. There are 10 rows, each with a macro ID (#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 51: Configuring Keyboard Macros window

This makes it convenient to quickly do off 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** get 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, and then only the next time the Remote Console is launched – changes will not affect a Remote Console already running.

7.4.2.1 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 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)	

7.5 Remote Control

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

- Console redirection
- Server power control

7.5.1 Console Redirection

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

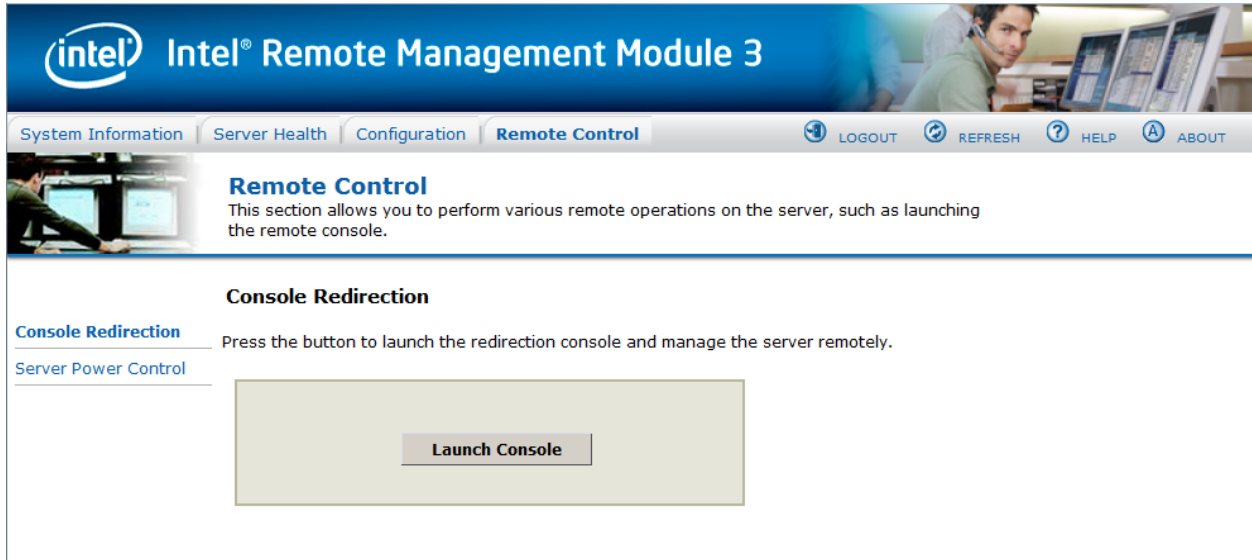


Figure 52: Remote Control Console Redirection window

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

Note: Java Run-Time Environment* (JRE*, version 6 update 10 or later) must be installed on the client prior to launch of JNLP file.

