Intel® Remote Management Module 3

User Guide

Revision 1.0

March 2009

Legal Statements

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS FOR THE PURPOSE OF SUPPORTING INTEL DEVELOPED SERVER BOARDS AND SYSTEMS. 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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. 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.

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

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

AMI is a trademark, or registered trademark, a property of American Megatrends, Inc in the United States and/or other countries.

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

Table of Contents

List of Figures

<This page intentionally left blank.>

1 Introduction

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

Designed to work with the Integrated Baseboard Management Controller (BMC), this small form-factor mezzanine card enables server control via a built-in Web Console from anywhere, at 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 Guide 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.

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
FML	Fast Management Link
FPGA	Field Programmable Gate Array
ICMP	Internet Control Message Protocol
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
OOB	Out Of Band- No operating system interaction on Server
PBDE	Polybrominated Biphenyls Diphenyl Ethers
RMII	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.

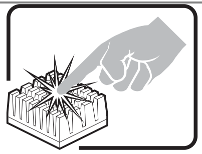
⚠ **Installing or removing jumpers:** A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle nosed pliers. If your jumpers do not have such a tab, take care when using needle 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://support.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:

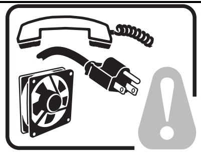
1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide some electrostatic 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://support.intel.com/support/motherboards/server/sb/cs-010770.htm.



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

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

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

⚠ 重要安全指导

在执行任何指令之前，请阅读本文档中的所有注意事项及安全声明。参见 Resource CD（资源光盘）和/或http://support.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://support.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.

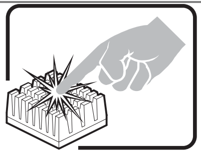
Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.

⚠ 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://support.intel.com/support/motherboards/server/sb/cs-010770.htm.

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

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

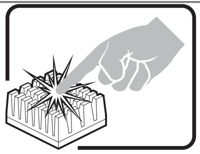


Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

⚠ AVVERTENZA: Italiano

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

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



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

1.4 Support Information

If you encounter an issue with your server system, follow these steps to obtain support:

1. Visit the following Intel support web page: http://support.intel.com/support/motherboards/server

   This web page provides 24x7 support when you need it 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 to your issue, send an email to Intel's technical support center using the online form available at http://supportmail.intel.com/scripts-emf/welcome.aspx
3. Lastly, you can contact an Intel support representative using one of the support phone numbers available at http://support.intel.com/support/9089.htm

   (charges may apply). Intel customer support suggests filling out the issue report form (see Appendix A) to better service the issue.

   Intel also offers Channel Program members around-the-clock 24x7 technical phone support on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management at http://www.intel.com/reseller/

   Note: *You will need to log in to the Reseller site to obtain the 24x7 number.*

1.4.1 Warranty Information

To obtain warranty information, visit the following Intel web site:

http://support.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 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.

2.1 Intel® RMM3 Features

The Intel® RMM3 add-on card offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs in the Integrated Baseboard Management Controller, utilizing expanded capabilities provided by the Intel® RMM3 hardware, so there is no impact to the server operation or network performance.

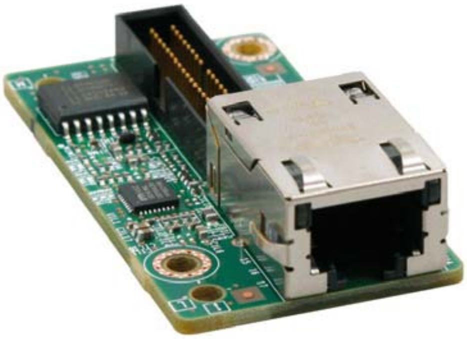


Figure 1. Intel® Remote Management Module 3

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 UI - Remote Power on\off, system health, system info, Event log.
- KVM redirection via Dedicated NIC or through the server board NIC used for management traffic – high performance, multiple concurrent sessions. KVM can be redirected to either the RMM3 NIC or the server board NIC used for management traffic.

- 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; allows remote viewing and configuration in pre-boot POST and BIOS setup.

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 (KVM) connections. During Remote Console connections, the Keyboard, Mouse, and Video of the console system operate just as if you were at the server where the Intel® RMM3 is connected. During Remote Console connections, the interaction with the host operating system limits the support to operating systems that have been validated. The validated operating systems are listed below.

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
- Red Hat* Enterprise Linux 5.2
- SuSE* 10 SP1
- Red Hat* Enterprise Linux 5.2 U3
- Red Hat* Enterprise Linux 5.2 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* 3.01
- 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

Before working with your server product, pay close attention to the Safety Information at the beginning of this manual.

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 is currently supported on the following Intel® server boards:

- All SKUs of Intel® Server Board S5500BC
- All SKUs of Intel® Server Board S5520HC
- All SKUs of Intel® Workstation Board S5520SC
- All SKUs of Intel® Server Board S5520UR
- All SKUs of Intel® Server Board S5520WB

The Intel® RMM3 box contains the following components:

- Intel® Remote Management Module
- Plastic bag containing screws, slot bracket and cabling

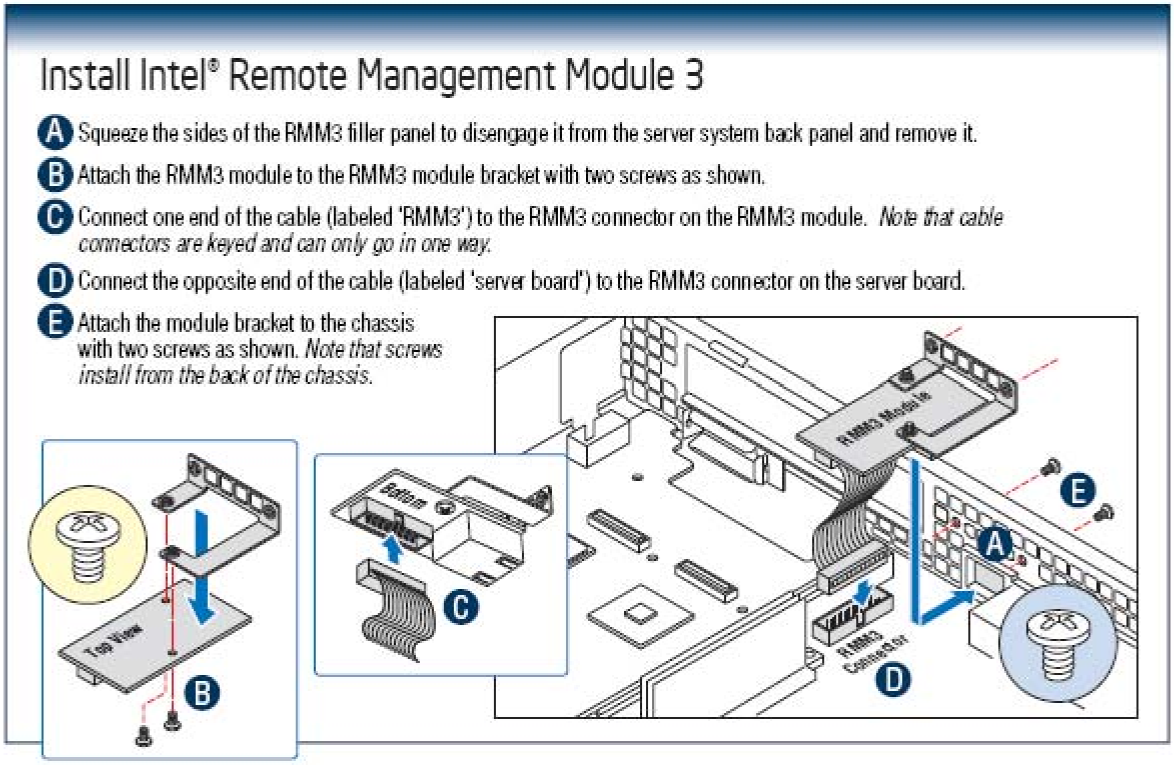
The installation varies between these server boards and their chassis configurations. The following sections detail installation instructions.

⚠ **Caution:** Remove AC power from the server and wait at least 10 seconds before installing the Intel® RMM3.

3.3.1 Installation on Intel® Server Boards S5500UR and S5500WB

The Intel® Server Boards S5500UR and S5500WB install in a rack mount 1U or 2U chassis. The same installation steps apply to both chassis types. The high-level steps are provided below. For detailed instructions, refer to the individual Server Board and/or System Service Guides.

1. Mount the Intel® RMM3 module to the header on the server board and secure the metal fastening bracket to the back of the chassis as shown in figure 2. This aligns the RJ-45 with the opening in the chassis.



Install Intel® Remote Management Module 3

A Squeeze the sides of the RMM3 filler panel to disengage it from the server system back panel and remove it.

B Attach the RMM3 module to the RMM3 module bracket with two screws as shown.

C Connect one end of the cable (labeled 'RMM3') to the RMM3 connector on the RMM3 module. *Note that cable connectors are keyed and can only go in one way.*

D Connect the opposite end of the cable (labeled 'server board') to the RMM3 connector on the server board.

E Attach the module bracket to the chassis with two screws as shown. *Note that screws install from the back of the chassis.*

Figure 2. Installing Intel® RMM3 on Intel® Server Boards S5500UR and S5500WB

2. Replace the chassis cover, attach AC power, and connect a network cable to the Intel® RMM NIC.

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

The Intel® Server Boards S5520HC, S5520BC, and S5520SC install in a pedestal style chassis. The high-level steps are provided below. For detailed instructions, refer to the individual Server Board and/or System Service Guides.

1. Attach the cable from the server board to the Intel® RMM3 module as shown in figure 3.

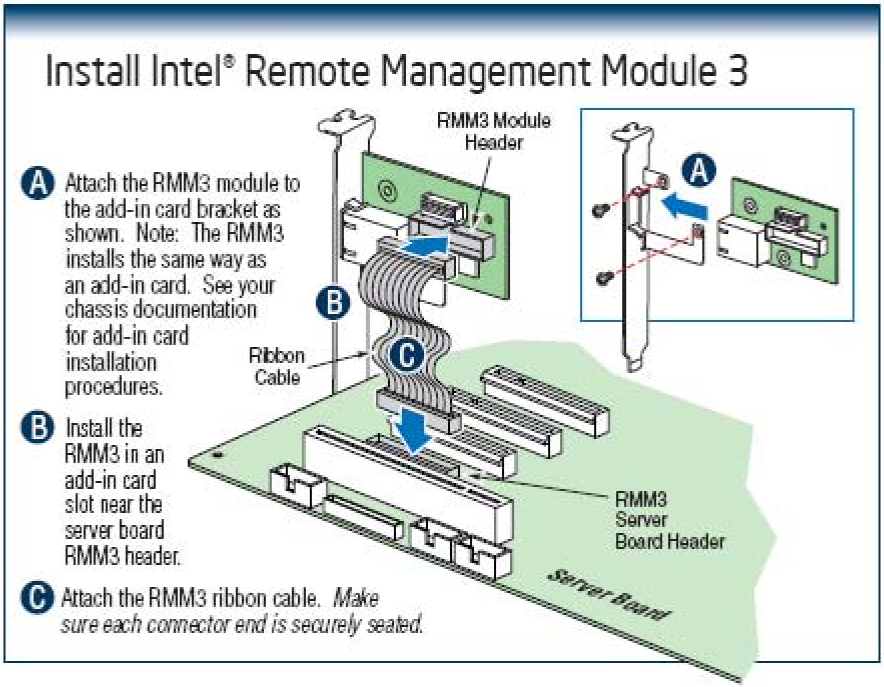

Install Intel® Remote Management Module 3
RMM3 Module Header
A Attach the RMM3 module to the add-in card bracket as shown. Note: The RMM3 installs the same way as an add-in card. See your chassis documentation for add-in card installation procedures.
B Install the RMM3 in an add-in card slot near the server board RMM3 header.
C Attach the RMM3 ribbon cable. Make sure each connector end is securely seated.
Ribbon Cable
B
C
A
RMM3 Server Board Header
Server Board

Figure 3. Installing Intel® RMM3 on Intel® Server Boards S5520HC, S5520BC, and S5520SC

2. Replace the chassis cover, attach AC power, and connect a network cable to the Intel® RMM NIC

4 Configuring Intel® RMM3

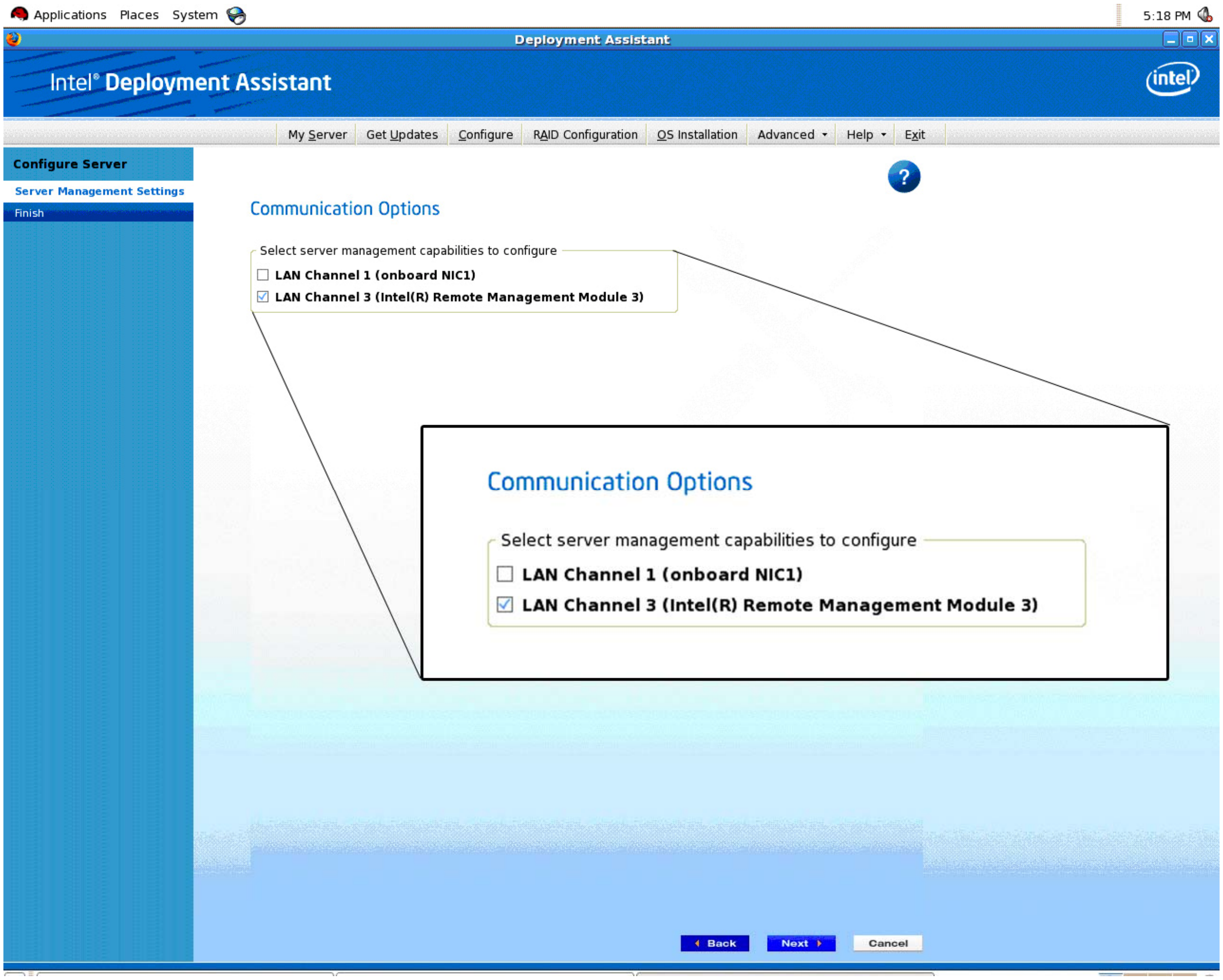
This section discusses using the server configuration utilities to enable an Intel® RMM3 from a new, unconfigured state to an operational state. When first installed, by default, the Intel® RMM3 uses a static IP address of 0.0.0.0. The Intel® RMM3 must be configured using either the syscfg utility or the Intel® Deployment Assistant (IDA) CD that is provided with your Intel® server board. Third-party IPMI-based configuration utilities can be used to configure the Intel® RMM3 for management, but support for these utilities are beyond the scope of this document.

The following two steps must be performed before Intel® RMM3 can be used:

1. Either the BMC LAN channel or the RMM3 LAN channel (or both) must be configured for management.
   a. The server board BMC LAN channel is channel 1.
   b. The RMM3 LAN channel is channel 3.
2. At least one user must be enabled to use the LAN channel(s).
   a. The Intel® RMM3 cannot use the anonymous user for RMM3 functionality, a user with both a valid user name and password are required.

The following sections explain how you can configure Intel® RMM3 using syscfg commands and Intel® Deployment Assistant.

4.1 Configuring Your Server Using Intel® Deployment Assistant (IDA)



Communication Options

Select server management capabilities to configure

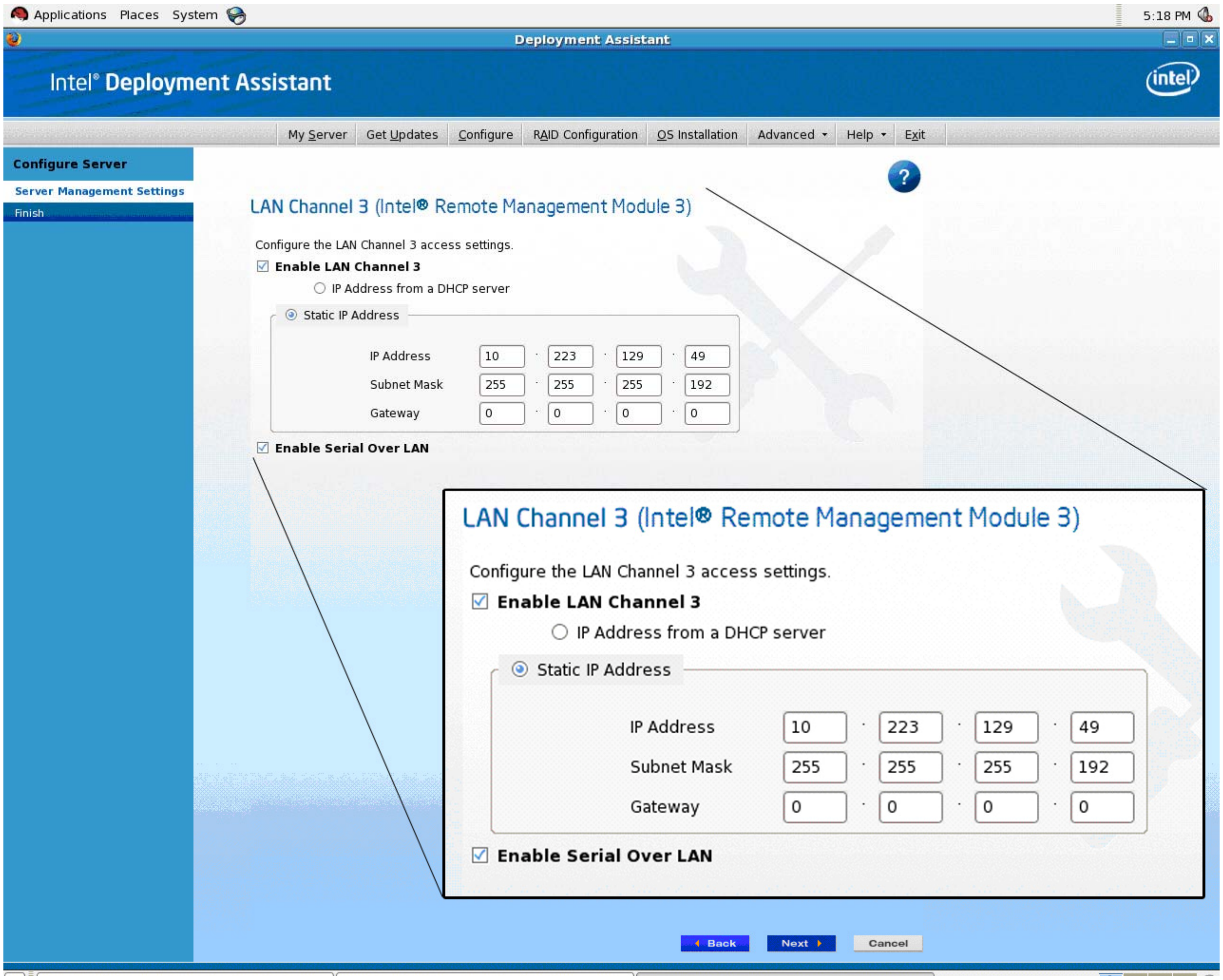
- □ LAN Channel 1 (onboard NIC1)
- ☑ LAN Channel 3 (Intel(R) Remote Management Module 3)

Communication Options

Select server management capabilities to configure

- □ LAN Channel 1 (onboard NIC1)
- ☑ LAN Channel 3 (Intel(R) Remote Management Module 3)

Figure 4. IDA Configure Server: Communication Options Window



LAN Channel 3 (Intel® Remote Management Module 3)

Configure the LAN Channel 3 access settings.

☑ Enable LAN Channel 3

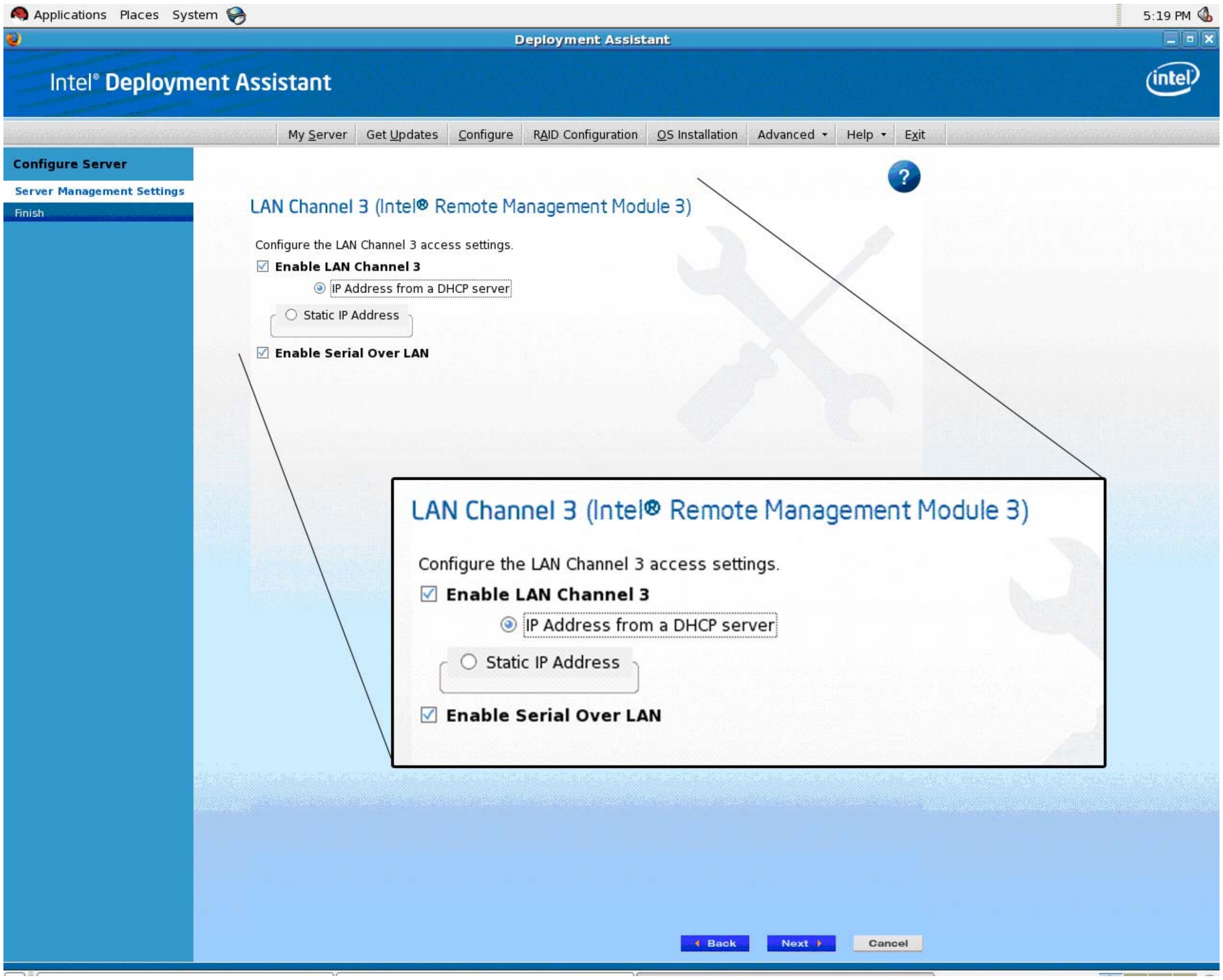
○ IP Address from a DHCP server

● Static IP Address

IP Address	10	223	129	49
Subnet Mask	255	255	255	192
Gateway	0	0	0	0

☑ Enable Serial Over LAN

Figure 5. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Settings Window 1



LAN Channel 3 (Intel® Remote Management Module 3)

Configure the LAN Channel 3 access settings.

☑ Enable LAN Channel 3

● IP Address from a DHCP server

○ Static IP Address

☑ Enable Serial Over LAN

LAN Channel 3 (Intel® Remote Management Module 3)

Configure the LAN Channel 3 access settings.

☑ Enable LAN Channel 3

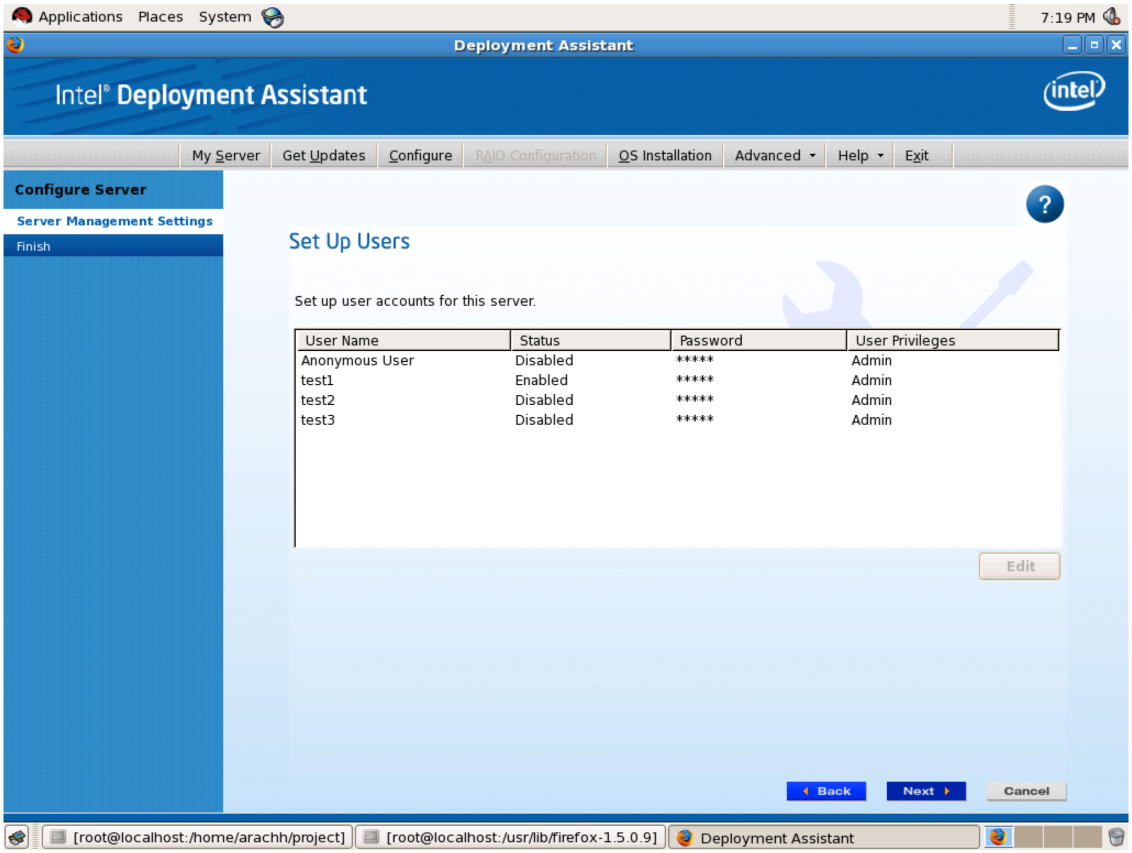
● IP Address from a DHCP server

○ Static IP Address

☑ Enable Serial Over LAN

Figure 6. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Static IP Address Window

- **WARNING**: The server board BMC LAN channel 1 and RMM3 LAN channel 3 cannot be configured for management on the same subnets. This restriction only applies to the management functionality of these NICs, not the operating system network traffic.



Set Up Users

Set up user accounts for this server.

User Name	Status	Password	User Privileges
Anonymous User	Disabled	*****	Admin
test1	Enabled	*****	Admin
test2	Disabled	*****	Admin
test3	Disabled	*****	Admin

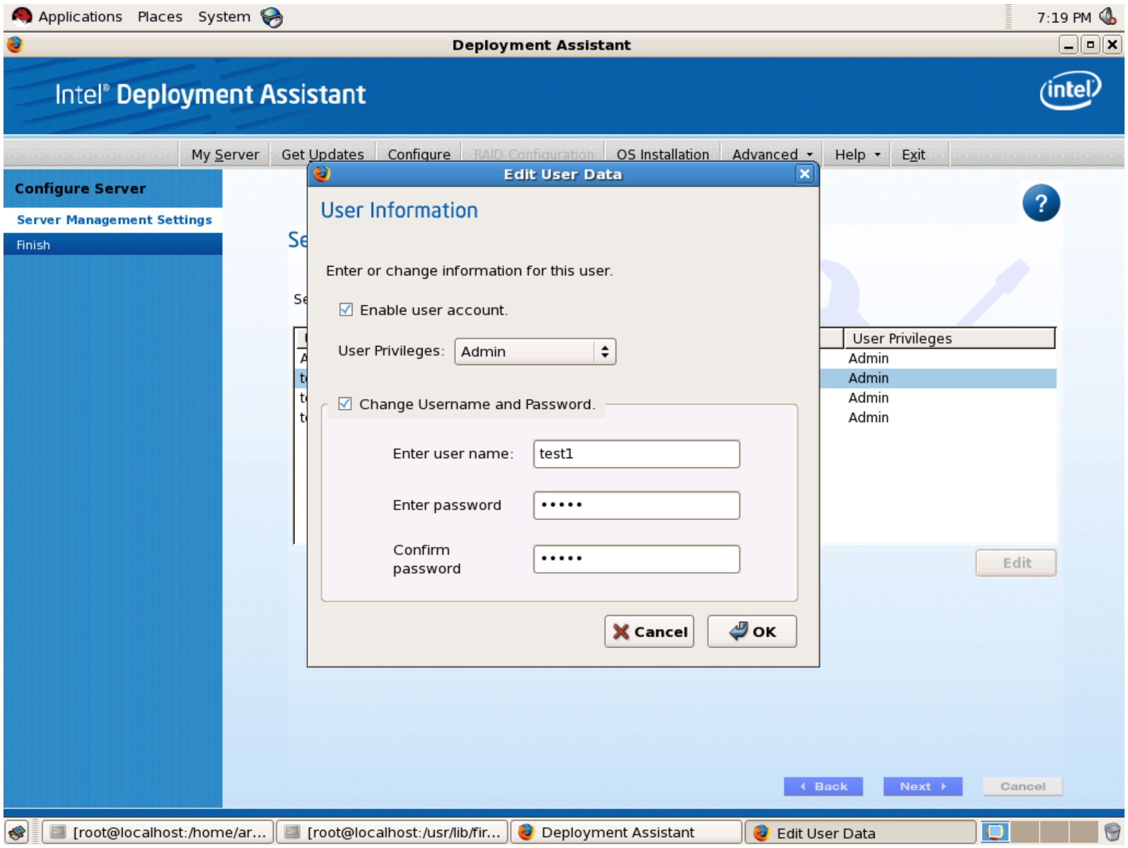
Figure 7. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Set Up Users Window

You have the option to edit user information data. Select the user and click **Edit**. The Edit User Data dialog box appears.

Notes:

- *You cannot use the anonymous user for RMM3 functionality.*
- *To connect remotely to LAN Channel 1 or 3, you need to configure users.*

Details to edit the username/passwords and set privileges for the users are provided below.



User Information

Enter or change information for this user.

☑ Enable user account.

User Privileges: Admin

☑ Change Username and Password.

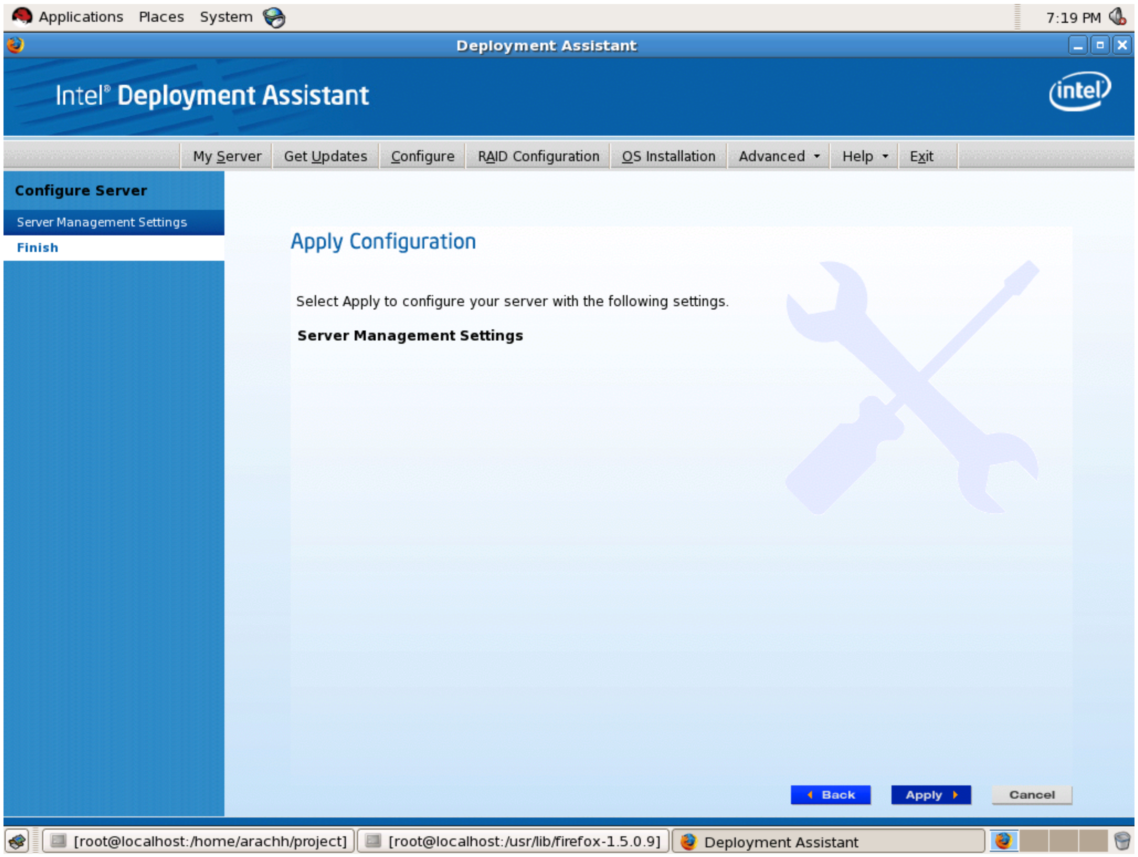
Enter user name: test1

Enter password •••••

Confirm password •••••

Figure 8. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Edit User Information Window

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

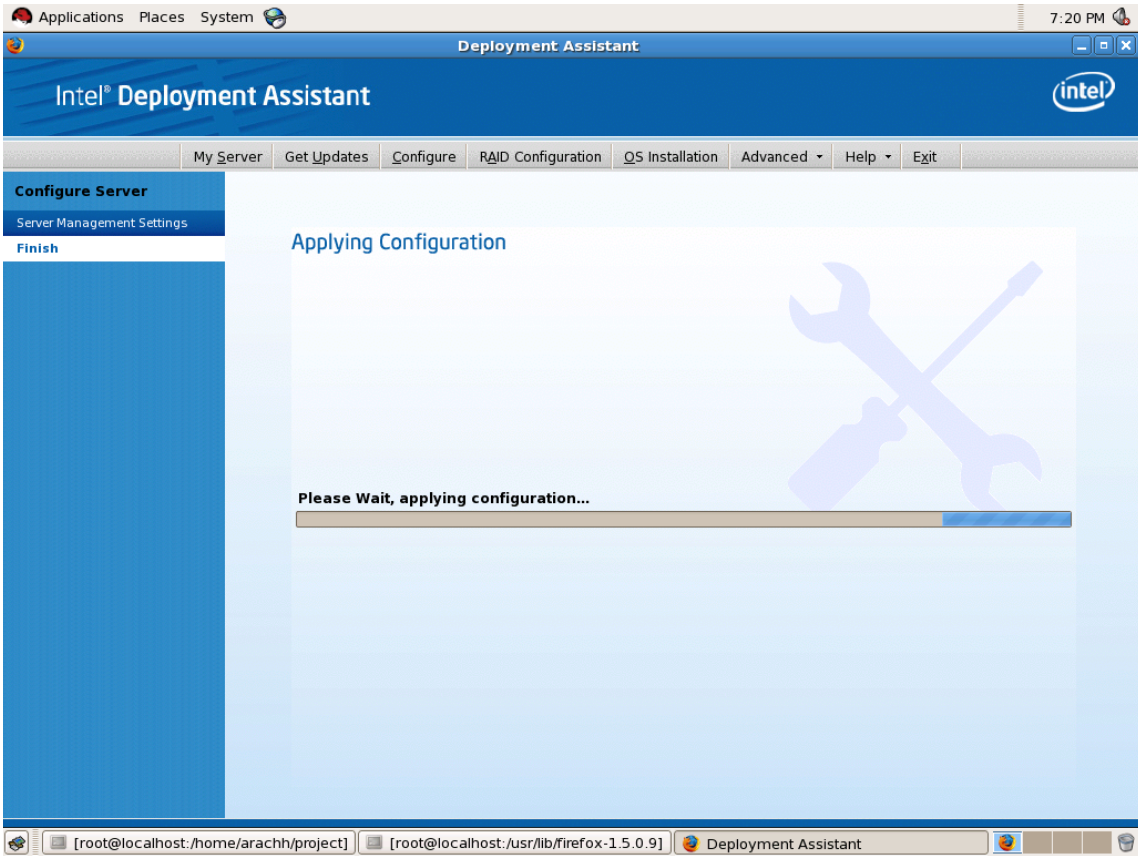


Apply Configuration

Select Apply to configure your server with the following settings.

Server Management Settings

Figure 9. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Apply Configuration Window


Applications Places System
7:20 PM
Deployment Assistant
Intel® Deployment Assistant
intel
My Server | Get Updates | Configure | RAID Configuration | OS Installation | Advanced | Help | Exit
Configure Server
Server Management Settings
Finish
[root@localhost:/home/arachh/project]
[root@localhost:/usr/lib/firefox-1.5.0.9]
Deployment Assistant

Applying Configuration

Please Wait, applying configuration...

Figure 10. IDA Configure Server: Configure LAN Channel 3 (Intel® RMM3) Applying Configuration progress Window

4.1.1 Configuring the Intel® RMM3 using syscfg commands

Syscfg is a command-line utility that can be used to save and restore BIOS and firmware settings to a file, or to set and display individual settings. Syscfg may be used in a script to automate the process of configuring multiple servers. The description of each command is available in the *Syscfg User's Guide* or using the /h or /? switch to display usage.

The general syntax is:

syscfg [{/|-}command [arguments]] [...next_command [arguments]]

There are versions of the utility that run in the EFI, Linux, Windows command prompt, and Windows Preinstallation Environment. The utility can be used to configure an individual server via the host interface, but can be used in conjunction with scripts to configure many systems at a time.

The latest syscfg software and User's Guide can be downloaded from http://downloadcenter.intel.com/default.aspx by searching for 'update & configuration utilities' for your specific server platform.

4.1.1.1 Running the Syscfg

The syscfg utility is executed from a command shell in the operating system or EFI environment. Refer to the syscfg User's Guide for operating system dependencies and more detailed usage.

The following sections detail the basic commands required for setting up an Intel® RMM3 for operation. Options enclosed in angular brackets (<>) must be provided by the user based on the desired setting for that parameter. The <CHANNEL> option can be either 1 or 3 (see the following examples)

4.1.1.2 Configuring IP address

- To set LAN channel with a static IP address:

  ```
  syscfg  -le <CHANNEL> static <STATIC_IP> <SUBNET_MASK>
  ```

  Example for channel 3:

  ```
  syscfg –le 3 static 192.168.1.100 255.255.255.0
  ```

- To set the default gateway:

  ```
  Syscfg -lc <CHANNEL> 12 <DEFAULT_GATEWAY_IP>
  ```

- To set LAN channel to obtain a dhcp IP address:

  ```
  syscfg -le <CHANNEL> dhcp
  ```

- To enable LAN channel for Serial Over LAN (SOL) (can be used for either static or DHCP):

  ```
  syscfg -sole <CHANNEL> Enable Admin <BAUD_RATE> <RETRY_COUNT>
  ```

```
<RETRY_INTERVAL_IN_MILLISECONDS>
```

4.1.1.3 Configuring the LAN channel

- To enable a specific BMC LAN channel:
  ```
  syscfg /c <CHANNEL> 7 Always
  ```

  Example for channel 3:

  ```
  syscfg /c 3 7 always
  ```

4.1.1.4 Configuring Users

- To set the password for a BMC user:

  ```
  syscfg /u <USER#> <username> <password>
  ```

  Example for user number 3:

  ```
  syscfg /u 3 “root” “password1”
  ```
- To enable a BMC user to use a BMC channel:

  ```
  syscfg /ue <USER#> enable <CHANNEL>
  ```
- To enable “admin” privilege and payload type to “SOL” for the BMC user 3 on BMC channel 1, type:

  ```
  syscfg /up <USER#> <CHANNEL> admin  sol
  ```

4.1.1.5 Obtaining the assigned DHCP address

The syscfg utility can display the assigned IP address if DHCP is used. After waiting for a short time for the DHCP server to assign a new address to the BMC, execute the following command:

```
syscfg /d lan <CHANNEL>
```

5 Getting Started with Intel® RMM3 Operation

This section describes how to get started on the Intel® RMM3 operation. It also explains how to log into the advanced features of the module, navigate the options available, and how to log out.

5.1 Before You Begin

The Intel® RMM3 module 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.

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

HTTP/HTTPS: Full access is provided by the embedded web server. You can access the Intel® RMM3 module using the HTTP protocol or using the encrypted HTTPS protocol.
Note: Intel recommends that you use HTTPS to enable data encryption of the kVM session.

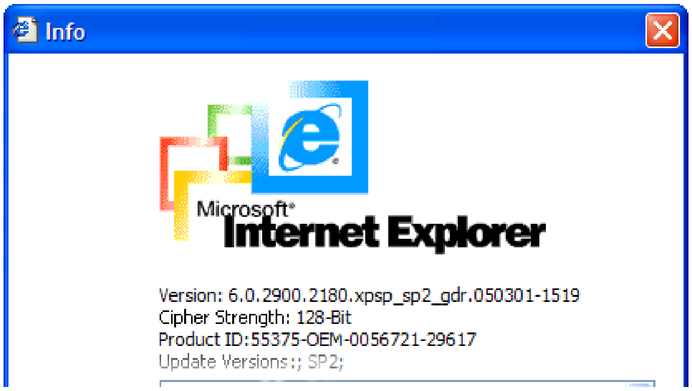
Java Runtime Environment (JRE) 1.6 or later must be installed on the management system used to connect to the Intel® RMM3 via the web browser.