7.5.2 Server Power Control

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

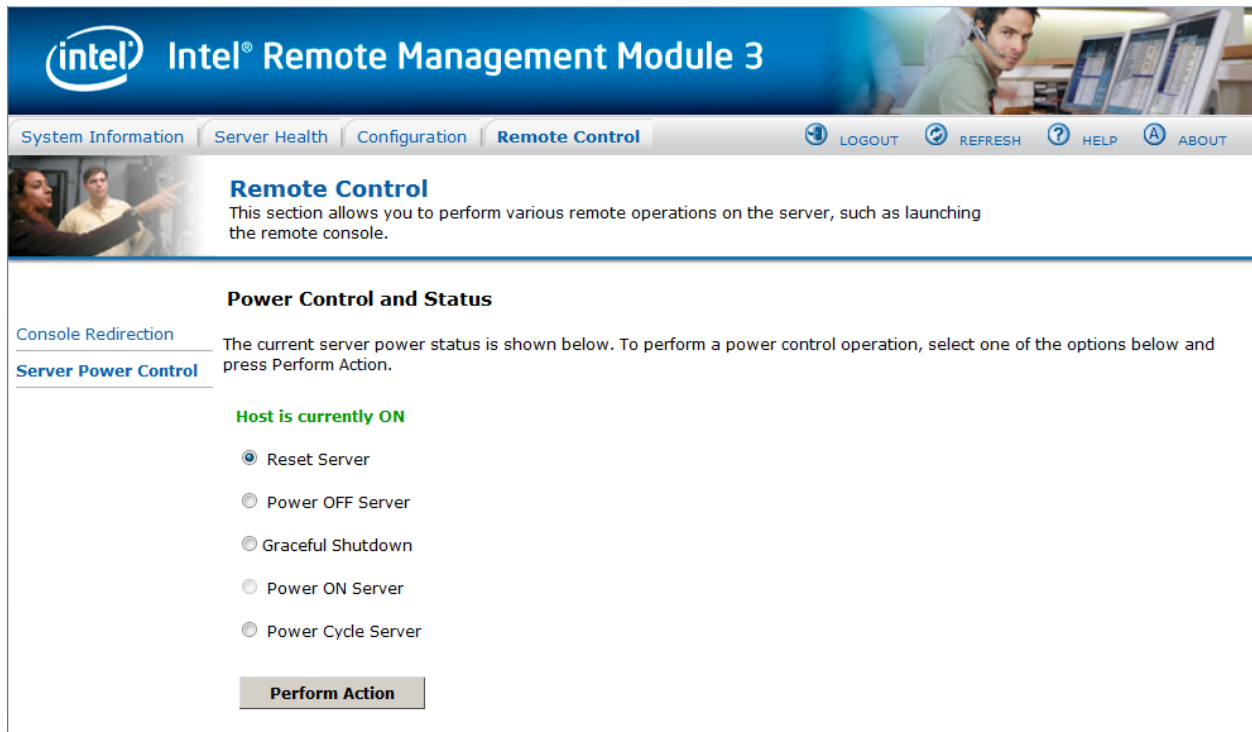


Figure 53: Server Power Control window

The following power control operations can be performed:

Table 11: 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 from the KVM interface or other interface before initiating power actions.	

8. SMASH-Lite* Interface (System Management Architecture for Server Hardware* by AMI*)

The Intel® RMM3 module, that includes Intel® RMM3 Lite and RMM3 Lite-V, supports an interface for the System Management Architecture for Server Hardware* (SMASH-Lite*).

The SMASH* v1.0 suite of specifications was released by the Distributed Management Task Force, Inc. in December, 2006. The information that follows is reproduced with permission from the *SMASH-Lite User Guide** developed by AMI*.

The SMASH-Lite* interface is a direct, command line interface to the RMM3.

8.1 Logging into the SMASH* Session

1. `ssh` to BMC from the client machine.
2. SMASH console screen ('□') should appear. If not, execute `/usr/local/bin/smash` from the `#` prompt.
3. This executable initializes all the required variables, discovers the targets, and displays the SMASH console screen.

8.2 SMASH* Targets

SMASH* targets are the first layer of SMASH that contain two targets - settings1 and system1. Settings1 contains all the current session supported values and system1 is the server/blade.

8.2.1 Supported Properties

The supported property of the SMASH* target is identity.

Table 12: SMASH* Targets - Supported Properties

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.2.2 Supported Verbs

Following are the supported verbs of the SMASH* targets:

Table 13: SMASH* Targets - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```
>> SMASH-CLP Console v1.09 <<
->show
COMMAND COMPLETED :
show

ufip=/
Targets:

    settings1/
    system1/

Properties:
    identity=root

Verbs:
    cd
    exit
    help
    show
    version

-> █
```

Figure 54: SMASH* Target

8.3 System1

The system target represents the server/blade. Power control is available on the target `system1`. It contains `sol1`, `sp1`, and other sensor monitoring targets. Here `sp1` stands for Service Process Configuration.

8.3.1 Supported Properties

The supported properties of the target `system1` are as follows:

Table 14: System1 - Supported Properties

Property	Task
CurrentPowerStatus	This Read-Only property shows the power status of the system as ON or OFF. The value of the property is assigned to any of the following values: <ul style="list-style-type: none"> • ON - If the power status of the system is on, then the value of this property is ON. • OFF - If the power status of the system is off, then the value of this property is OFF.
SysIdSupported	This read only property indicates if System Identification is <ul style="list-style-type: none"> • SUPPORTED or • NOT SUPPORTED
SysIdentification	This R/W property reflects the current state of system identification. <ol style="list-style-type: none"> 1. It can set to any of the following values: <p>System identification can be turned off as follows:</p> <ul style="list-style-type: none"> > Set SysIdentification=OFF <p>System identification can be timed ON as follows:</p> <ul style="list-style-type: none"> > Set SysIdentification=TIMED 2. Set the timeout value. The TimeOutValue property is set to TIMED and SysIdentification property value is set to ON. <p>Note: If set SysIdentification=INDEFINITE, then TimeOutValue property is set to INDEFENITE and SysIdentification property value is set to ON.</p>
TimeOutValue	This value is R/W, which is associated with TIMED (ON) gives input in seconds as follows: <ul style="list-style-type: none"> • INDEFINITE – System identification is ON for an indefinite period of time. • TIMED – System identification is ON for only a known period of time. • OFF – System identification is currently OFF. • If TimeOutValue is TIMED then set the TimeOutValue to <ul style="list-style-type: none"> > Set TimeOutValue=3 (only numeric, non-zero values accepted).
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.3.2 Supported Verbs

The supported verbs of the `system1` targets are as follows:

Table 15: System1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the R/W supported properties.
reset	reset the R/W supported properties
show	show all the targets, properties, and verbs supported by this target.
start	start the device.
stop	stop the device.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1
Targets:

    sensor2/
    sol1/
    sp1/
    system2/
    system3/
    system4/
    pwrsupply1/

Properties:
CurrentPowerStatus=ON
SysIdSupported=SUPPORTED
SysIdentification=OFF
TimeOutValue=INVALID
identity=host

Verbs:
cd
exit
help
reset
set
show
start
stop
version

->

```

Figure 55: System Target

```
->set sysidentification=TIMED
COMMAND COMPLETED :
set sysidentification=TIMED

  ufip=/system1
    sysidentification=TIMED
Please set the Timeoutvalue for timed on

->set TimeOutValue=3
COMMAND COMPLETED :
set TimeOutValue=3

  ufip=/system1
    TimeOutValue=3

->show
COMMAND COMPLETED :
show

  ufip=/system1
    Targets:

      sensor2/
      sol1/
      sp1/
      system2/
      system3/
      system4/
      pwrsupply1/

  Properties:
    CurrentPowerStatus=ON
    SysIdSupported=SUPPORTED
    SysIdentification=ON
    TimeOutValue=TIMED
    identity=host

  Verbs:
    cd
    exit
    help
    reset
    set
```

Figure 56: Example of System Target

8.4 Settings1

Settings1 target represents the settings of the current session of SMASH* and does not have any targets. This target affects the current session:

8.4.1 Supported Properties

The supported properties of the target `settings1` as follows:

Table 16: Settings1 - Supported Properties

Property	Task
cdt	Represents the current default directory. This is the path from where the session starts.
outputformat	<p>This R/W property gives the output format: clpxml, text, clpcsv.</p> <p>Keyword of the current running SMASH* session. The values supported by this property are explained as follows:</p> <ul style="list-style-type: none"> • Clpxml – The output format of the current running SMASH* session is in the .xml format > set outputformat=clpxml • Keyword – The output format of the current running SMASH8 session is in the keyword format > set outputformat=keyword. • Text – The output format of the currently running SMASH session is in the text format- >set outputformat=text. By default, this property value is assigned to text. • Clpcsv – This output format of the currently running SMASH* session has a “clpcsv” table to represent the Command Status. Each line of the “clpcsv” output data has its first item either as the “header” or as the “group” keyword. Rows beginning with the “header” keyword specify the start of a new table and the items in the comma-separated list of keywords identify the output data elements that appear in each row of the table. Rows beginning with the “group” keyword specify a row of table values for the preceding header.
timeout	<ul style="list-style-type: none"> • The R/W property timeout represents the inactivity timeout value in seconds of the currently running SMASH* session. If the SMASH* session is inactive for the timeout value seconds mentioned, then after reaching the timeout value this session will exit automatically. <p>The value of this property can be set to a preferred inactivity time. > set timeout=300. By default it is assigned to 500.</p>
identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.4.2 Supported Verbs

The supported verbs of the `settings1` target are as follows:

Table 17: Settings1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the R/W supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

ufip=/settings1

Properties:
  cdt=NULL
  outputformat=text
  timeout=500
  identity=session parameters