5.1.1 Browsers

In order to access the web console using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using 128-bit Cipher Strength (encryption). 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.

The following figure displays the dialog box presented by Microsoft Internet Explorer* 6.0.



Version: 6.0.2900.2180.xpsp_sp2_gdr.050301-1519
Cipher Strength: 128-Bit
Product ID:55375-OEM-0056721-29617
Update Versions:; SP2;

Figure 11. 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

To log in to the Intel® RMM3 module, follow these steps:

4. Enter the configured IP address of the Intel® RMM3 add-on card into your web browser.

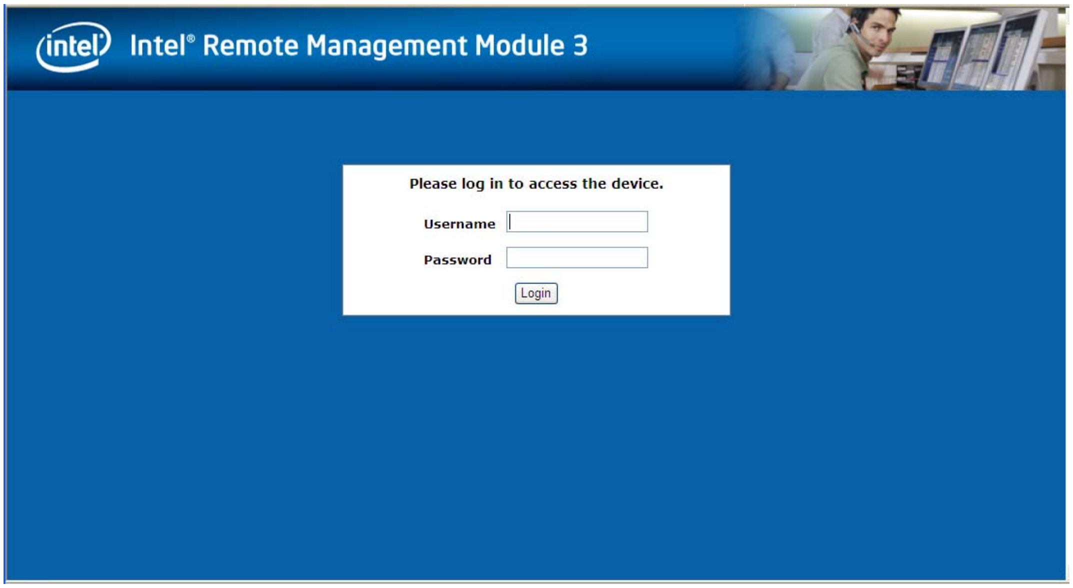
   For example:

   http://10.223.131.36/

   In order to use a secure connection, type in as shown in the following example:

   https://10.223.131.36/

   This will take you to the Intel® RMM3 module login page as shown in Figure 12.



Please log in to access the device.

Figure 12. Intel® RMM3 Login Page

5. Enter the username and password to log in.

   For example:

   - Username = root
   - Password = superuser

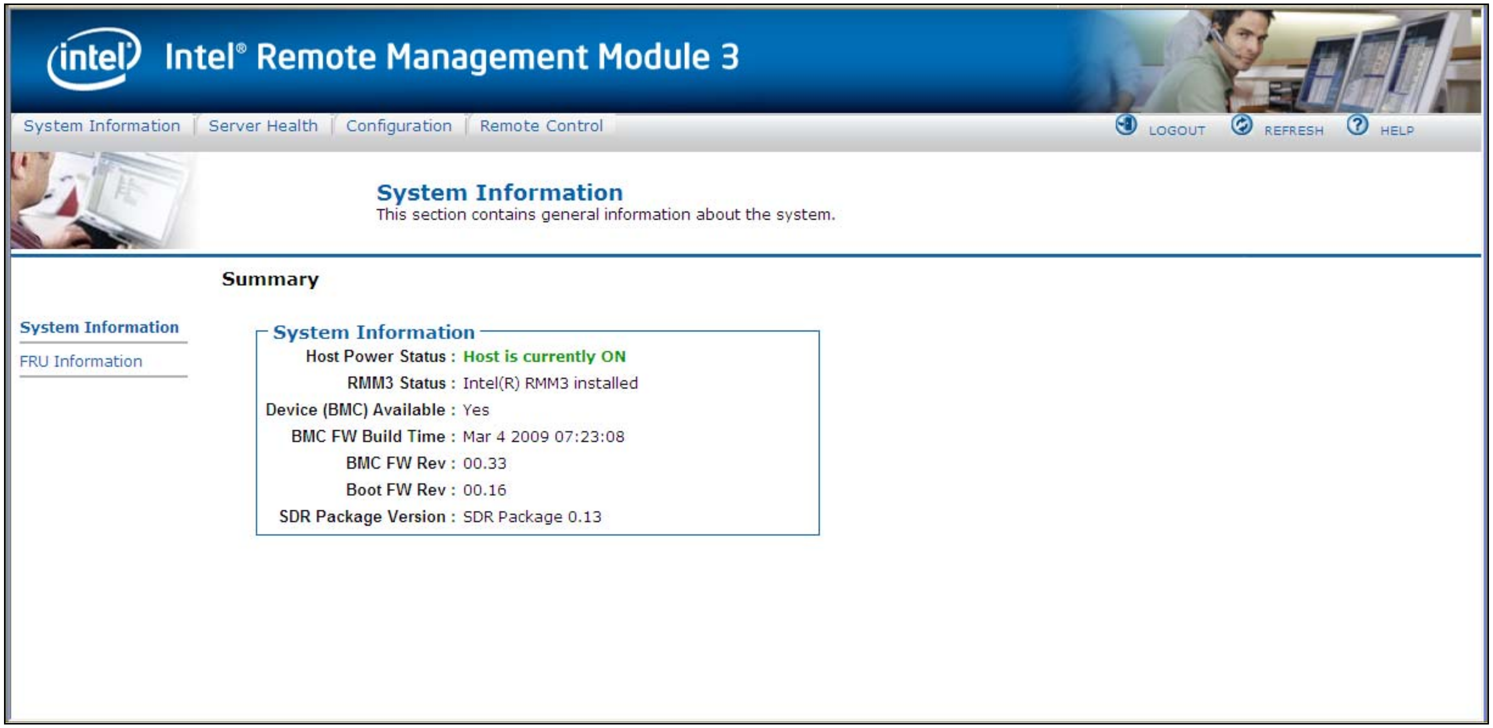
   Note: The Username and Password are case sensitive. Any username and password can be used (except anonymous).

6. Click the **Login** button to view the RMM3 home page as shown in Figure 13.

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

5.3 Navigation

After successful login to the Intel® RMM3 module, the Intel® RMM3 home page appears as shown in Figure 13:



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 :	Mar 4 2009 07:23:08
BMC FW Rev :	00.33
Boot FW Rev :	00.16
SDR Package Version :	SDR Package 0.13

Figure 13. 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 identified in the following table:

Tab	Function
System Information	Click this tab to access general information about the server. The 'System Information' page automatically opens. In general, this tab provides access to the following: • System information • FRU information
Server Health	Click this tab for access to the sensors and event log. The 'Sensor Readings' page automatically opens. In general, this tab provides access to the following: • Sensor readings • Event log
Configuration	Click this tab to configure various settings for the server. The 'Network' configuration page automatically opens. In general, this tab provides access to the following: • Network • Users • LDAP • SSL • Remote Session • Mouse Mode
Remote Control	Click this tab for access to the remote console and to control the power state of the server. In general, this tab provides access to the following: • Console Redirection • Server Power Control

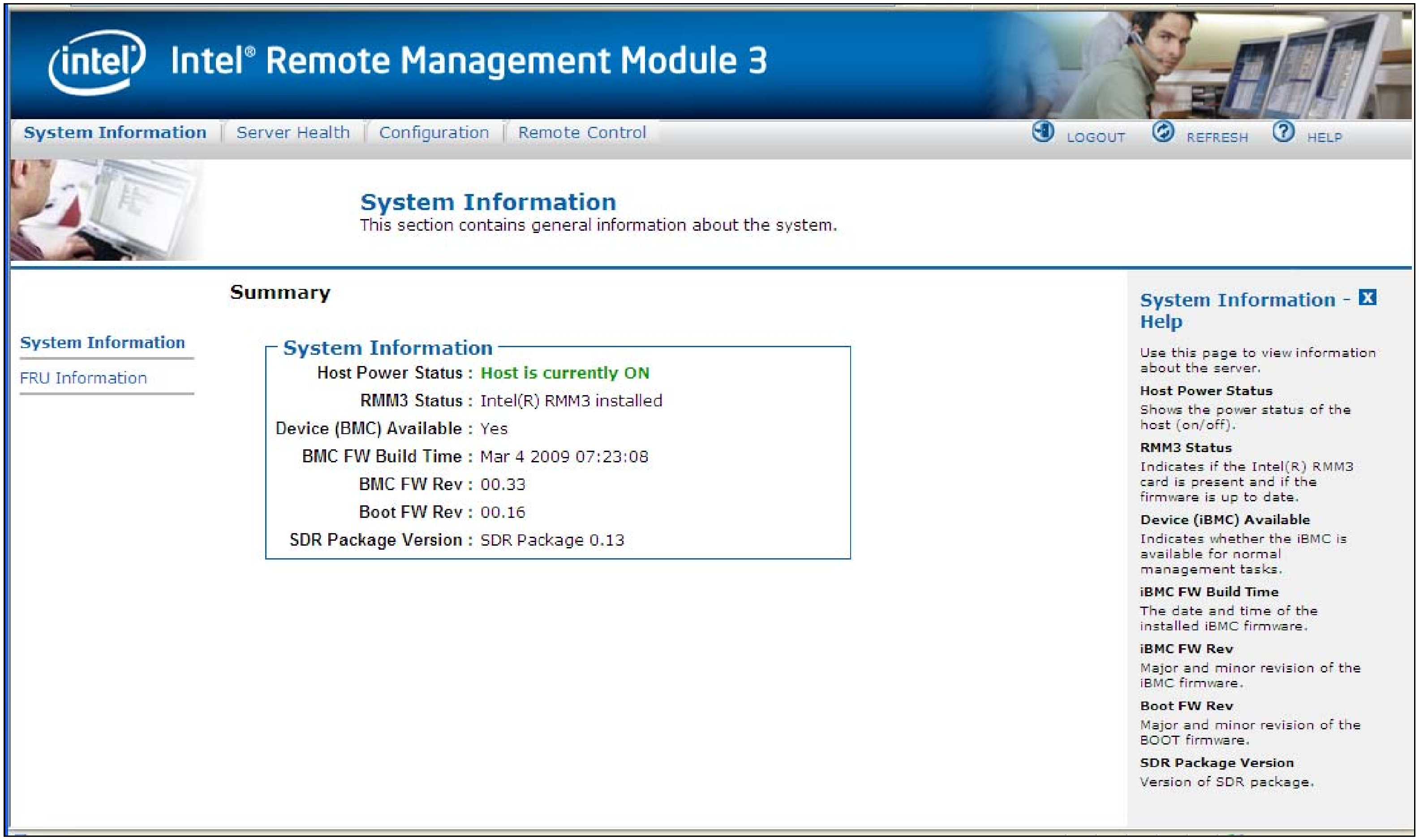
The four tabs on the horizontal menu allow you to navigate within the Intel® RMM3 Web Console. Each of these tabs contains a secondary menu on the left edge of the browser window. For detailed information on the specific functionality of the secondary menu items, see Chapter 7: Intel® RMM3 Web Console Options.

The top horizontal toolbar consists of the Logout, Refresh, and Help buttons. Click these buttons to perform tasks as desribed in the following table.

Button	Function
	Click this button to end the current Web Console session. Note that a remote console (KVM) window, if active, is closed when you log out. After logging out, the Web Console returns to the Login screen.
	Click this button to refresh the current web page, including any data shown on the page.
	Click this button to view a brief description of the current page in a frame at the right-hand side of the browser window. Close the Help frame by clicking the 'X' in the upper right corner of the frame or by clicking the HELP button again.

5.4 Online Help

The Web Console user interface gives specific online help for each page. For additional information on a certain topic or group of options, click the ? HELP button on the top horizontal toolbar to view the online help as shown in Figure 14. The right Help panel is visible only when the online Help is being accessed.



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 :	Mar 4 2009 07:23:08
BMC FW Rev :	00.33
Boot FW Rev :	00.16
SDR Package Version :	SDR Package 0.13

System Information - Help

Use this page to view information about the server.

Host Power Status

Shows the power status of the host (on/off).

RMM3 Status

Indicates if the Intel(R) RMM3 card is present and if the firmware is up to date.

Device (iBMC) Available

Indicates whether the iBMC is available for normal management tasks.

iBMC FW Build Time

The date and time of the installed iBMC firmware.

iBMC FW Rev

Major and minor revision of the iBMC firmware.

Boot FW Rev

Major and minor revision of the BOOT firmware.

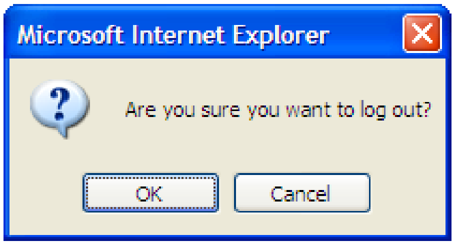
SDR Package Version

Version of SDR package.

Figure 14. Launching the Online Help

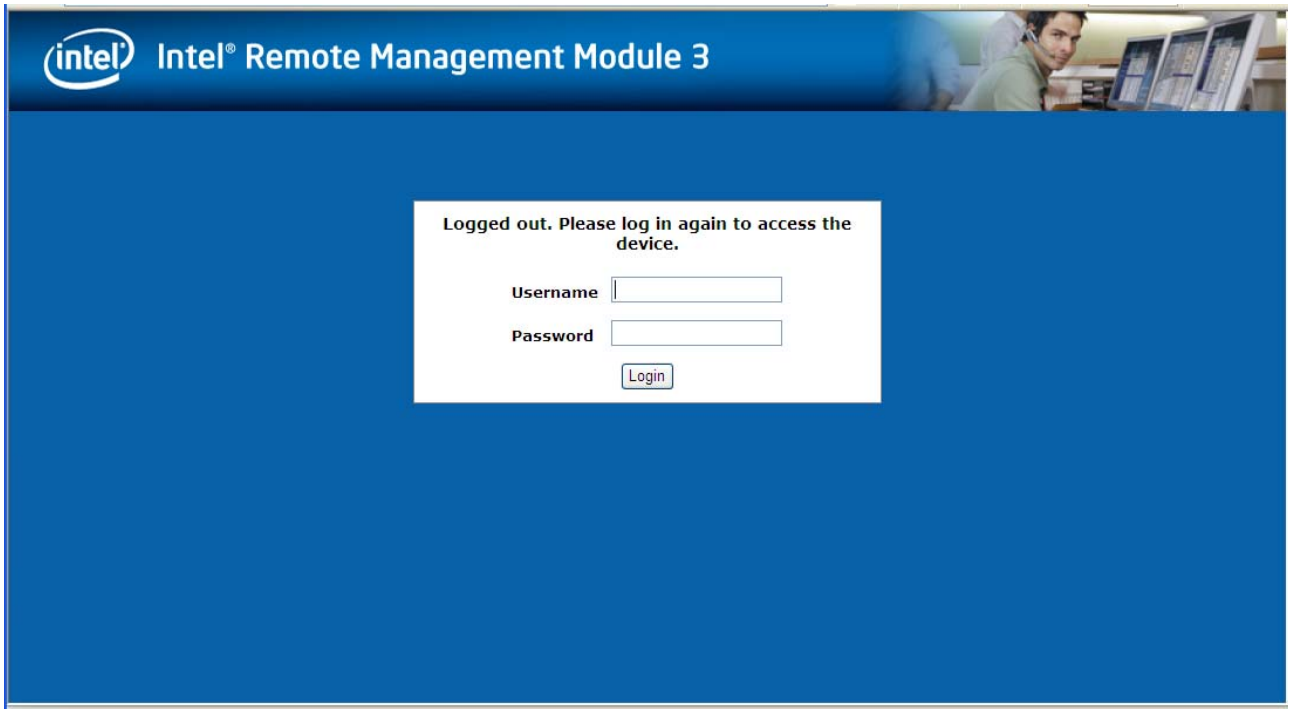
5.5 Logging Out of Intel® RMM3

Click the LOGOUT button to log out the current user and revert to a new login screen as shown in Figure 15 and Figure 16.



Are you sure you want to log out?

Figure 15. Logging Out of Intel® RMM3 – Step 1



Logged out. Please log in again to access the device.

Username

Password

Figure 16. Logging Out of Intel® RMM3 – Step 2

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

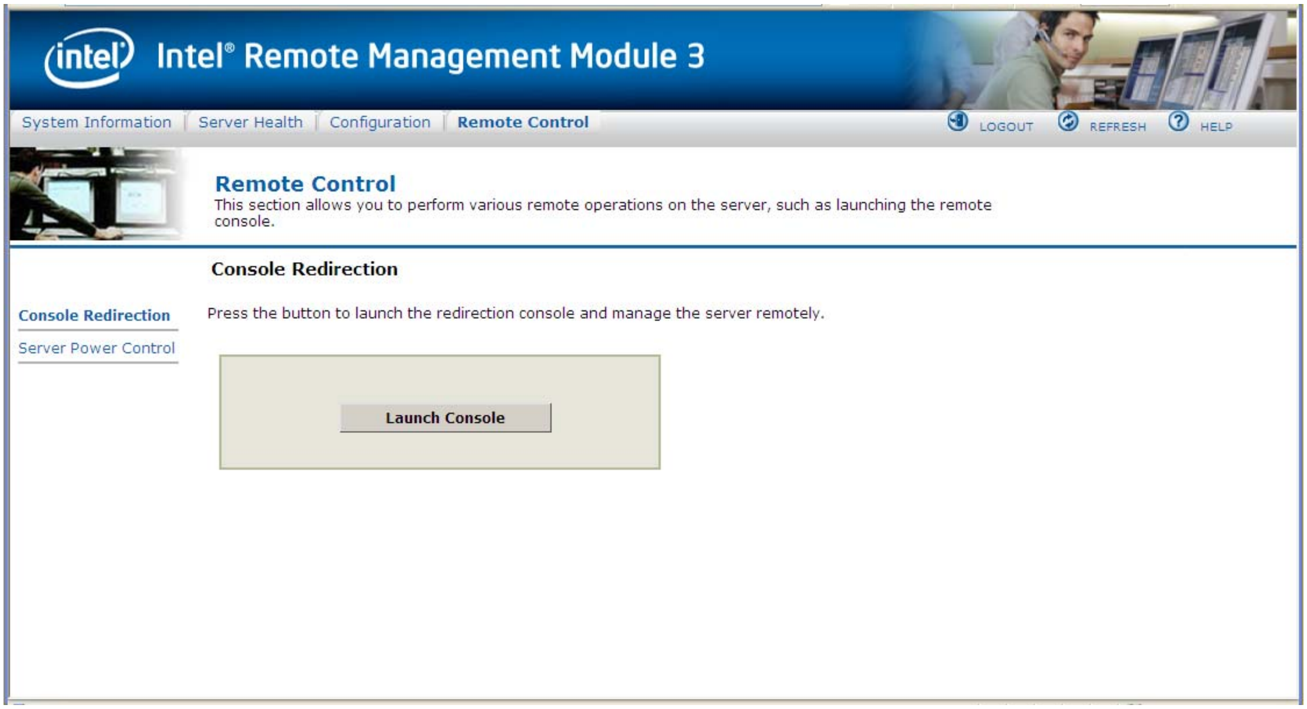
6 Remote Console (KVM) Operation

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.

When the Remote Console is launched, a new window opens to display the screen content of the host system. The Remote Console acts as if the administrator is 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.



Remote Control

This section allows you to perform various remote operations on the server, such as launching the remote console.

Console Redirection

Press the button to launch the redirection console and manage the server remotely.

Figure 17. Remote Control> Console Redirection window

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

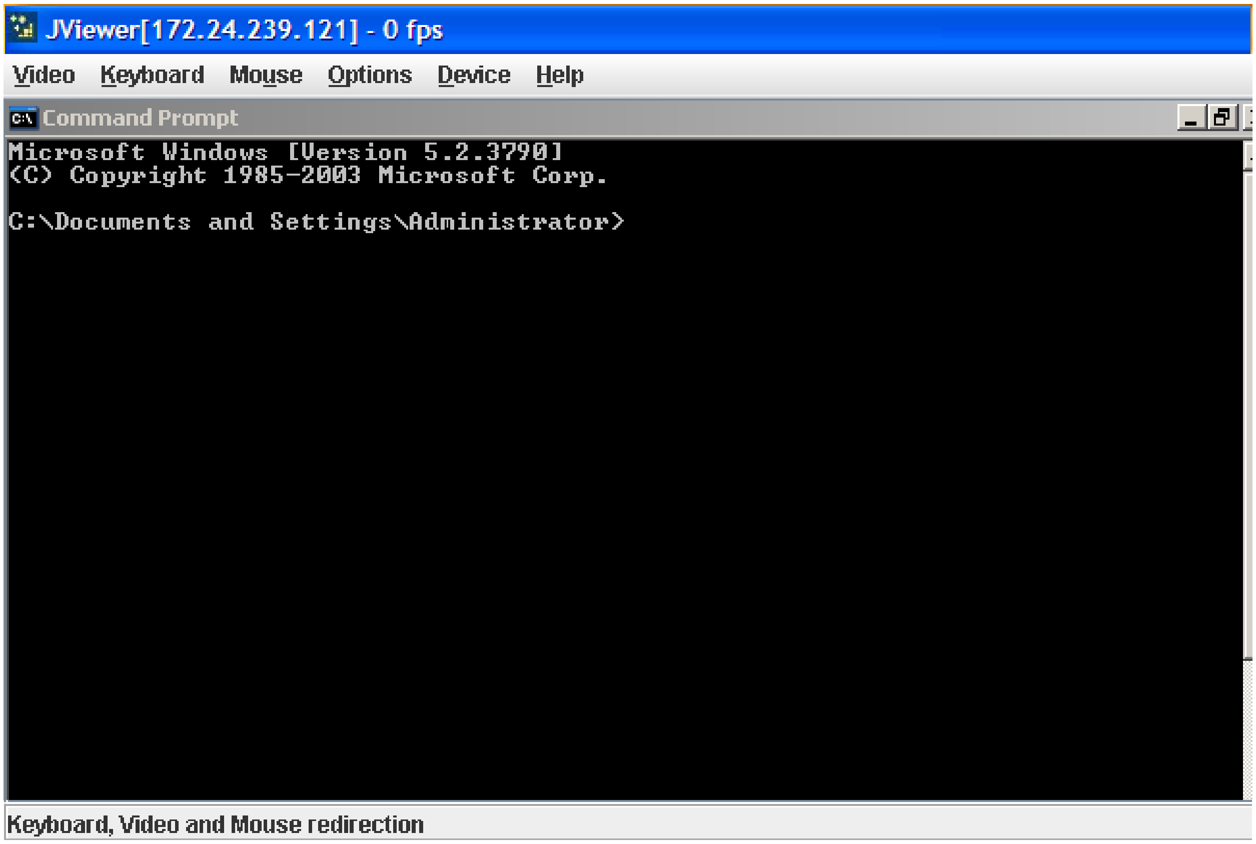
When the Launch Console button is clicked, a pop-up window appears to download the Java

Network Launch Protocol jviewer.jnlp file. This in turn downloads the standalone Java application implementing the Remote Console.

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

Notes:

- Java Runtime Environment (JRE) version 6, update 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.


JViewer[172.24.239.121] - 0 fps
Video
Keyboard
Mouse
Options
Device
Help
Command Prompt
Keyboard, Video and Mouse redirection