Verbs:
  cd
  exit
  help
  set
  show
  version

->
```

Figure 57: Setting1 Target

8.5 SP1

The SP1 target (service processor) provides information of the user accounts Ethernet port and logs. It contains three targets - `enetport1` (Ethernet port target), accounts, and logs.

8.5.1 Supported Properties

The supported property of the SMASH* target is identity.

Table 18: SP1 - Supported Properties

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.5.2 Supported Verbs

The supported verbs of the `sp1` target are as follows:

Table 19: SP1 - Supported Verbs

Verb	Is used to
<code>cd</code>	change from one valid target path to any other valid target path.
<code>exit</code>	exit from the current SMASH* session.
<code>help</code>	provide information on using SMASH*.
<code>show</code>	show all the targets, properties, and verbs supported by this target.
<code>version</code>	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1
Targets:

    account10/
    account1/
    account2/
    account3/
    account4/
    account5/
    account6/
    account7/
    account8/
    account9/
    enetport1/
    logs1/

Properties:
    identity=service processor

Verbs:
    cd
    exit
    help
    show
    version

->

```

Figure 58: SP1 Target

8.6 SOL1

Serial Over LAN (SOL) is the name for the redirection of baseboard serial controller traffic over an IPMI session. It does not have any targets.

8.6.1 Supported Properties

The supported property of the target `soll` is as follows:

Table 20: SOL1 - Supported Properties

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.6.2 Supported Verbs

The supported verbs of the `soll` target are as follows:

Table 21: SOL1 - Supported Verbs

Verb	Is used to
<code>cd</code>	change from one valid target path to any other valid target path.
<code>exit</code>	exit from the current SMASH* session.
<code>help</code>	provide information on using SMASH*.
<code>show</code>	show all the targets, properties, and verbs supported by this target.
<code>start</code>	start the device.
<code>version</code>	show the current version of SMASH*.

```
->cd soll
COMMAND COMPLETED :
cd soll

  ufip=/system1/soll

->show
COMMAND COMPLETED :
show

  ufip=/system1/soll
  Properties:
    identity=serial redirection

  Verbs:
    cd
    exit
    help
    show
    start
    version

->
```

Figure 59: SOL1 Target

8.6.3 Terminating an SOL Session

SOL session can be terminated using the following control key sequence:

- CR, ESC, T or t
- CARRIAGE RETURN/ENTER key, followed by ESCAPE key, followed by T or t
- Control key sequence 'Ctrl + [can be used in place of ESCAPE key].

Once terminated, the control returns to SMASH-Lite* session.

8.7 Enetport1

The BMC in the managed system needs the system's IP Address and MAC Address in order to be able to respond to UDP/IP packets or generate LAN alerts. `Enetport1` (Ethernet port target) gives the port address information. `Enetport1` contains only one target named `lanendpt1`.

8.7.1 Supported Properties

The supported properties of the target `enetport1` are as follows:

Table 22: Enetport1 - Supported Properties

Property	Task
macaddress	Address that was received by the activated session. This read only property gives the value of the MAC address. Mac address is a unique identifier attached to most network adaptors (NICs).
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.7.2 Supported Verbs

The supported verbs of the `enetport1` target are as follows:

Table 23: Enetport1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/enetport1
Targets:

    lanendpt1/

Properties:
    macaddress=00:5A:4A:3C:2E:41
    identity=ethernet port

Verbs:
    cd
    exit
    help
    show
    version

->

```

Figure 60: Enetport1 Target

8.8 Lanendpt1

The target `lanendpt1` gives information about LAN configuration. It contains the target: `Ipendpt1` - IP configuration.

8.8.1 Supported Properties

Following is the supported property of target `lanendpt1`:

Table 24: Lanendpt1 - Supported Properties

Property	Task
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.8.2 Supported Verbs

The supported verbs of the `lanendpt1` target are as follows:

Table 25: Lanendpt1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
start	start the device.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/enetport1/lanendpt1
Targets:

    ipendpt1/

Properties:
    identity=lan information

Verbs:
    cd
    exit
    help
    show
    version

->

```

Figure 61: LANENDPT1 Target

8.9 Ipendpt1

The target `ipendpt1` provides information about `ipaddress` and other information related to the SP. It contains two targets - `dnsendpt1` and `remotesap1`. The supported properties and supported verbs of the `ipendpt1` are as follows.