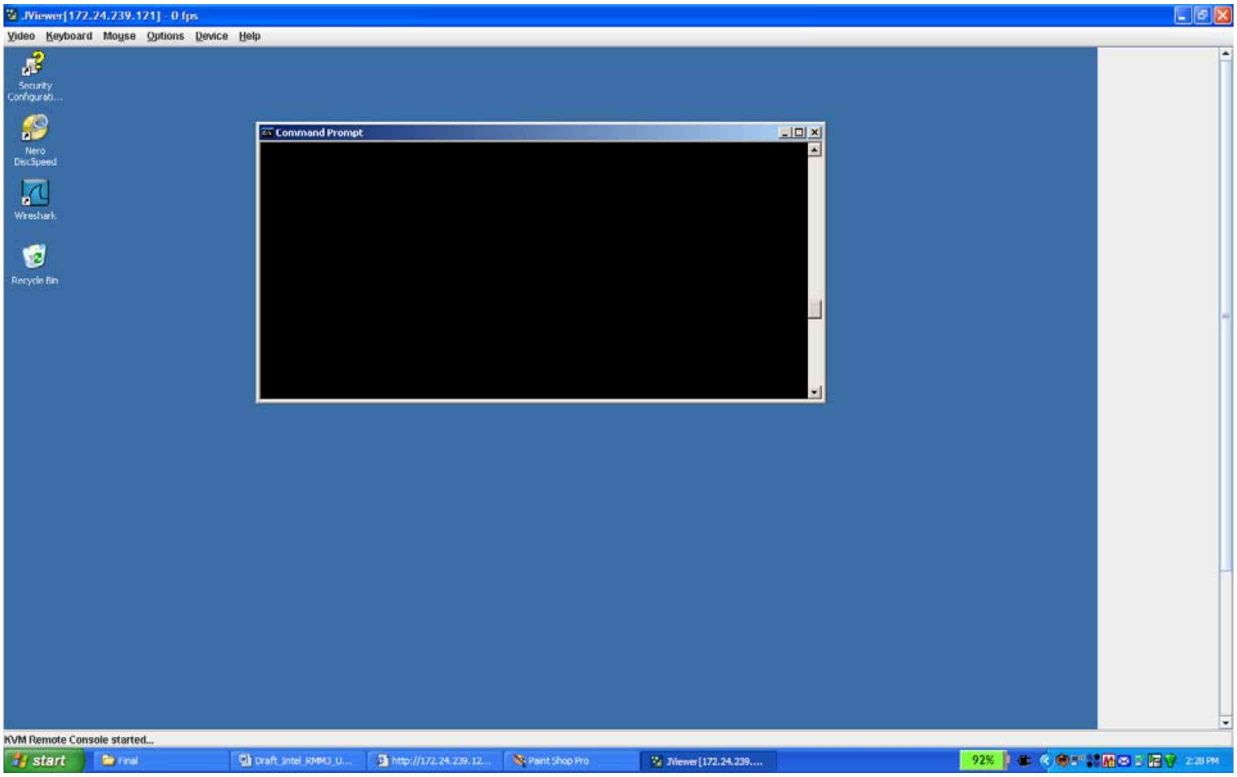
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>
```

Figure 18. Remote Console

The Remote Console window is a Java Applet that establishes TCP connections to the Intel® RMM3 module. The protocol that runs over these connections is a unique KVM protocol and not HTTP or HTTPS. This protocol uses ports #7578 for KVM, #5120 for CD-ROM 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, if you have a private internal network, your NAT (Network Address Translation) settings must be configured accordingly.

6.2 Main Window

When the Remote Console is launched, an additional window appears as shown in the following figure.



KVM Remote Console started...

Figure 19. Remote Console Main Window

It displays the screen content of your remote server. The Remote Console behaves as if you were located at the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between the Intel® RMM3 module and Remote Console. Enabling KVM and/or media encryption on the Configuration > Remote Session web page degrades performance as well.

The Remote Console window always tries to show the remote screen with its optimal size. That 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 system as usual.

6.3 Remote Console Menu Bar

The upper part of the Remote Console window contains a menu bar. You can use the items on the menu bar to view the status of the Remote Console and configure the local Remote Console settings.

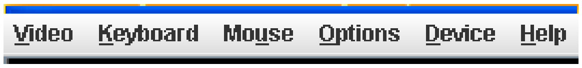


Figure 20. Remote Console Control Bar

The following sections describe each control.

6.3.1 Remote Console Video Menu

Click **Video** in the Remote Console control bar to open the Remote console Video menu as shown in the following figure.

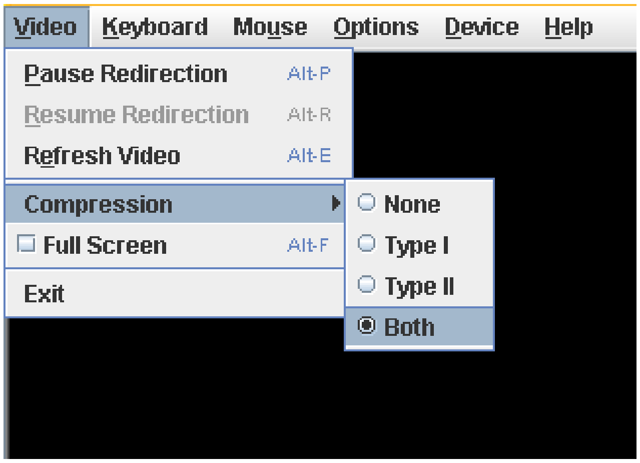


Figure 21. Remote Console Video Menu

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. Keyboard shortcut is ALT+R.
- **Refresh Video:** Refreshes the Remote Console window. Keyboard 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 between window and full screen mode for the Remote Console. Shortcut is ALT+F.
- **Exit:** Closes the Remote Console.

6.3.2 Remote Console Keyboard Menu

Click **Keyboard** to open the Keyboard menu with options to perform tasks as shown in the following figure.

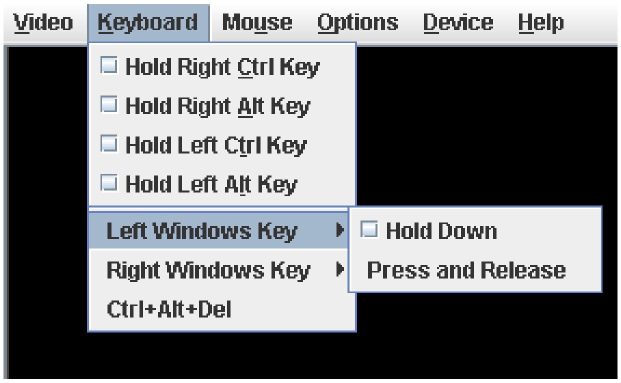


Figure 22. Remote Console Keyboard Menu

Using this menu, you can do the following:

- **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:** Issues a Ctrl+Alt+Del to the remote OS.

6.3.3 Remote Console Mouse Menu

Click **Mouse** to open the Mouse menu with options to perform tasks as shown in the following figure.

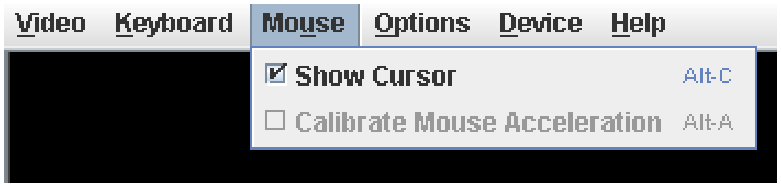


Figure 23. Remote Console Mouse Menu

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. The keyboard shortcut is ALT+C.

- **Calibrate Mouse Acceleration**: This option is used to detect the acceleration settings on the remote system and set the local client's acceleration setting accordingly. It only applies when in the Relative Mouse Mode, selected on the Configuration > Mouse Mode web page. Absolute Mouse Mode does not require calibration. The keyboard shortcut is ALT+A.

For Relative mouse mode operation, the following is the mechanism to synchronize the mouse settings.

6.3.3.1 Mouse Acceleration Calibration

1. If the remote mouse and local mouse cursor are not in sync, start mouse acceleration calibration by selecting the 'Calibrate Mouse Acceleration' menu item or by pressing <ALT+A>.

   Once started, you will see two mouse cursors moving diagonally across the screen (starting at 0, 0 location). The local mouse cursor is displayed in RED color to differentiate between the two mouse cursors.

   Depending upon the difference in acceleration settings on both ends, mouse cursors may eventually go out of sync.
2. Press '+' or '-' key to change the acceleration settings.

   If the local mouse cursor is lagging behind the host cursor, press '+' to try to be in sync. If the local cursor is moving ahead of the host cursor, press '-' to sync it up.

   Adjust the sync using '+' or '-' until you achieve the maximum sync possible. A good indicator of that setting is that the mouse movement switches from lagging to leading or vice-versa when the most optimal value is crossed.
3. To ensure that both cursors are in sync, wait until they reach the bottom of the screen and are still in sync.
4. Once in sync, press <ALT+A> to stop acceleration calibration and save the current acceleration settings.
5. When acceleration sync is done, start mouse threshold calibration by selecting the 'Calibrate Mouse Threshold' menu item or by pressing <ALT+T>.

   The behavior is same as in mouse acceleration case. Once started, you will see two mouse cursors moving diagonally across the screen (starting at 0, 0 location). The local mouse cursor is displayed in RED color to differentiate between the two mouse cursors.

   Depending upon the difference in threshold settings on both ends, mouse cursors may eventually go out of sync.
6. Press '+' or '-' key to change the threshold settings.

   If the local mouse cursor is lagging behind the host cursor, press '+' to try to be in sync. If the local cursor is moving ahead of the host cursor, press '-' to sync it up.

   Adjust the sync using '+' or '-', until you achieve the maximum sync possible. A good indicator of that setting is that the mouse movement switches from lagging to leading or vice-versa when the most optimal value is crossed.
7. To ensure that both cursors are in sync, wait until they reach the bottom of the screen and are still in sync.
8. Once in sync, press <ALT+T> to stop threshold calibration and save the current threshold settings.

   At this point, both local and the remote mouse cursors should be in synchronization. **NOTE:** Once the acceleration calibration is preformed, you must calibrate threshold settings for the mouse to be in sync.

6.3.4 Remote Console Options Menu

Click **Options** to open the menu with options to perform tasks as shown in the following figure.

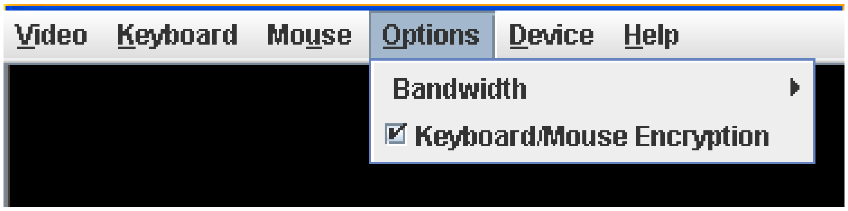


Figure 24. Remote Console Options Menu

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

Click **Device** to open the Device menu with options to perform tasks as shown in the following figure.

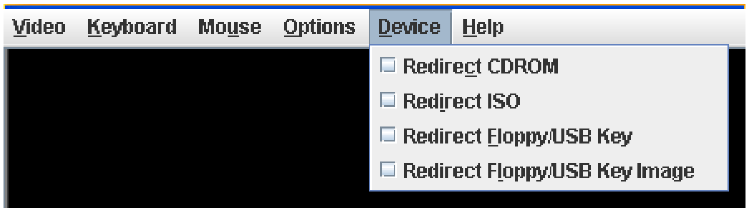


Figure 25. Remote Console Device Menu

This menu option allows starting/stopping remote media redirection.

- **Redirect CDROM / Redirect ISO:** Allows you to redirect either a local CD-ROM/DVD drive or an ISO image on your local client file system as a virtual CD-ROM device on the remote system.
- **Redirect Floppy/USB Key / Redirect Floppy/USB Key Image:** Allows 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.

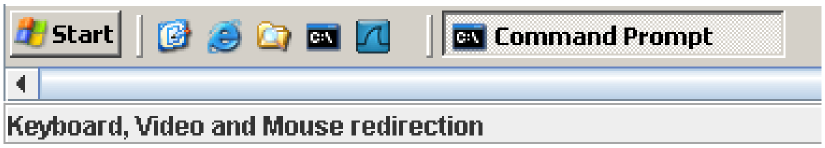
The virtual devices act just like any other CD-ROM or floppy on the remote system. They can be read, written (assuming they are not read-only), and booted. The pair of virtual devices only appear on the remote OS or BIOS setup menus when some media redirection is active. The virtual devices persist across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

Note that the virtual devices are not limited to normal floppy/CD-ROM sizes and can 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 CD-ROM 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 displays the console state as shown in the following figure. As you navigate the menu options, the status line gives a more detailed definition for each option.



Keyboard, Video and Mouse redirection

Figure 26. 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 on the horizontal menu. Within each section, each menu choice from the left-hand menu is illustrated and described in detail.

Notes:

- The first menu item for each tab is the default page which appears when the tab is selected.
- Similar information about each page is available in the Web Console by clicking the HELP button at the right side of the horizontal menu.
- When the Web Console is working on current user request, a busy indicator bar appears as shown in Figure 27.

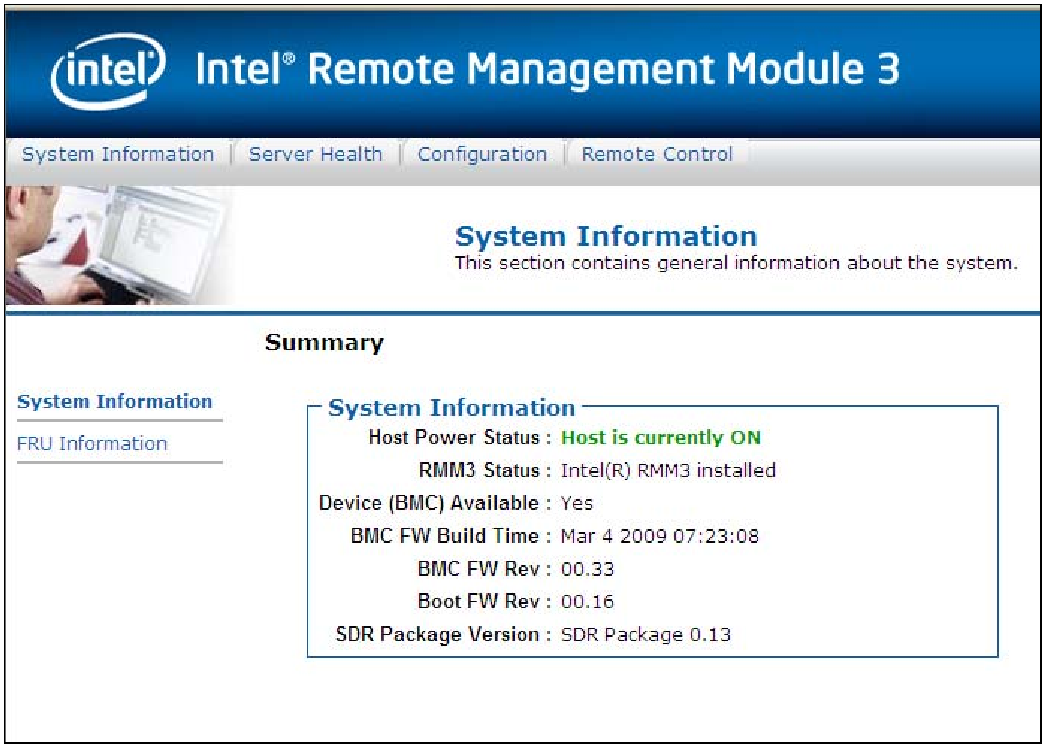
Figure 27. Busy Indicator Bar

7.1 System Information

By default, the Intel® RMM3 home page displays the System Information page. It contains general information about the system as explained in the following subsections.

7.1.1 Viewing System Information

The System information page displays a summary of the general system information as shown in Figure 28.



Host Power Status : Host is currently ON
RMM3 Status : Intel(R) RMM3 installed
Device (BMC) Available : Yes
BMC FW Build Time : Mar 4 2009 07:23:08
BMC FW Rev : 00.33
Boot FW Rev : 00.16
SDR Package Version : SDR Package 0.13

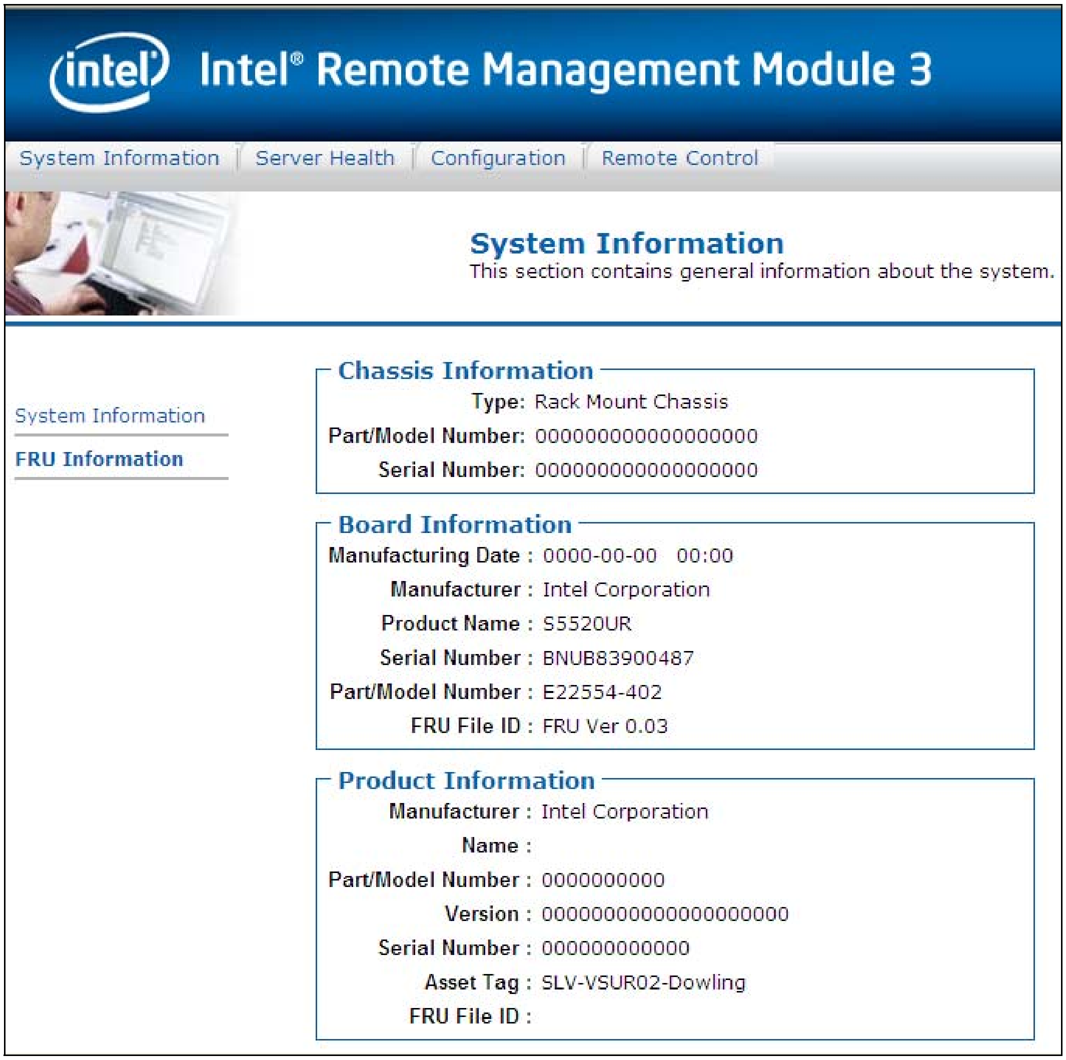
Figure 28. System Information page

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

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.
SDR Package Version	Displays the version of the SDR package loaded in the system.

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 as shown in Figure 29.



System Information

This section contains general information about the system.

Chassis Information

Type: Rack Mount Chassis

Part/Model Number: 000000000000000000

Serial Number: 000000000000000000

Board Information

Manufacturing Date : 0000-00-00 00:00

Manufacturer : Intel Corporation

Product Name : S5520UR

Serial Number : BNUB83900487

Part/Model Number : E22554-402

FRU File ID : FRU Ver 0.03

Product Information

Manufacturer : Intel Corporation

Name :

Part/Model Number : 0000000000

Version : 00000000000000000000

Serial Number : 000000000000

Asset Tag : SLV-VSUR02-Dowling

FRU File ID :

Figure 29. System Information > FRU Information page

The FRU Information page has the following BMC FRU file data:

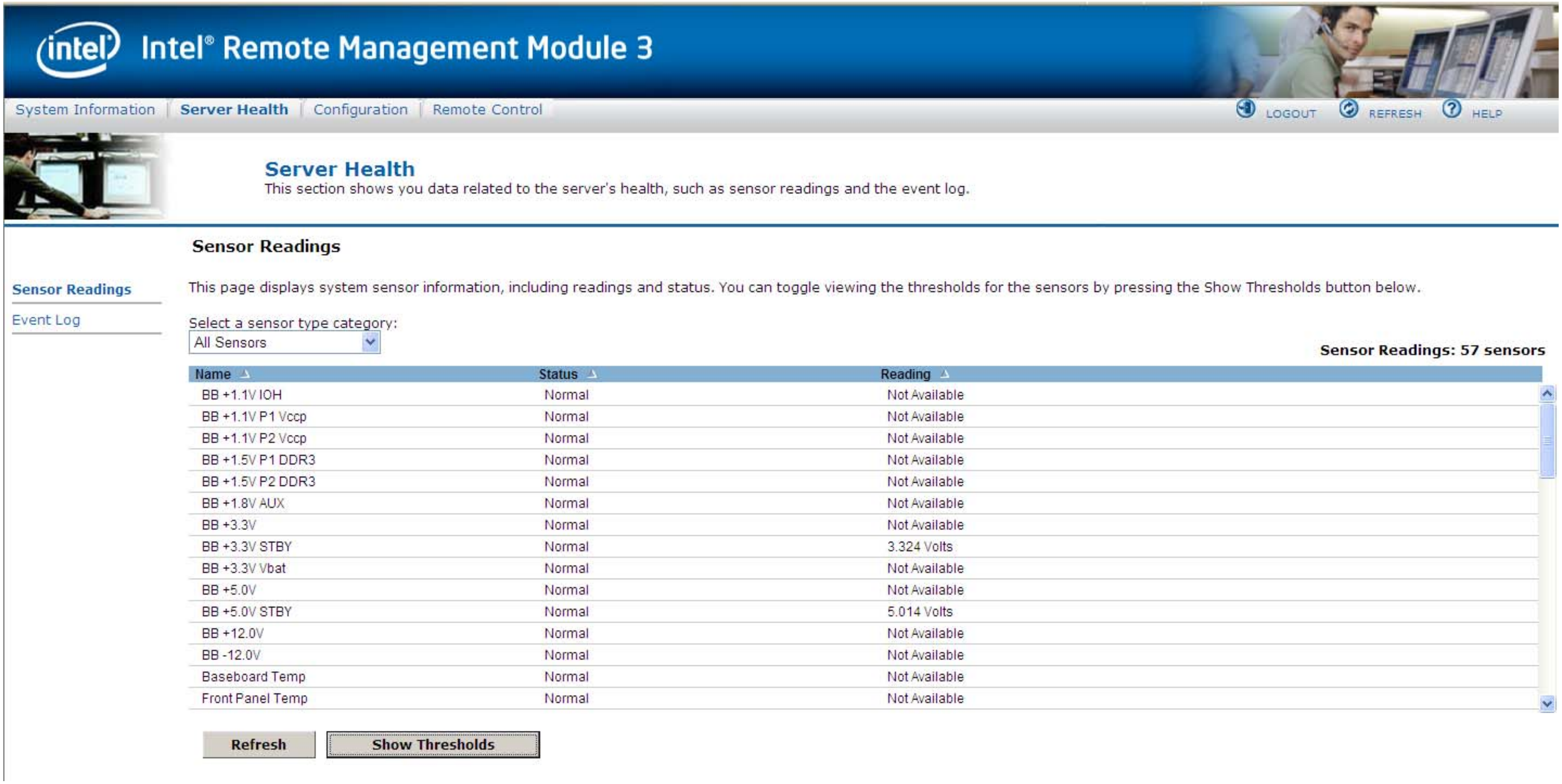
Information	Details
FRU Chassis Information	Shows the following: • Type • Part/Model Number • Serial Number.
FRU Board Information	Shows the following: • Manufacturing Date • Manufacturer • Product Name • Serial Number • Part/Model Number • FRU File ID
FRU Product Information	Shows the following: • Manufacturer • Name • Part/Model Number • Version, Serial Number • Asset Tag • FRU File ID

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 31.

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

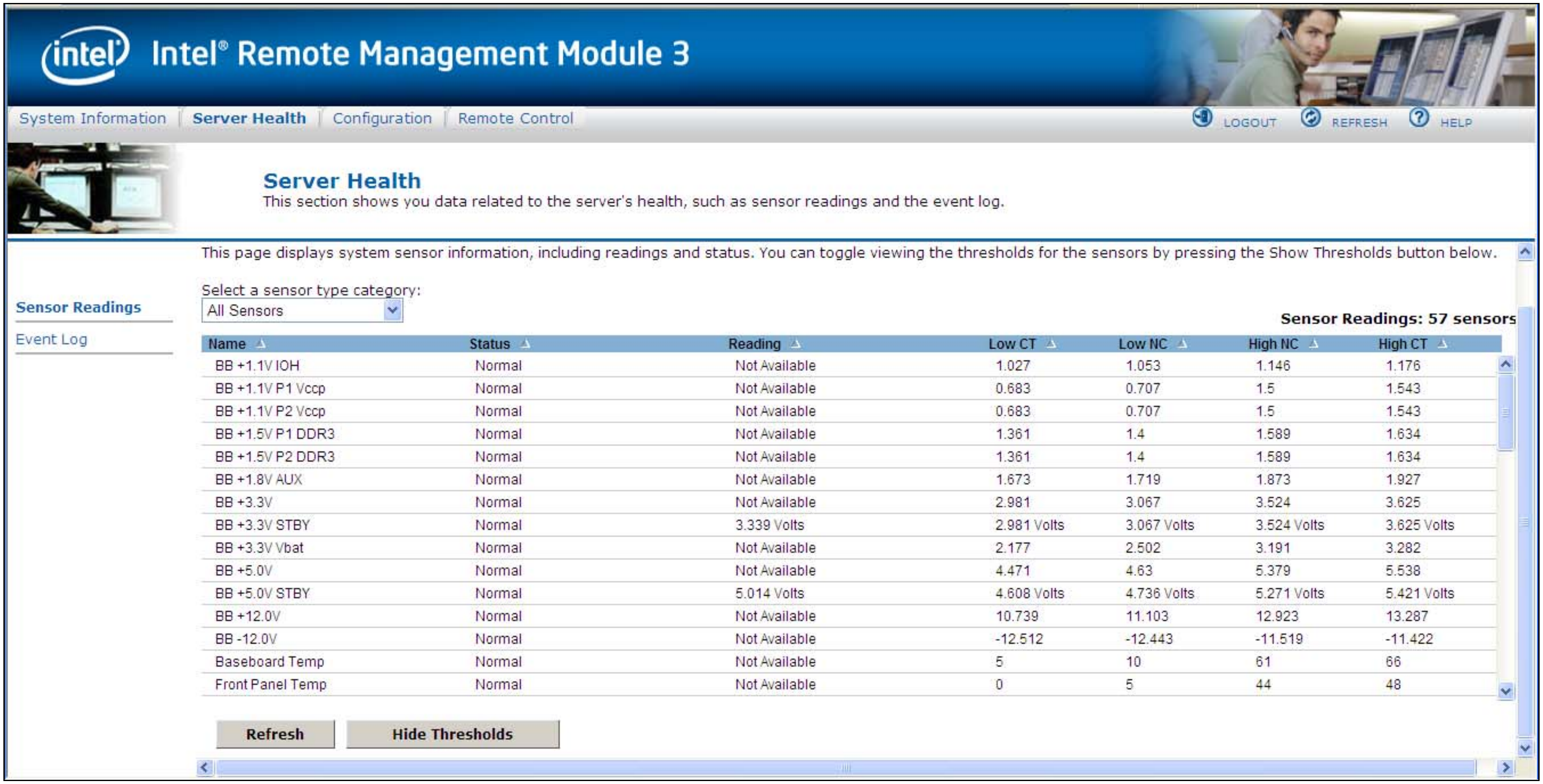
This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.

Select a sensor type category: All Sensors

Sensor Readings: 57 sensors

Name	Status	Reading
BB +1.1V IOH	Normal	Not Available
BB +1.1V P1 Vccp	Normal	Not Available
BB +1.1V P2 Vccp	Normal	Not Available
BB +1.5V P1 DDR3	Normal	Not Available
BB +1.5V P2 DDR3	Normal	Not Available
BB +1.8V AUX	Normal	Not Available
BB +3.3V	Normal	Not Available
BB +3.3V STBY	Normal	3.324 Volts
BB +3.3V Vbat	Normal	Not Available
BB +5.0V	Normal	Not Available
BB +5.0V STBY	Normal	5.014 Volts
BB +12.0V	Normal	Not Available
BB -12.0V	Normal	Not Available
Baseboard Temp	Normal	Not Available
Front Panel Temp	Normal	Not Available

Figure 30. Server Health > Sensor Readings window (Thresholds not displayed)



Server Health

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

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: 57 sensors

Name	Status	Reading	Low CT	Low NC	High NC	High CT
BB +1.1V IOH	Normal	Not Available	1.027	1.053	1.146	1.176
BB +1.1V P1 Vccp	Normal	Not Available	0.683	0.707	1.5	1.543
BB +1.1V P2 Vccp	Normal	Not Available	0.683	0.707	1.5	1.543
BB +1.5V P1 DDR3	Normal	Not Available	1.361	1.4	1.589	1.634
BB +1.5V P2 DDR3	Normal	Not Available	1.361	1.4	1.589	1.634
BB +1.8V AUX	Normal	Not Available	1.673	1.719	1.873	1.927
BB +3.3V	Normal	Not Available	2.981	3.067	3.524	3.625
BB +3.3V STBY	Normal	3.339 Volts	2.981 Volts	3.067 Volts	3.524 Volts	3.625 Volts
BB +3.3V Vbat	Normal	Not Available	2.177	2.502	3.191	3.282
BB +5.0V	Normal	Not Available	4.471	4.63	5.379	5.538
BB +5.0V STBY	Normal	5.014 Volts	4.608 Volts	4.736 Volts	5.271 Volts	5.421 Volts
BB +12.0V	Normal	Not Available	10.739	11.103	12.923	13.287
BB -12.0V	Normal	Not Available	-12.512	-12.443	-11.519	-11.422
Baseboard Temp	Normal	Not Available	5	10	61	66
Front Panel Temp	Normal	Not Available	0	5	44	48

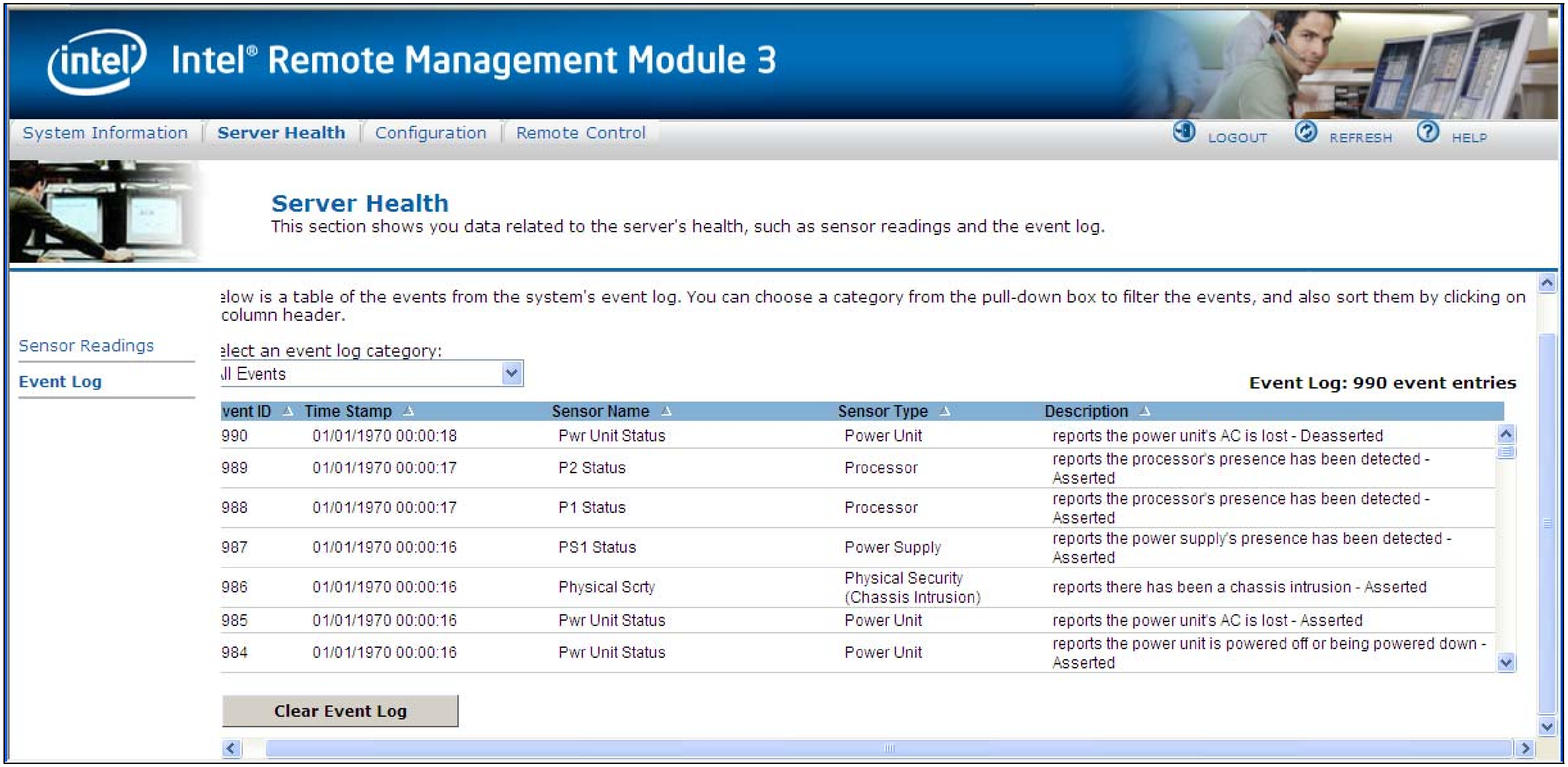
Figure 31. Server Health > Sensor Readings window (Thresholds displayed)

The following table lists the options available on this page:

Option	Task
Sensor Selection drop-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 located at the bottom of the page to move the display to the 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 32.



Server Health

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

elow is a table of the events from the system's event log. You can choose a category from the pull-down box to filter the events, and also sort them by clicking on column header.

elect an event log category: ll Events

Event Log: 990 event entries

vent ID	Time Stamp	Sensor Name	Sensor Type	Description
990	01/01/1970 00:00:18	Pwr Unit Status	Power Unit	reports the power unit's AC is lost - Deasserted
989	01/01/1970 00:00:17	P2 Status	Processor	reports the processor's presence has been detected - Asserted
988	01/01/1970 00:00:17	P1 Status	Processor	reports the processor's presence has been detected - Asserted
987	01/01/1970 00:00:16	PS1 Status	Power Supply	reports the power supply's presence has been detected - Asserted
986	01/01/1970 00:00:16	Physical Scrty	Physical Security (Chassis Intrusion)	reports there has been a chassis intrusion - Asserted
985	01/01/1970 00:00:16	Pwr Unit Status	Power Unit	reports the power unit's AC is lost - Asserted
984	01/01/1970 00:00:16	Pwr Unit Status	Power Unit	reports the power unit is powered off or being powered down - Asserted

Figure 32. Server Health > Event Log

The following table lists the options available on this page:

Option	Task
Event Log Category drop-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 settings page is used to configure settings such as network, users, and alerts.

Note: The RMM3 IP address must be on a different subnet than the server board IP address used for management traffic.

It has the following options for server management as shown in Figure 33:

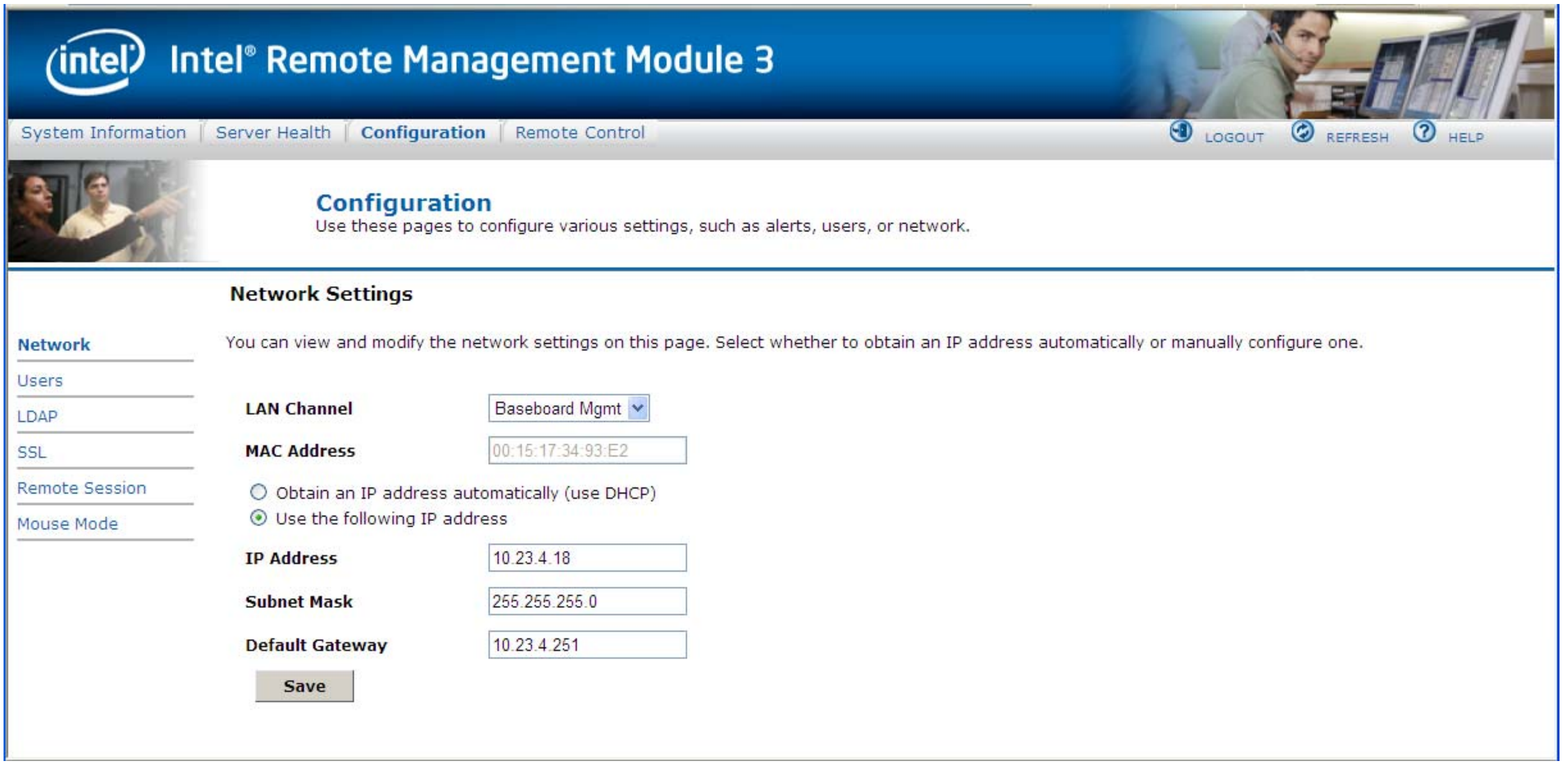
- Network
- Users
- LDAP
- SSL
- Remote Session
- Mouse Mode

7.3.1 Configuring Network Settings

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

- **Automatic**: Obtain an IP address automatically (using DHCP)

  OR
- **Manual:** Manually configure an IP address.



Configuration

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

Network Settings

You can view and modify the network settings on this page. Select whether to obtain an IP address automatically or manually configure one.

LAN Channel: Baseboard Mgmt

MAC Address: 00:15:17:34:93:E2

○ Obtain an IP address automatically (use DHCP)

● Use the following IP address

IP Address: 10.23.4.18

Subnet Mask: 255.255.255.0

Default Gateway: 10.23.4.251

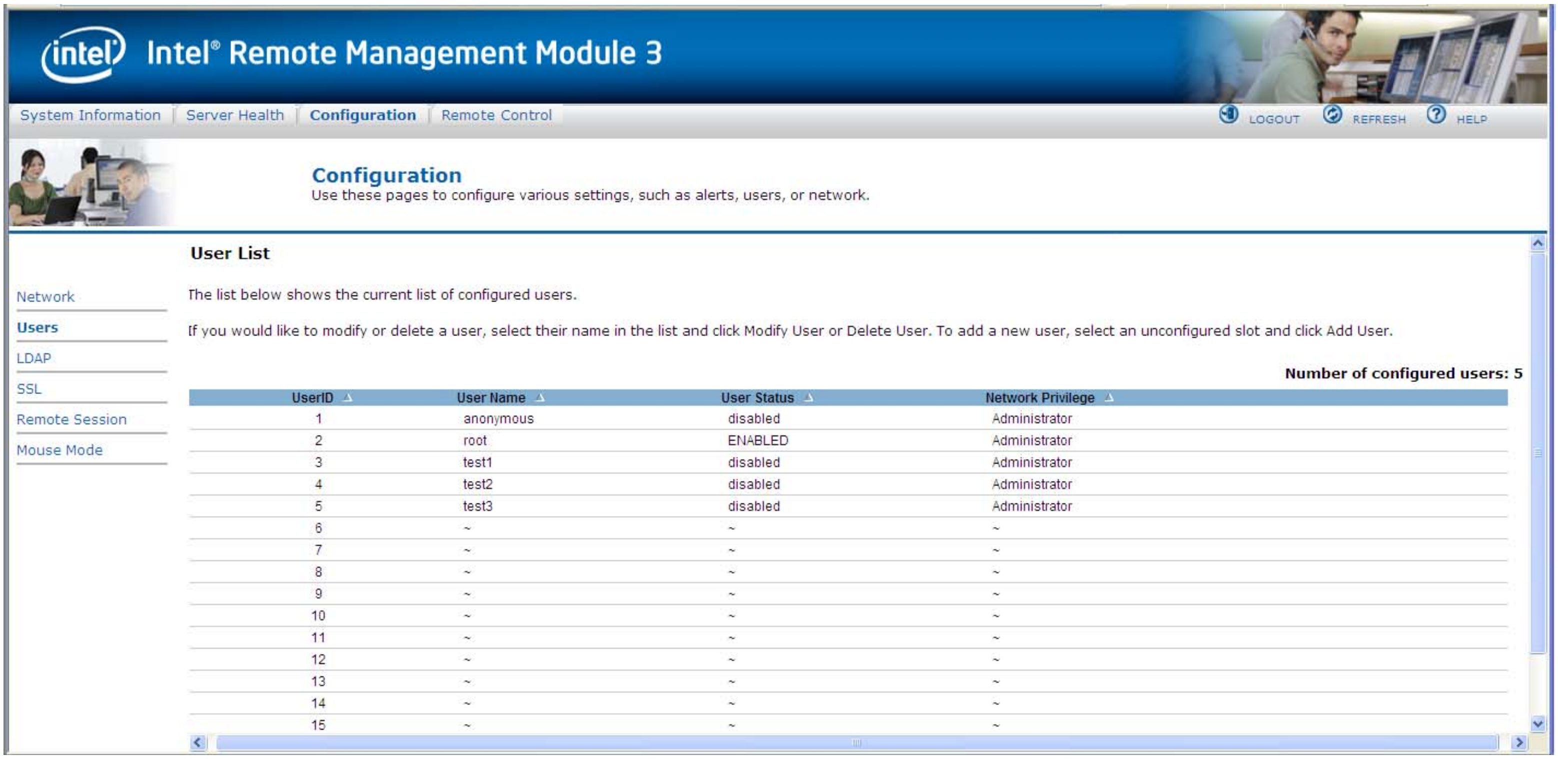
Figure 33. Configuration> Network Settings window

The following table lists the options available in this page:

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 Mgmt channel (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system.
MAC Address	The MAC address of the device (read only)
IP Address	Select the type of IP assignment using the radio buttons. If configuring a static IP, enter the requested address, subnet mask, and gateway in the given fields. • IP Address is made of four numbers, with each number separated by a period (.) as in "xxx.xxx.xxx.xxx". • '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

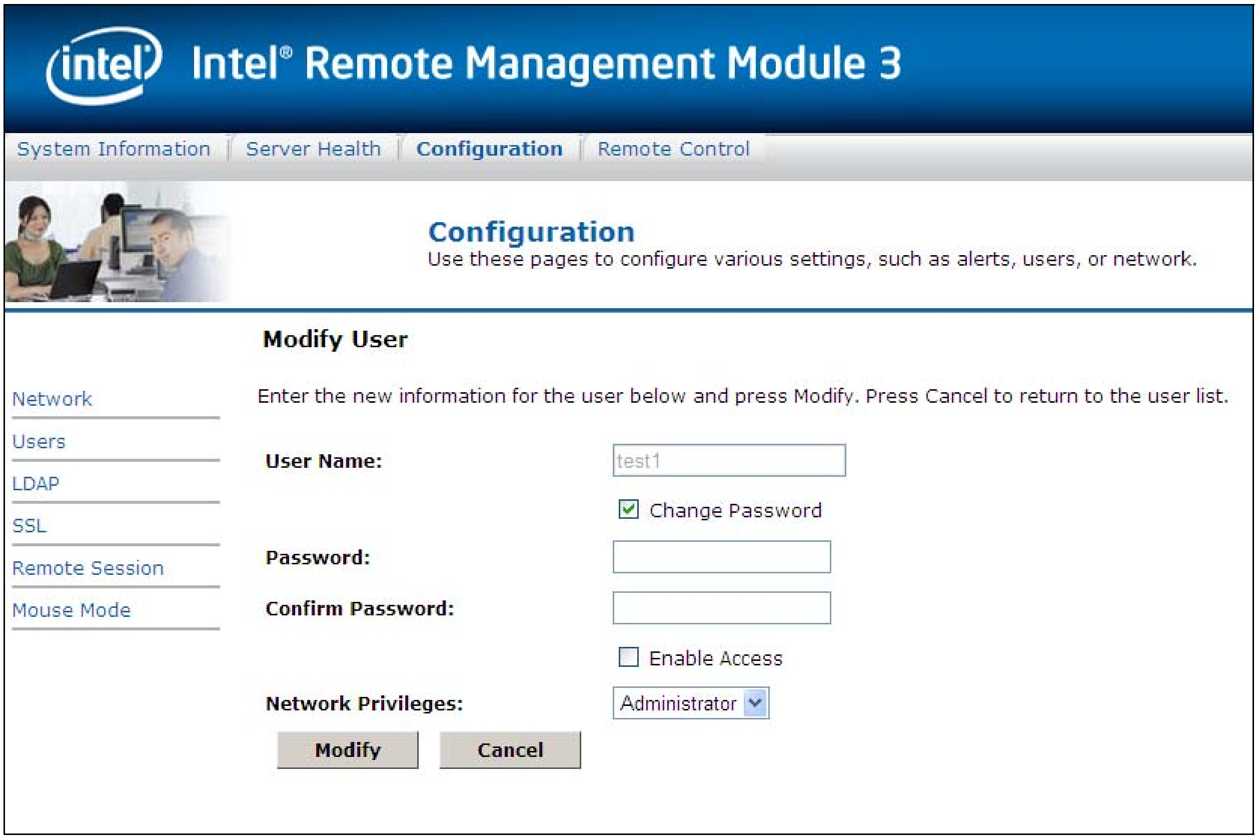
The list below shows the current list of configured users.

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

Figure 34. Configuring User List window



Configuration

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

Modify User

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

User Name: test1

☑ Change Password

Password:

Confirm Password:

□ Enable Access

Network Privileges: Administrator

Figure 35. 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.

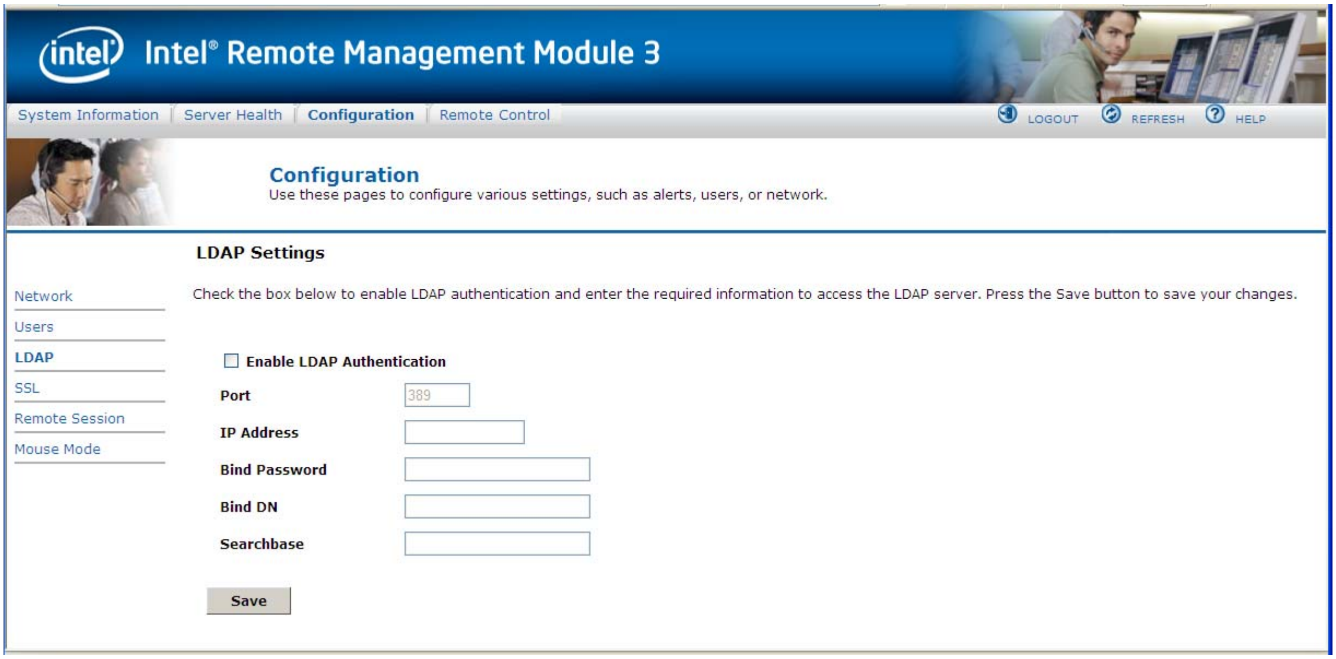
Notes:

- UserID 1 (anonymous) may not be renamed or deleted.
- UserID 2 (root) may not be renamed or deleted. Also, the network privileges of UserID 2 cannot 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 a user, select an empty slot in the list and click to add a new user.
- To modify a user, select a user in the list and click to modify their settings.
- To delete a user, select a user in the list and click to delete.

7.3.3 Configuring LDAP Settings

To enable/disable LDAP, select or clear the "Enable LDAP Authentication" checkbox respectively.



Configuration

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

LDAP Settings

Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Press the Save button to save your changes.

☐ Enable LDAP Authentication

Port: 389

IP Address:

Bind Password:

Bind DN:

Searchbase:

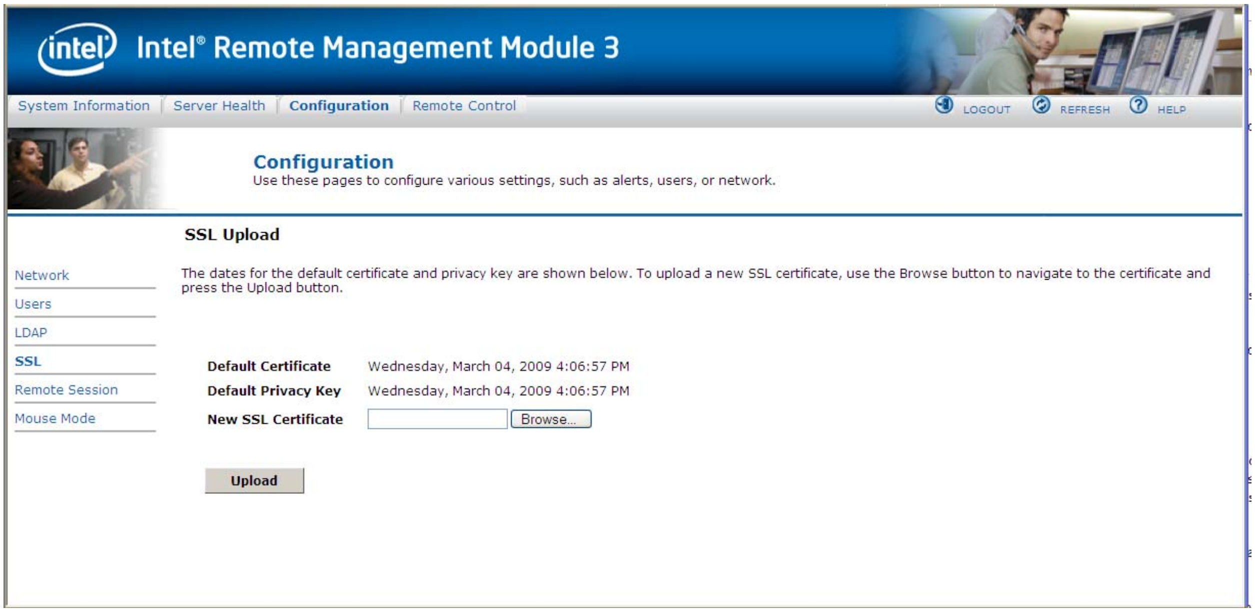
Figure 36. Configuring LDAP Settings window

The following table lists the options available on this page:

Option	Task
LDAP Authentication	Select this checkbox to enable LDAP authentication, and then enter the required information to access the LDAP server.
Port	Specify the LDAP Port.
IP Address	The IP address of LDAP server • IP Address is made of four numbers, with each number separated by a period (.) 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, "dc=my-domain, dc=com".
Save button	Click to save the current settings.

7.3.4 Configuring SSL Upload

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



Configuration

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

SSL Upload

The dates for the default certificate and privacy key are shown below. To upload a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button.

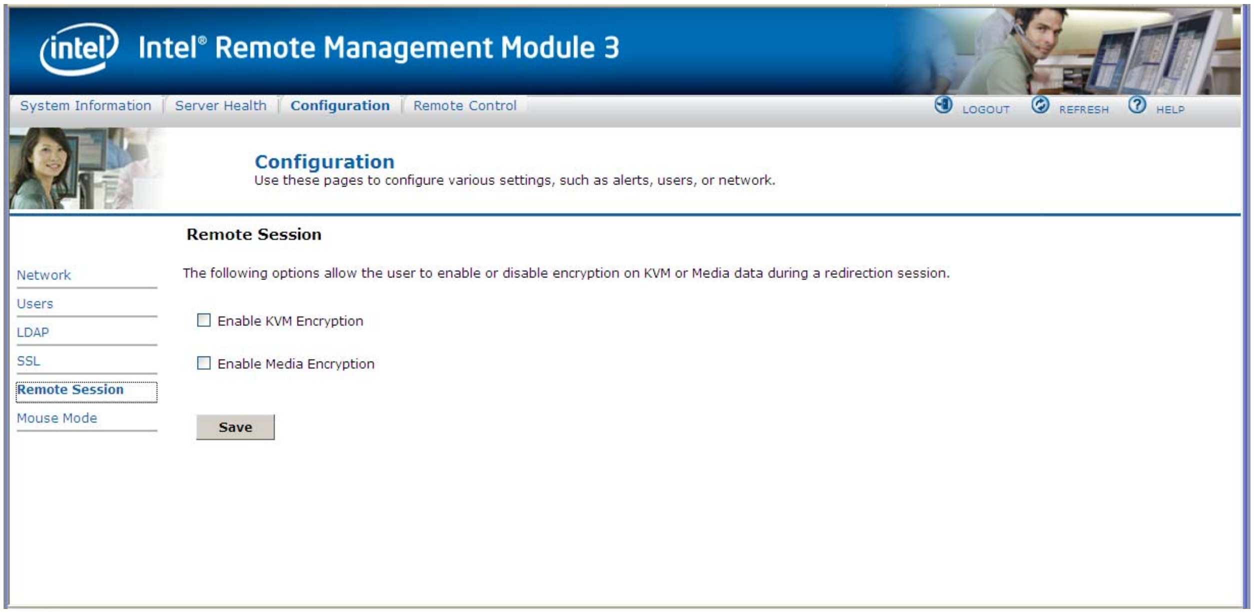
Default Certificate	Wednesday, March 04, 2009 4:06:57 PM
Default Privacy Key	Wednesday, March 04, 2009 4:06:57 PM
New SSL Certificate	

Figure 37. Configuring SSL Upload window

First, upload the SSL certificate and then the device prompts to upload the privacy key. If any of the files are invalid, the device provides a notification. The device also provides a notification on successful upload. After the SSL certificate is successful uploaded, the device will prompt to reboot the device. If you want to reboot, click 'Ok' or click 'Cancel' to cancel the reboot operation.

7.4 Configuring Remote Session

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



Configuration

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

Remote Session

The following options allow the user to enable or disable encryption on KVM or Media data during a redirection session.

☐ Enable KVM Encryption

☐ Enable Media Encryption

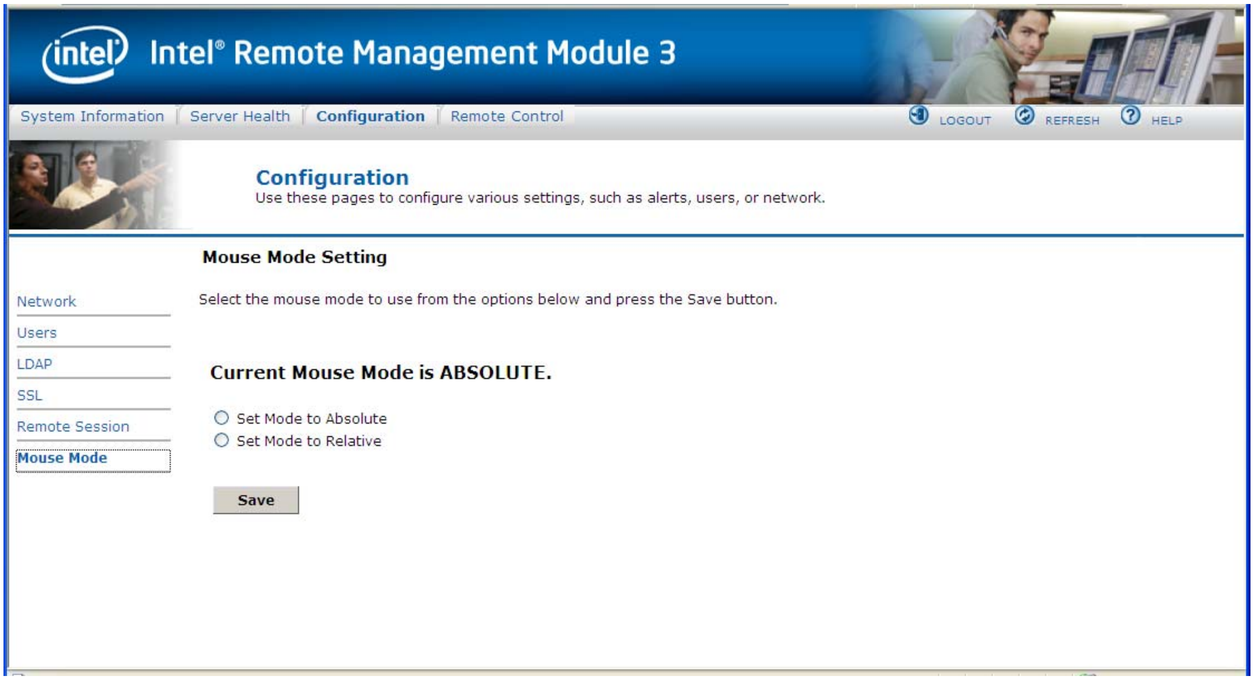
Figure 38. Configuring Remote Session window

The following table lists the options allowing you to enable or disable encryption on KVM or media data during a redirection session.

Option	Task
Enable/Disable Encryption mode	Enable/Disable encryption on KVM or Media data during a redirection session. **Notes:** • KVM and Media encryption are enabled by default. • Disabling encryption can improve performance of KVM or Media redirection.
Save button	Click to use the 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 39.



Configuration

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

Mouse Mode Setting

Select the mouse mode to use from the options below and press the Save button.

Current Mouse Mode is ABSOLUTE.

○ Set Mode to Absolute

○ Set Mode to Relative

Figure 39. Configuring Mouse Mode Setting window

The Redirection Console handles mouse emulation from a local window to the remote screen using one of the following two methods:

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

Click **Save** to use the selected mode.

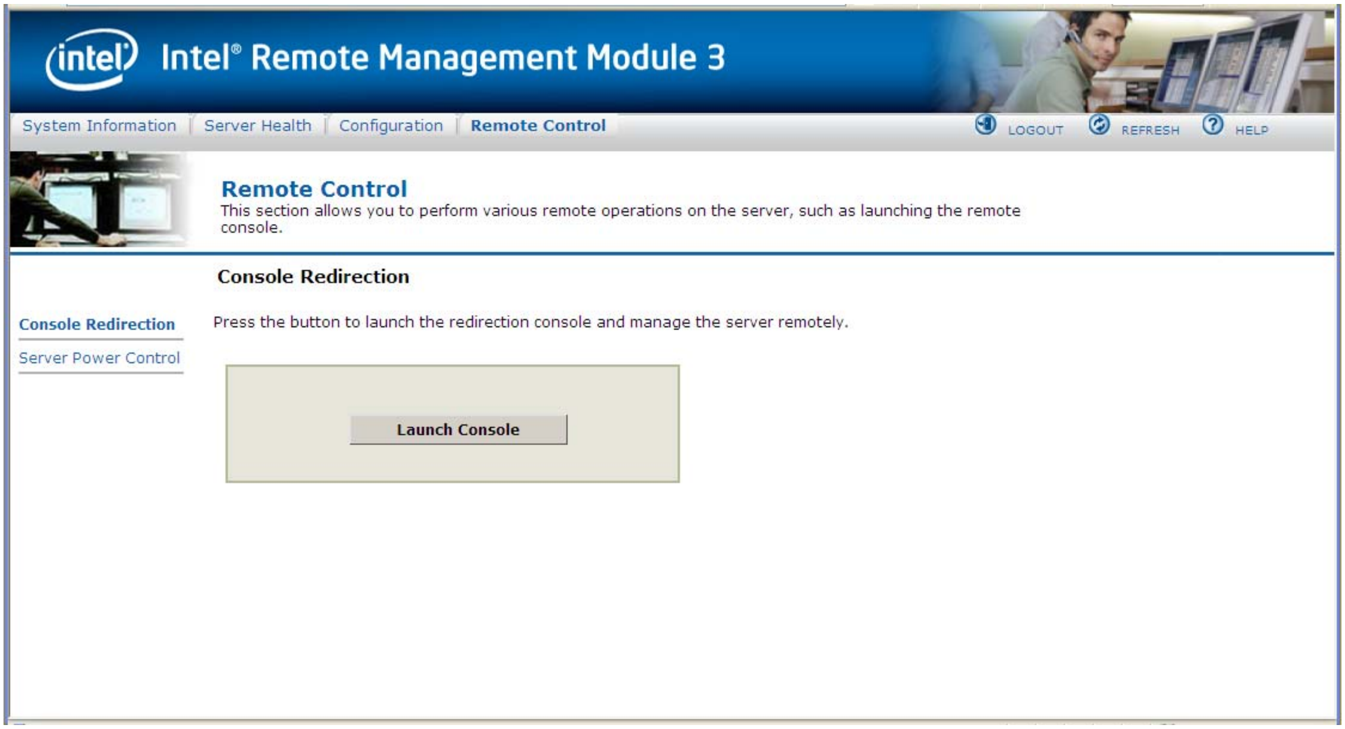
7.5 Remote Control

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

- Console redirection
- Server power control

7.5.1 Console Redirection

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



Remote Control

This section allows you to perform various remote operations on the server, such as launching the remote console.

Console Redirection

Press the button to launch the redirection console and manage the server remotely.

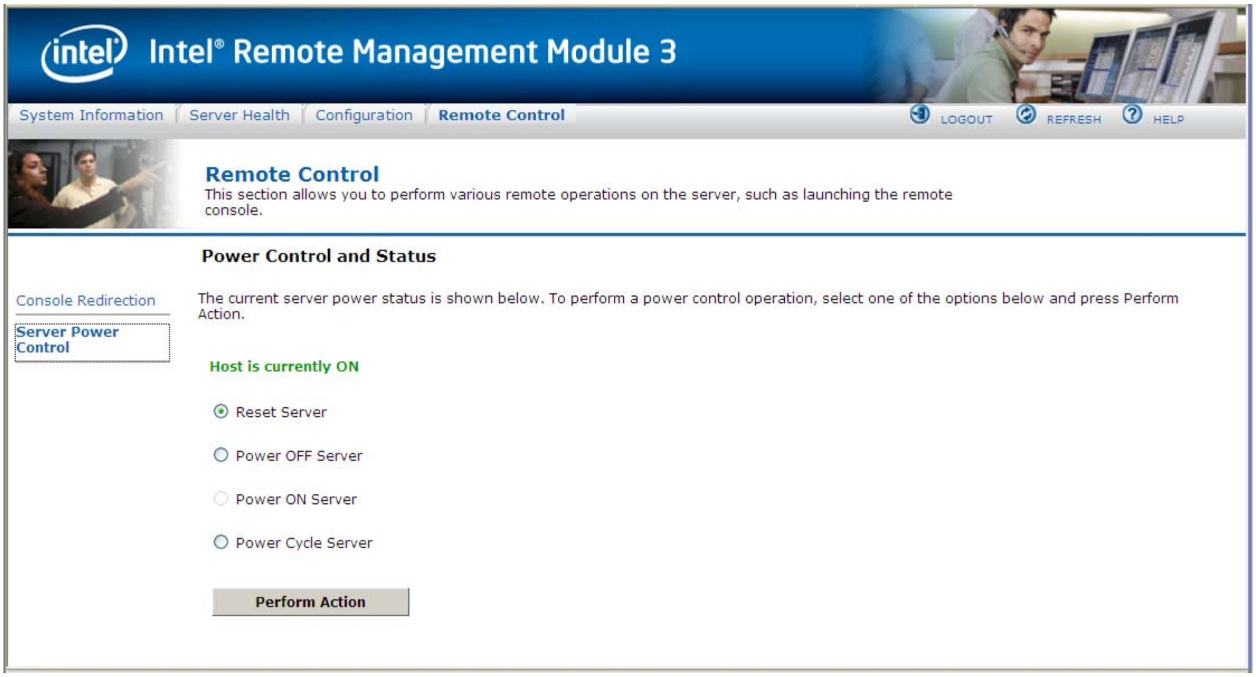
Figure 40. Remote Control > Console Redirection window

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

Note: Java Runtime Environment (JRE) version 6, update 10 or later must be installed on the client prior to launching the JNLP file.

7.5.2 Server Power Control

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



Remote Control

This section allows you to perform various remote operations on the server, such as launching the remote console.

Power Control and Status

The current server power status is shown below. To perform a power control operation, select one of the options below and press Perform Action.

Host is currently ON

● Reset Server

○ Power OFF Server

○ Power ON Server

○ Power Cycle Server

Figure 41. Server Power Control window

The following power control operations can be performed:

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

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

The Intel® RMM3 supports an interface to System Management Architecture for Server Hardware-Lite* (SMASH–Lite*).

The SMASH* v1.0 suite of specifications was released by 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 Intel® RMM3.

8.1 Logging into the SMASH* session

1. ssh to BMC from the client machine.

2. SMASH console screen(‘ ’) should appear.

3. This executable will initialize all the needed variables, discover the targets and will show the SMASH console screen.

8.2 SMASH* Targets

SMASH Targets is the first layer of the SMASH which contains two targets: settings1 and system1. The settings1 contains all the current session supported values and the system1 is the server/blade and about this target is explained in the next section.

8.2.1 Supported Properties

The supported properties of the SMASH targets are identity. Each property is explained in the following sections.

8.2.1.1 Identity

This property gives a one word brief explanation about the present target. This property is a read-only property. It cannot be changed.

8.2.2 Supported Verbs

The supported verbs of the SMASH targets are as follows:

8.2.2.1 cd

The verb cd is used to change from one valid target path to the any other valid target path

8.2.2.2 exit

The verb exit is used to exit from the current SMASH session.

8.2.2.3 help

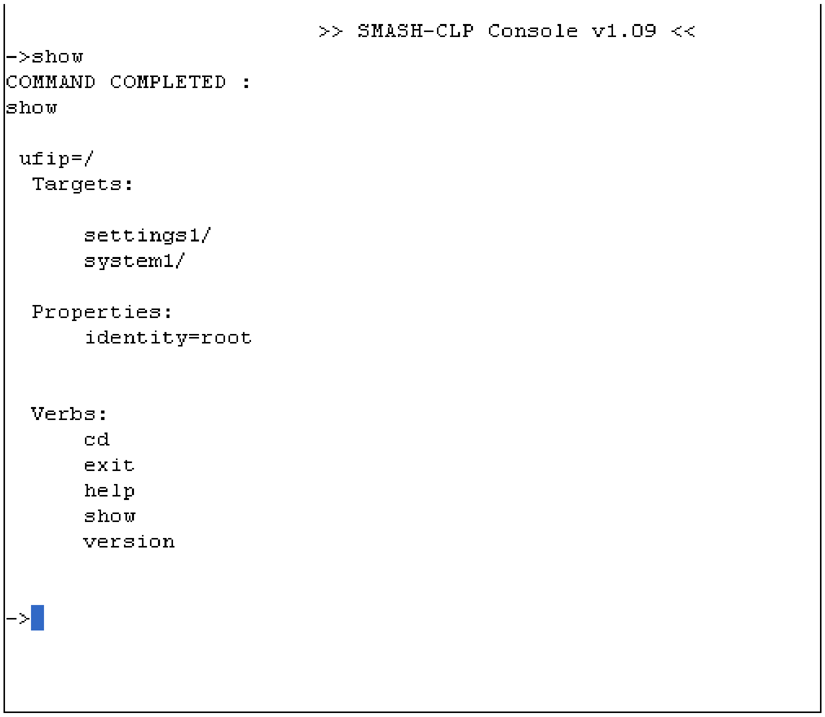
The verb help is used to provide information for the SMASH usage.

8.2.2.4 show

The verb show is used to show all the targets, supported properties, and supported verbs by this target.

8.2.2.5 version

The verb version, is used to shows 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 42. SMASH* Target

8.3 System1

The system target represents the server/blade. Power control is available on this target .System1 contains sol1, sp1 and other sensor monitoring targets. Here sp1 means Service Process Configuration.

8.3.1 Supported Properties

The supported properties of the target system1 are as follows:

8.3.1.1 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:

- 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.

8.3.1.2 SysIdSupported

This read-only property indicates if System Identification is supported or not.

- SUPPORTED – indicates that system identification is supported
- NOT SUPPORTED - indicates that system identification is not supported.

8.3.1.3 SysIdentification

This R/W property reflects the current state of system identification.

1. It can set to any of the following values:

   System identification can be turned off as follows.
   ->Set SysIdentification=OFF

   System identification can be timed ON as follows.
   ->Set SysIdentification=TIMED

2. Set the timeout value. Now, the TimeOutValue property is set to TIMED and SysIdentification property value is set to ON

   Note: If we
   ->set SysIdentification=INDEFINITE, then TimeOutValue property is set to INDEFENITE and SysIdentification property value is setted to ON

8.3.1.4 TimeOutValue

This value is R/W, which is associated with TIMED (ON) gives input in seconds as follows:

- 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 we have to set the TimeOutValue as
  ->Set TimeOutValue=3 (only numeric, non zero values accepted).

8.3.1.5 identity

This read-only property gives a brief explanation of current target. This property cannot be changed.

8.3.2 Supported Verbs

The supported verbs of the system1 targets are as follows:

8.3.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.3.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.3.2.3 help

The verb help is used to provide information on using SMASH*.

8.3.2.4 set

The verb set is used to the set the R/W supported properties.

8.3.2.5 reset

The verb reset is used to reset the device.

8.3.2.6 show

The verb show is used to show all the targets, supported properties, and supported verbs of this target.

8.3.2.7 start

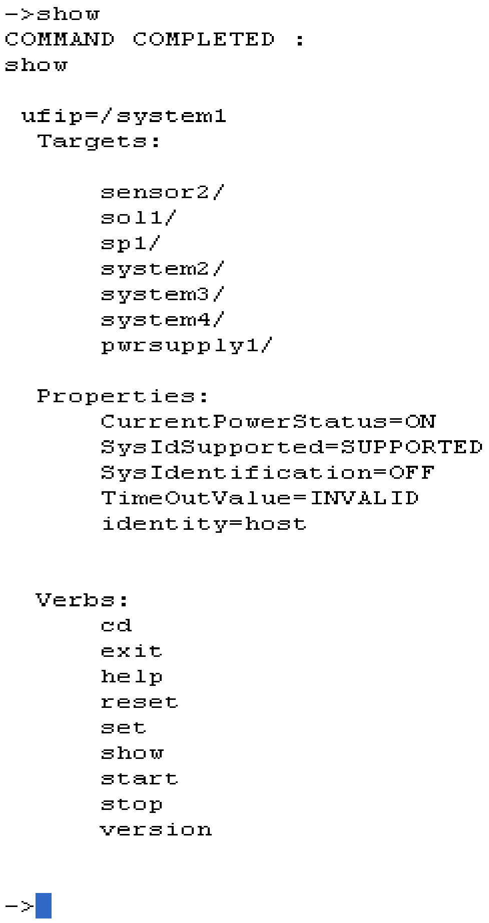
The verb start is used to start the device.

8.3.2.8 stop

The verb stop is used to stop the device.

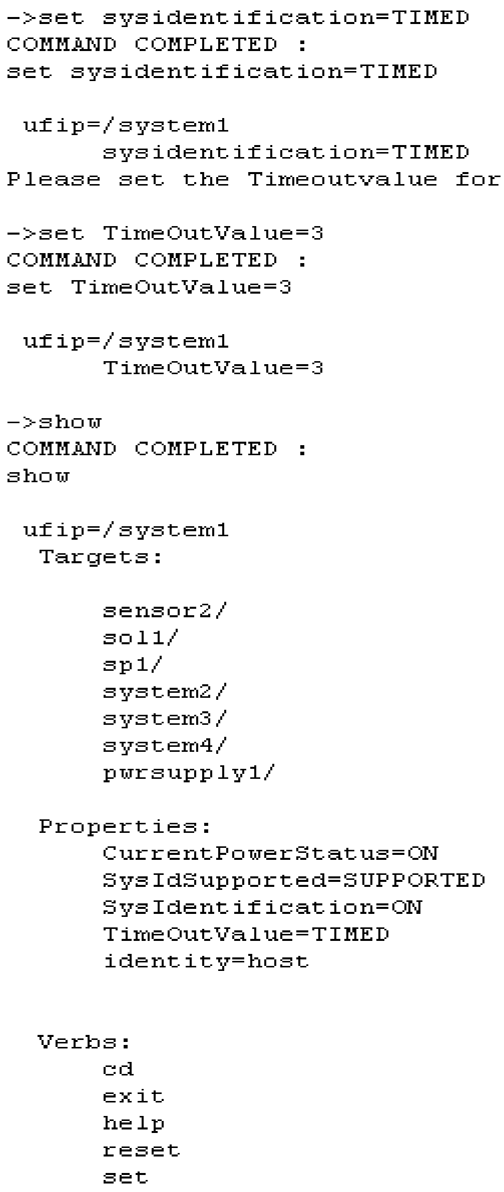
8.3.2.9 version

The verb version is used to show the current version of the 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 43. 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 44. System Target - an example

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:

8.4.1.1 cdt

This property represents the current default directory. This is the path from where the session starts.

8.4.1.2 outputformat

This R/W property gives the output format: clpxml, text, clpcsv.

Keyword of the currently running SMASH* session.

The values supported by this property are explained below.

- Clpxml - The output format of the currently running SMASH* session will be in the .xml format ->set outputformat=clpxml
- Keyword - The output format of the currently running SMASH session will be in the keyword format ->set outputformat=keyword.
- Text - The output format of the currently running SMASH session will be 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.

8.4.1.3 timeout

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. This is.

The value of this property can be set to preferred inactivity time. By default it is assigned to

500.

```
->set timeout=300
```

8.4.1.4 identity

This property gives a brief explanation about the present target. This property is a read-only property and cannot be changed.

8.4.2 Supported Verbs

The supported verbs of the settings1 target are as follows:

8.4.2.1 cd

The verb cd is used to change from one valid target path to the any other valid target path.

8.4.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.4.2.3 help

The verb help is used to provide information on using SMASH*.

8.4.2.4 set

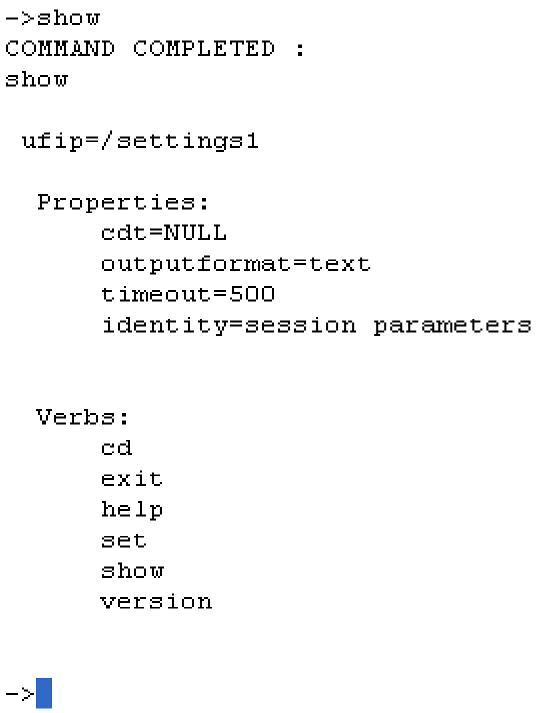
The verb set is used to the set the r/w supported properties.

8.4.2.5 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.4.2.6 version

The verb version is used to show the current version of the 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 45. 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 target SP1 is as follows:

8.5.1.1 Identity

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.5.2 Supported Verbs

The supported verbs of the SP1 target are as follows.

8.5.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path

8.5.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.5.2.3 help

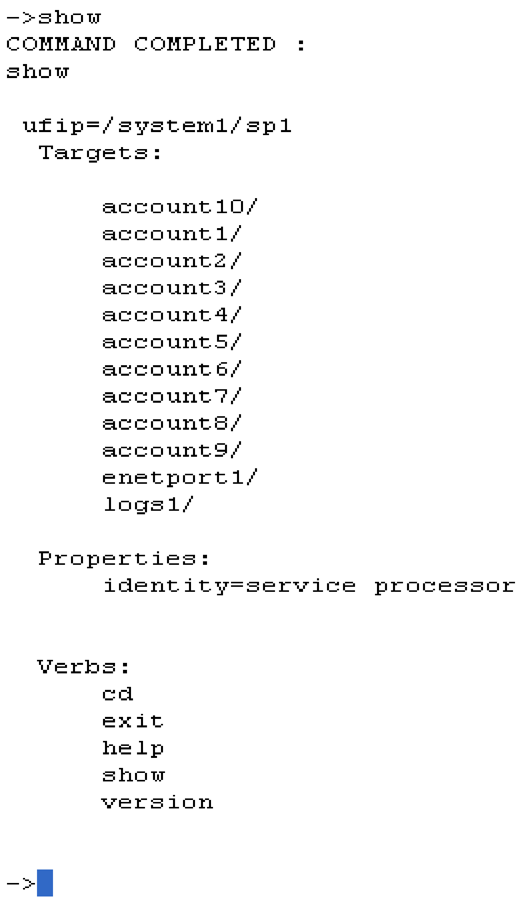
The verb help is used to provide information on using SMASH*.

8.5.2.4 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.5.2.5 version

The verb version is used to show the current version of the 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 46. 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 SOL1 is as follows:

8.6.1.1 identity

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.6.2 Supported Verbs

The supported verbs of the SOL1 target are as follows:

8.6.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.6.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.6.2.3 help

The verb help is used to provide information on using SMASH*.

8.6.2.4 show

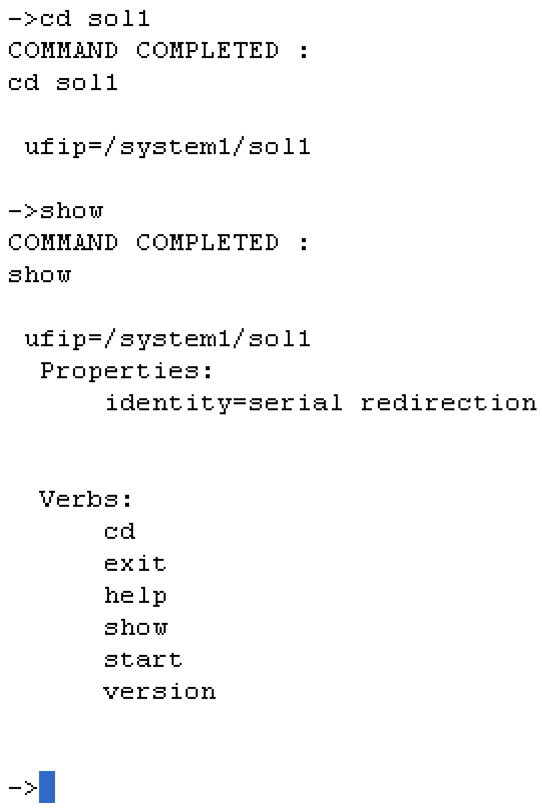
The verb show is used to show all the targets, properties, and verbs supported by this target.

8.6.2.5 start

To start the device.

8.6.2.6 version

The verb version is used to show the current version of the SMASH*.