8.9.1 Supported Properties

The supported properties of the target `ipendpt1` are as follows:

Table 26: Ipendpt1 - Supported Properties

Property	Task
ipaddress	<p>The value of ipaddress is the IP address of the SP. An IP address (Internet Protocol address) is a unique address that is used to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). This is an R/W property. The value setting to the ipaddress affects the IP of the SP.</p> <p>> set ipaddress=10.0.4.79</p> <p>This will change the ipaddress of the sp. After changing, use committed property to save.</p>
subnetmask	<p>This is the value of the subnetmask of the SP. A subnetmask is a range of logical addresses within the address space that is assigned to an organization. This is an R/W property. The value setting to the ipaddress affects the IP of the SP.</p> <p>> set subnetmask=255.255.248.0</p> <p>This will change the subnetmask of the sp. After changing, use committed property to save.</p>
usedhcp	<p>Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices to obtain various parameters necessary for the networked devices to operate in an Internet Protocol (IP) network. This property has two values (1 for DHCP and 0 for Static). This is a R/W property.</p> <p>> set usedhcp=1</p>
committed	<p>Once the ipaddress or subnetmask is set to 1, the property saves all the changes made. In addition, the network settings also change and network connection is lost.</p> <p>> Set committed=1</p>
Identity	<p>This read only property gives a brief explanation of the present target and cannot be changed.</p>

8.9.2 Supported Verbs

The supported verbs of the `ipendpt1` target are as follows:

Table 27: Lanendpt1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the r/w supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

  ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1
  Targets:

      dnsendpt1/
      remotesap1/

  Properties:
      ipaddress=10.0.3.26
      subnetmask=255.255.248.0
      usedhcp=1
      committed=1
      identity=network parameters

  Verbs:
      cd
      exit
      help
      set
      show
      version

->

```

Figure 62: IPENDPT1 Target

8.10 Remotesap1

The `remotesap1` target will enumerate all the configurable IPs under the containing target. A remote access server enables users who are not on a local network to access. This does not contain any targets.

8.10.1 Supported Properties

The supported properties of the target `remotesap1` are as follows:

Table 28: Remotesap1 - Supported Properties

Property	Task
defaultgatewayaddress	<ul style="list-style-type: none"> IP address of the gateway. A gateway address is a private address and is the address to which traffic is sent from the LAN .This is an R/W property. The value of the gateway can be set as follows: <ul style="list-style-type: none"> > Set defaultgatewayaddress =0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.10.2 Supported Verbs

The supported verbs of the `remotesap1` target are as follows.

Table 29: Remotesap1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the r/w supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

uftp=/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1
Properties:
  defaultgatewayaddress=0.0.0.0
  identity=remote server access point

Verbs:
  cd
  exit
  help
  set
  show
  version

->

```

Figure 63: REMOTESAP1 Target

8.11 Dnsendpt1

The `dnsendpt` target has the configurable parameters for Domain Name System (DNS). The DNS associates various sorts of information with so-called domain names; most importantly, it serves the Internet by translating human-readable computer hostnames into the IP address, information that the networking equipment needs to deliver. `Dnsendpt1` contains two targets - `remotesap1` and `remotesap2`. The supported properties of `dnsendpt1` are as follows:

8.11.1 Supported Properties

The supported properties of the target `dnsendpt1` are as follows:

Table 30: Dnsendpt1 - Supported Properties

Property	Task
domainnamefromdhcp	Dhcp based DNS configuration. This is a read only property.
dnsdomainname	This property gives the DNS Domain. This is a read only property.
serversfromdhcp	This property shows the servers dhcp. This is a read only property.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.11.2 Supported Verbs

The supported verbs of the `dnsendpt1` target are as follows:

Table 31: Dnsendpt1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.


```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1
Targets:

    remotesap1/
    remotesap2/

Properties:
    domainnamefromdhcp=1
    dnsdomainname=Unknown
    serversfromdhcp=1
    identity=parameters of DNS

Verbs:
    cd
    exit
    help
    show
    version

->

```

Figure 64: DNSENDPT1 Target

8.12 Remotesap1

The `remotesap1` target enumerates all the configurable IPs under the containing target. A remote access server enables user access to those users who are not on a local network. This does not contain any targets.

8.12.1 Supported Properties

The supported properties of the target `remotesap1` are `dnsserveraddress` and `identity`.