```
->cd sol1
COMMAND COMPLETED :
cd sol1

 ufip=/system1/sol1

->show
COMMAND COMPLETED :
show

 ufip=/system1/sol1
  Properties:
      identity=serial redirection


  Verbs:
      cd
      exit
      help
      show
      start
      version


->
```

Figure 47. 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 the place of ESCAPE key.

Once terminated, the control will come back 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:

8.7.1.1 macaddress

Address that was received by the activated session. This property gives the value of macaddress. Mac address is an unique identifier attached to most network adaptors (NICs) This property is a read-only property.

8.7.1.2 identify

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.7.2 Supported Verbs

The supported verbs of the Enetport1 target as follows:

8.7.2.1 cd

The verb cd, is used to change from one valid target path to any other valid target path

8.7.2.2 exit

The verb exit s used to exit from the current SMASH* session.

8.7.2.3 help

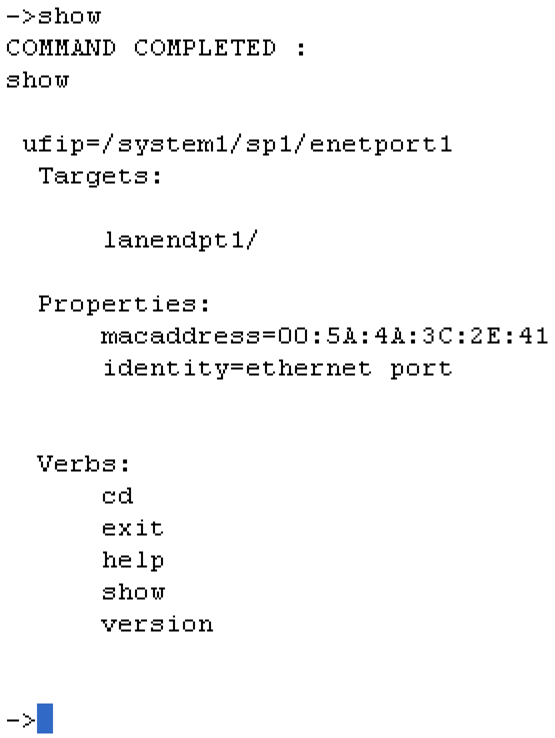
The verb help is used to provide information on using SMASH*.

8.7.2.4 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.7.2.5 version

The verb version is used to 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 48. Enetport1 Target

8.8 Lanendpt1

The target Lanendpt1 gives information about LAN configuration. It contains the following target:

- Ipendpt1 - IP configuration.

8.8.1 Supported Properties

Following is the supported property of target lanendpt1:

8.8.1.1 identity

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.8.2 Supported Verbs

The supported verbs of the Lanendpt1 target are as follows:

8.8.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.8.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.8.2.3 help

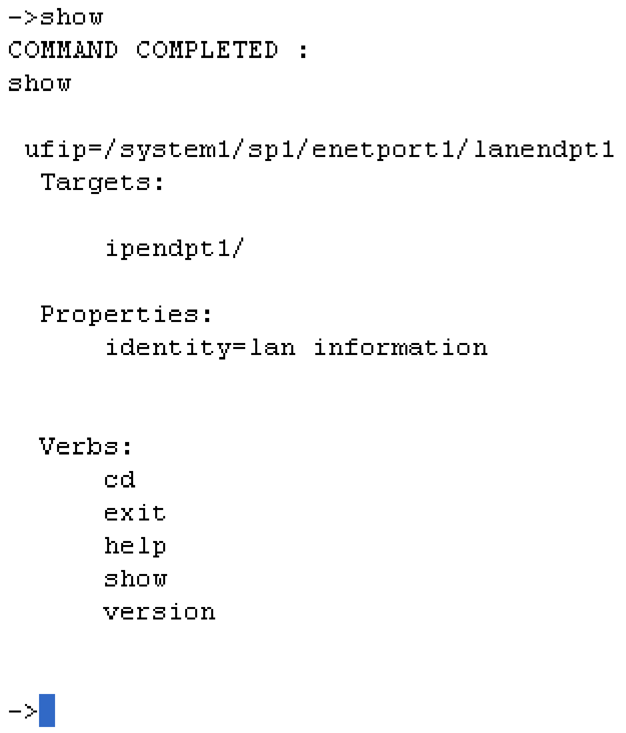
The verb help is used to provide information on using SMASH*.

8.8.2.4 show

The verb show is used to show all the targets, properties and verbs supported by this target.

8.8.2.5 version

The verb version is used to 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 49. 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:

8.9.1.1 ipaddress

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.