Table 32: Remotesap1 - Supported Properties

Property	Task
dnsserveraddress	This property gives the dns server address. This is a R/W property. The value of this property can be set as follows: > set dnsserveraddress=0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.12.2 Supported Verbs

The supported verbs of the `remotesap1` target as follows:

Table 33: Remotesap1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the r/w supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

The `remotesap1` target enumerates all the configurable IPs under the containing target. A remote access server enables users who are not on a local network to access. This does not contain any targets.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1
Properties:
  dnsserveraddress=0.0.0.0
  identity=remote server access point

Verbs:
  cd
  exit
  help
  set
  show
  version

->

```

Figure 65: REMOTESAP1 Target

8.13 Remotesap2

8.13.1 Supported Properties

The supported properties of the target `remotesap2` are as follows:

Table 34: Remotesap2 - Supported Properties

Property	Task
dnsserveraddress	Gives the dns server address. This is a R/W property. The value of this property can be set as follows: > set dnsserveraddress=0.0.0.0
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.13.2 Supported Verbs

The supported verbs of the `remotesap2` target are as follows.

Table 35: Remotesap2 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
set	set the r/w supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2

Properties:
  dnsserveraddress=0.0.0.0
  identity=remote server access point

Verbs:
  cd
  exit
  help
  set
  show
  version

->

```

Figure 66: REMOTESAP2 Target

8.14 Account

The `account` target represents user accounts. It does not contain any targets.

8.14.1 Supported Properties

The supported properties of the target `account` are as follows:

Table 36: Account - Supported Properties

Property	Task
userid	This read only property defines the unique id for each user.
username	This property gives the user name of a particular account. This is settable except for <code>userid=1</code> . Username Length must be more than 1 character and less than 16 characters. > set username=sdf
ipmilanprivileges	This property gives the ipmi LAN privileges. It can be set except for <code>userid=1</code> . Only numbers are allowed. > set ipmilanprivileges=4
password	This property gives the password of a particular user. It can be set except for <code>userid=1</code> ; password length should be less than 16 characters. > set password=ssd
enabledstate	This property shows the state of the user. This property is settable except for <code>userid=1</code> . Use 0 for disable and 1 for enable. For example to enable the user set the value of this property to 1

Property	Task
	<pre>> set userid=1</pre> For example to enable the user set the value of this property to 1 <pre>> set userid=1</pre>
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.14.2 Supported Verbs

The supported verbs of the `account` target are as follows:

Table 37: Account - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
delete	delete. To delete, go to sp1 target and delete account(n) where n>2.
set	set the r/w supported properties.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->cd account1
COMMAND COMPLETED :
cd account1

  ufip=/system1/sp1/account1

->show
COMMAND COMPLETED :
show

  ufip=/system1/sp1/account1
  Properties:
    userid=1
    username=anonymous
    ipmilanprivileges=4
    password=[INVISIBLE]
    enabledstate=User is enabled
    identity=user account

  Verbs:
    cd
    delete
    exit
    help
    set
    show
    version

->

```

Figure 67: ACCOUNT1 Target

8.15 Logs1

The logs target is the containing target for log records of the `ipmi sel`. The System Event Log is a non-volatile repository for system events and certain system configuration information. This target contains all the read only properties. It contains log records as the targets.

8.15.1 Supported Properties

The supported properties of the target `Logs1` are as follows:

Table 38: Logs1 - Supported Properties

Property	Task
MaxNumberOfRecords	This read only property gives information about maximum number of log records.
Description	A read only description about the target.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.15.2 Supported Verbs

The supported verbs of the `Logs1` target are as follows:

Table 39: Logs1 - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
delete	delete. To delete, go to sp1 target and delete account(n) where n>2.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```
->show
COMMAND COMPLETED :
show

ufip=/system1/sp1/logs1
Targets:

    record10/
    record11/
    record12/
    record13/
    record1/
    record2/
    record3/
    record4/
    record5/
    record6/
    record7/
    record8/
    record9/

Properties:
    MaxNumberOfRecords=3639
    CurrentNumberOfRecords=13
    Description=IPMI SEL
    identity=IPMI SEL

Verbs:
    cd
    delete
    exit
    help
    show
    version
```

Figure 68: LOGS1 Target

8.16 Record

The record target represents the individual SEL entries. SEL records are in a list. Each SEL entity is a record. This does not have any targets.

8.16.1 Supported Properties

The supported properties of the target `Record1` are as follows:

Table 40: Record - Supported Properties

Property	Task
LogCreationClassName	This read only property gives information about the log creation class name.
logname	This read only property gives the name of the log record.
CreationClassName	This read only property gives the creation class name of the record.
RecordID	SEL Entries have a unique 'Record ID' field. This is the unique ID for the particular record. This is a read only property.
MessageTimeStamp	This read only property gives the time stamp of the record creation.
RecordData	The record data field that is passed in the request consists of all bytes of the SEL event record. This property gives information of the record and is read only.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.16.2 Supported Verbs

The supported verbs of the record target are as follows:

Table 41: Record - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.


```
->show
COMMAND COMPLETED :
show

ufip=/system1/sensor2
Properties:
  Description=MDS-voltage33SBV(1.0.32):CIM Voltage for system1
  systemCreationClassName=CIM_ComputerSystem
  CurrentReading=3.32
  BaseUnits=Volts
  SystemName=system1
  CreationClassName=CIM_Sensor
  DeviceID=1.0.32
  Name=MDS-voltage33SBV(1.0.32)
  SensorType=CIM Voltage
  HealthState=Not Defined
  OperationalStatus=Not Defined
  identity=MDS-voltage33SBV(1.0.32):CIM Voltage for system1

Verbs:
  cd
  exit
  help
  show
  version

->
```

Figure 69: RECORD1 Target

8.17 Sensor

A typical server BMC would provide sensors for baseboard temperature, voltage, and chassis intrusion monitoring. A sensor uses one type of energy, a signal of some sort, and converts it into a reading for the purpose of information transfer. The sensor does not have any targets. All properties of this target are read only properties.

8.17.1 Supported Properties

Table 42: Sensor - Supported Properties

Property	Task
Description	This read only property describes the sensor and the target under which it is present.
SystemCreationClassName	This read only property gives the system creation class name and is a read only property.
CurrentReading	This read only property gives the current reading shown by the sensor.
BaseUnits	This read only property gives the units for the value given by current reading property.
SystemName	This read only property gives the target name under which this sensor exists.
CreationClassName	This read only property gives the creation class name of the sensor.
DeviceID	This read only property gives the device ID.
Name	This read only property gives the name of the current sensor.
SensorType	This read only property gives the type of sensor.
HealthState	This read only property gives the health status of the sensor.
OperationalStatus	This read only property defines the operational status of the sensor.
Identity	This read only property gives a brief explanation of the present target and cannot be changed.

8.17.2 Supported Verbs

The supported verbs of the sensor target are as follows:

Table 43: Sensor - Supported Verbs

Verb	Is used to
cd	change from one valid target path to any other valid target path.
exit	exit from the current SMASH* session.
help	provide information on using SMASH*.
show	show all the targets, properties, and verbs supported by this target.
version	show the current version of SMASH*.

```

->show
COMMAND COMPLETED :
show

ufip=/system1/sensor2
Properties:
  Description=MDS-voltage33SBV(1.0.32):CIM Voltage for system1
  systemCreationClassName=CIM_ComputerSystem
  CurrentReading=3.32
  BaseUnits=Volts
  SystemName=system1
  CreationClassName=CIM_Sensor
  DeviceID=1.0.32
  Name=MDS-voltage33SBV(1.0.32)
  SensorType=CIM Voltage
  HealthState=Not Defined
  OperationalStatus=Not Defined
  identity=MDS-voltage33SBV(1.0.32):CIM Voltage for system1

Verbs:
  cd
  exit
  help
  show
  version

->

```

Figure 70: SENSOR2 Target

8.18 Creating Targets

Dynamic targets in SMASH* (without CIM) are the sensors and their associated entities. You need to go through the SDR and search for Full and Compact record types. Name the Full type as *numsensor<index>* (indicates the analog sensors) and the Compact type as the *sensor<index>* (indicates the discrete sensors). While a sensor instance is discovered, the **EntityID** and the **EntityInstance** of the record are also seen. **EntityID** denotes the entity the sensor is monitoring. If the **EntityID** is of type CPU and **EntityInstance** is 1, then the parent of *sensor1* will be *cpu1*. Other sensor related entity instances are created in a similar manner.