```
->set ipaddress=10.0.4.79
```

This will change the ipaddress of the sp. After changing, use committed property to save.

8.9.1.2 subnetmask

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.

```
->set subnetmask=255.255.248.0
```

This will change the subnetmask of the sp. After changing, use committed property to save.

8.9.1.3 usedhcp

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 an R/W property.

```
->set usedhcp=1
```

8.9.1.4 committed

Once the ipadress 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.

```
->Set commited=1
```

8.9.1.5 identity

This property gives a brief explanation about the present target. This property is a read only property and cannot be changed.

8.9.2 Supported Verbs

The supported verbs of the Ipendpt1 target are as follows:

8.9.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.9.2.2 exit

The verb exit is used to exit from the current SMASH session.

8.9.2.3 help

The verb help is used to provide information on using SMASH*.

8.9.2.4 set

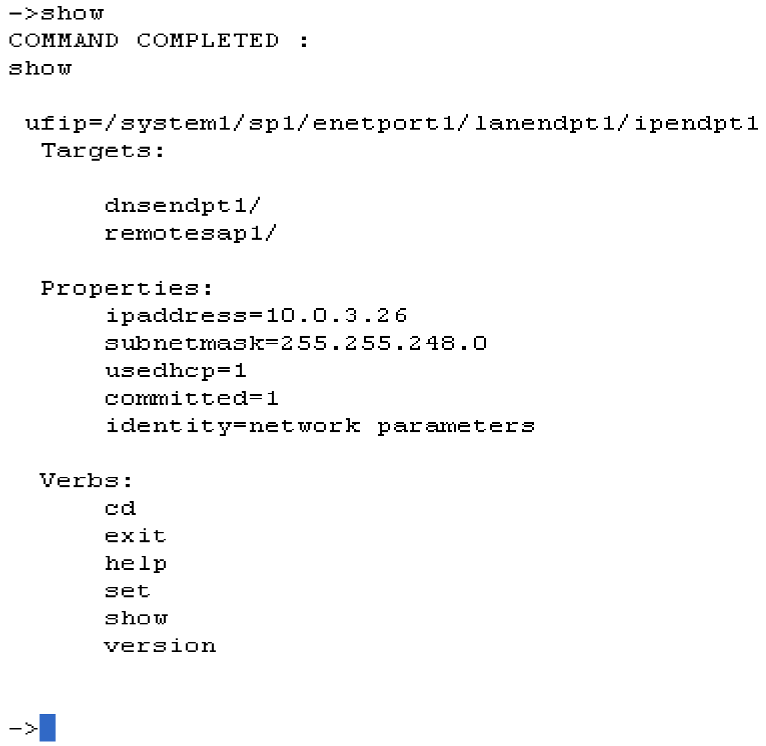
The verb set is used to set the r/w supported properties.

8.9.2.5 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.9.2.6 version

The verb version is used to 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 50. 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 contains any targets.

8.10.1 Supported Properties

The supported properties of the target remotesap1 are as follows:

8.10.1.1 . defaultgatewayaddress

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:

```
->Set defaultgatewayip=0.0.0.0
```

8.10.1.2 identity

This property gives a brief explanation about the present target. This property is a read only property and cannot be changed.

8.10.2 Supported Verbs

The supported verbs of the Remotesap1 target are as follows.

8.10.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.10.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.10.2.3 help

The verb help is used to provide information on using SMASH*.

8.10.2.4 set

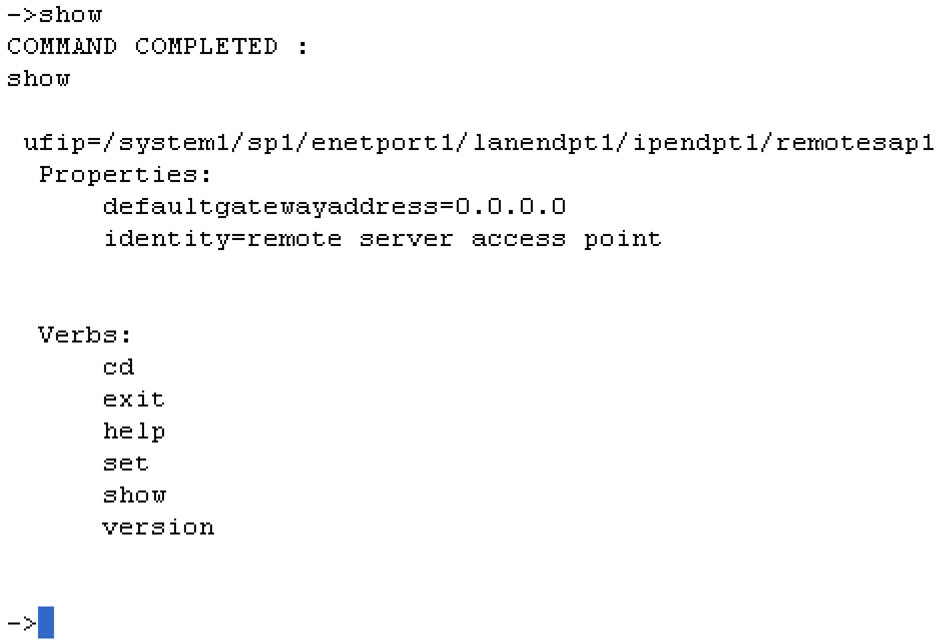
The verb set is used to set the r/w supported properties.

8.10.2.5 show

The verb show is used to show all the targets, properties and verbs supported by this target.

8.10.2.6 version

The verb version is used to show the current version of SMASH*.



```
->show
COMMAND COMPLETED :
show

 ufip=/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 51. 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:

8.11.1.1 domainnamefromdhcp

Dhcp based DNS configuration. This property is a read-only property.

8.11.1.2 dnsdomainname

This property gives the DNS Domain. This property is a read-only property.

8.11.1.3 serversfromdhcp

This property shows the servers dhcp. This is a read-only property.

8.11.1.4 identity

This property gives a brief explanation about the present target. This property is a read-only property and cannot be changed.

8.11.2 Supported Verbs

The supported verbs of the Dnsendpt1 target are as follows.

8.11.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.11.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.11.2.3 help

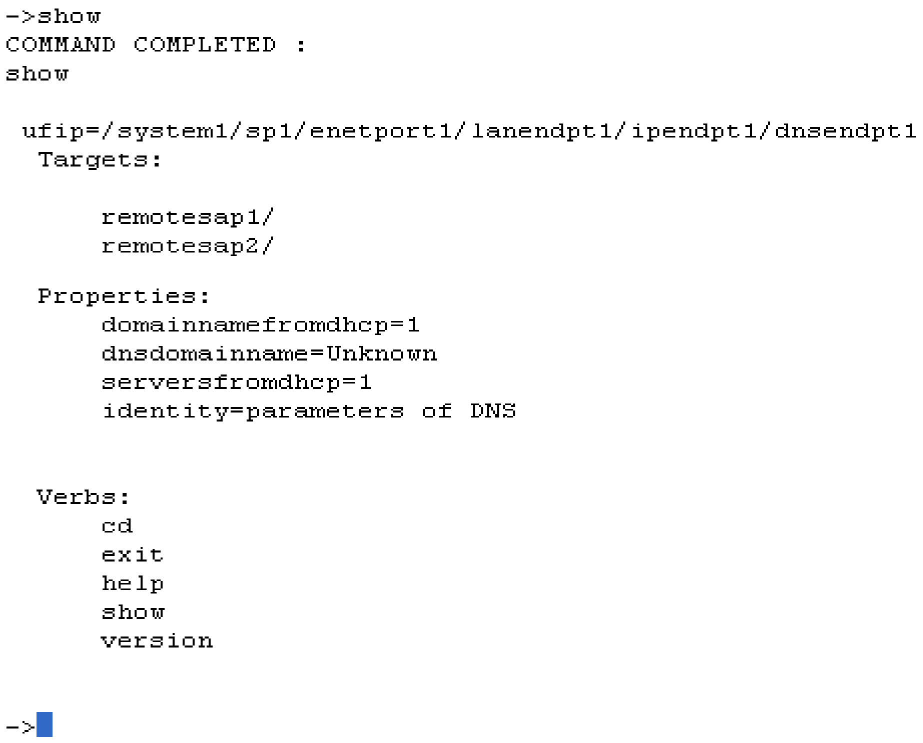
The verb help is used to provide information on using SMASH*.

8.11.2.4 show

The verb show is used to show all the targets, properties and verbs supported by this target.

8.11.2.5 version

The verb version is used to 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 52. 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.

8.12.1.1 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

8.12.1.2 identity

This property gives a one word brief explanation about the present target. This property is a read-only property and cannot be changed.

8.12.2 Supported Verbs

The supported verbs of the remotesap1 target as follows.

8.12.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.12.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.12.2.3 help

The verb help is used to provide information on using SMASH*.

8.12.2.4 set

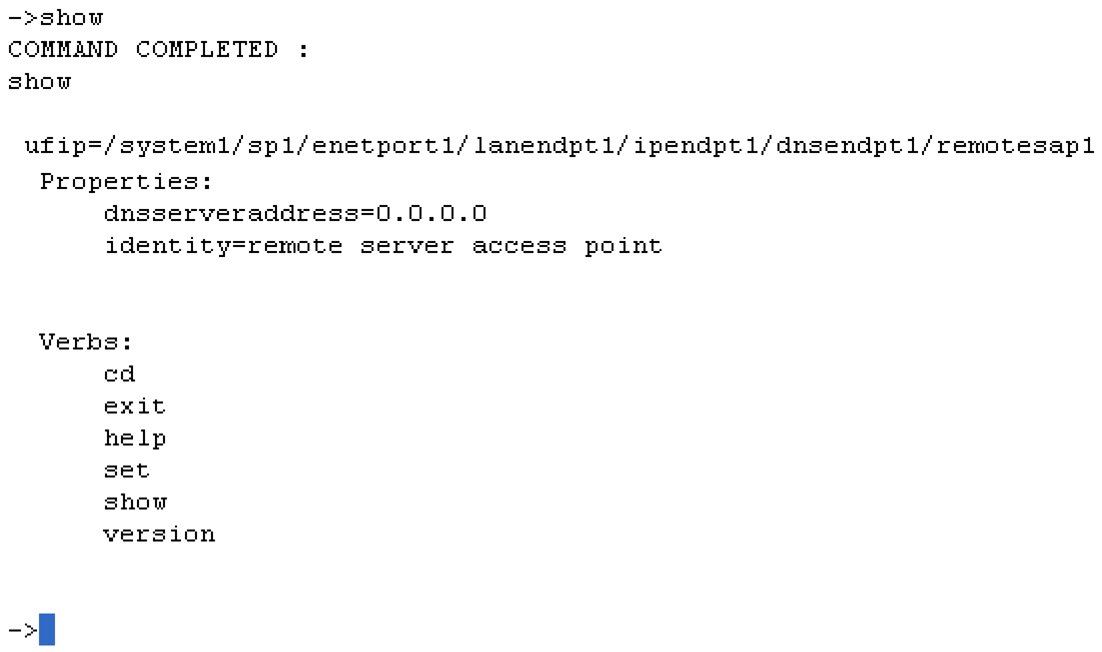
The verb set is used to set the r/w supported properties.

8.12.2.5 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.12.2.6 version

The verb version is used to show the current version of SMASH*.



```
->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 53. REMOTESAP1 Target

8.12.2.7 Remotesap2

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.

8.12.3 Supported Properties

The supported properties of the target remotesap2 are dnsserveraddress and identity.

8.12.3.1 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

8.12.3.2 identity

This property gives a brief explanation about the present target. This property is a read-only property and cannot be changed.

8.12.4 Supported Verbs

The supported verbs of the remotesap2 target are as follows.

8.12.4.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.12.4.2 exit

The verb exit is used to exit from the current SMASH* session.

8.12.4.3 help

The verb help is used to provide information on using SMASH*.

8.12.4.4 set

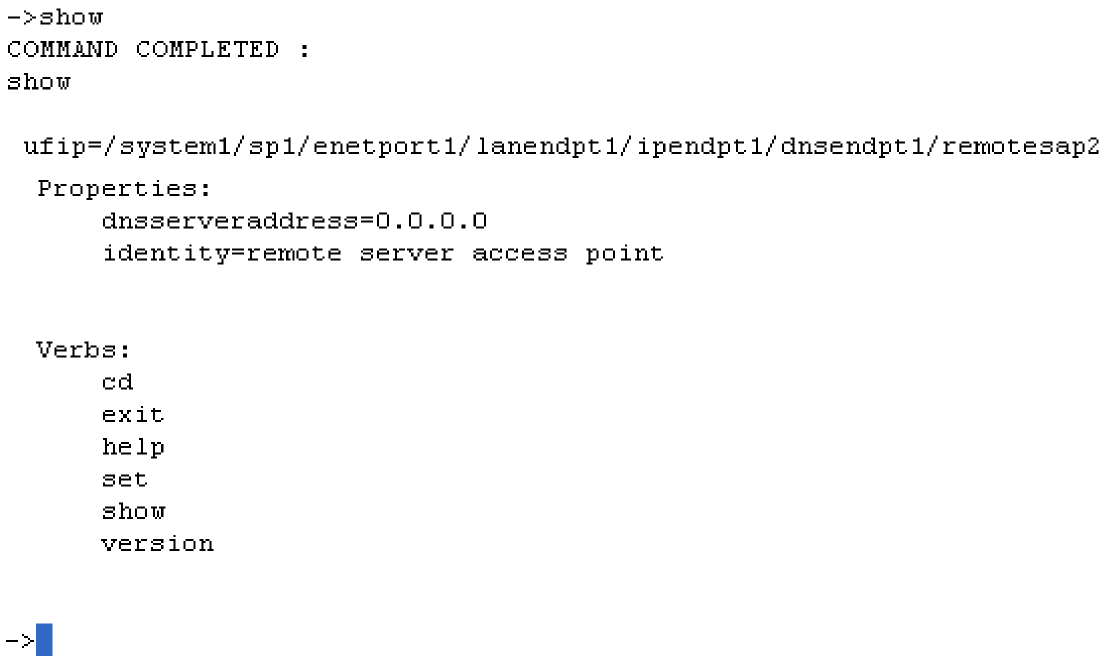
The verb set is used to set values to the r/w supported properties.

8.12.4.5 show

The verb show is used to show all the targets, properties and verbs supported by this target.

8.12.4.6 version

The verb version is used to 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 54. REMOTESAP2 Target

8.13 Account

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

8.13.1 Supported Properties

The supported properties of the target account are as follows.

8.13.1.1 userid

This property defines the unique id for each user. This property is read-only.

8.13.1.2 username

This property gives the usermname of a particular account. This is settable except for userid=1. Username Length must be more than 1 character and less than 16 characters.

->Set username=sdf

8.13.1.3 pmilanprivileges

This property gives the ipmi lan privileges. It can be set except for userid=1. Only numbers are allowed.

```
->set ipmilanprivileges=4
```

8.13.1.4 password

This property gives the password of a particular user. It can be set xcept for userid=1; password length should be less than 16 characters.

```
->Set password=ssd
```

8.13.1.5 enabledstate

This property shows the state of the user. This property is settable except for userid=1. Use 0 for disable and 1 for enable.

For example to enable the user set the value of this property to 1

```
->set userid=1
```

8.13.1.6 identity

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.13.2 Supported Verbs

The supported verbs of the account target are as follows.

8.13.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.13.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.13.2.3 help

The verb help is used to provide information on using SMASH*.

8.13.2.4 Delete

To delete, go to sp1 target and delete account(n) where n>2.

8.13.2.5 set

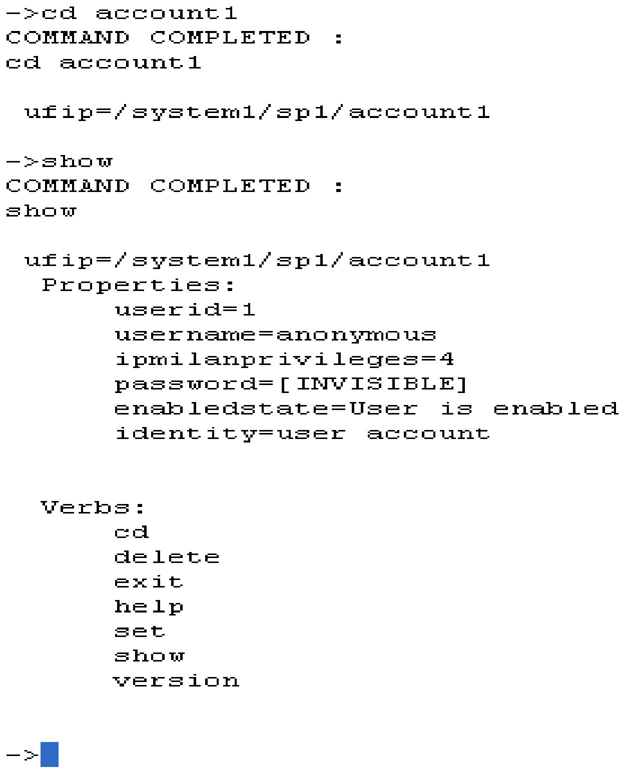
The verb set is used to set the r/w supported properties.

8.13.2.6 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.13.2.7 version

The verb version is used to 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 55. ACCOUNT1 Target

8.13.2.8 Logs1

The logs target is the containing target for log records of the ipmi System Event Log (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.

8.13.3 Supported Properties

The supported properties of the target Logs1 as follows.

8.13.3.1 MaxNumberOfRecords

This property is a read-only property and gives information about maximum number of log records.

8.13.3.2 MaxNumberOfRecords

This property is a read-only property gives the number of records found.

8.13.3.3 Description

This property is a read-only description about the target.

8.13.3.4 Identity

This property gives a brief explanation about the present target. This property is read-only and cannot be changed.

8.13.4 Supported Verbs

The supported verbs of the Logs1 target are as follows.

8.13.4.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.13.4.2 exit

The verb exit is used to exit from the current SMASH* session.

8.13.4.3 help

The verb help is used to provide information on using SMASH*.

8.13.4.4 delete

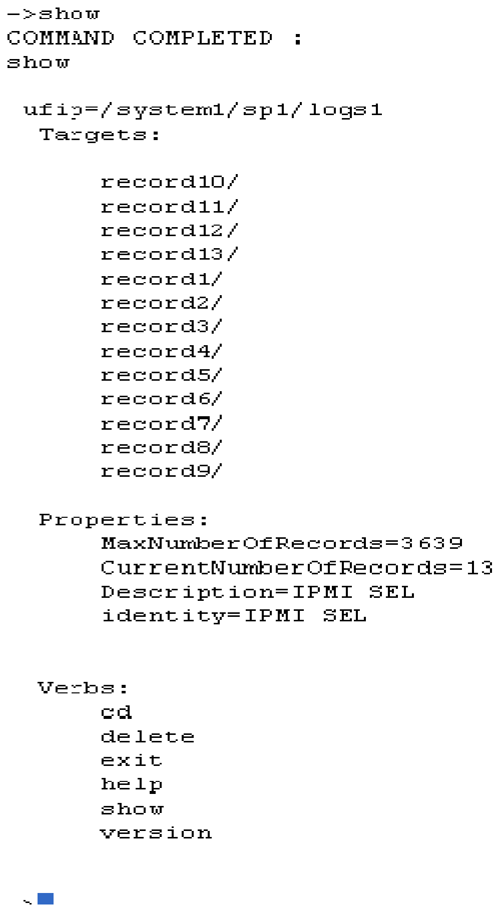
Individual SEL records cannot be deleted. Use Delete Logs1 to delete the entire set.

8.13.4.5 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.13.4.6 version

The verb version is used to 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 56. LOGS1 Target

8.14 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.

8.14.1 Supported Properties

The supported properties of the target Record1 are as follows.

8.14.1.1 LogCreationClassName

This property is a read-only property and gives information about the log creation class name.

8.14.1.2 LogName

This property is a read-only property and gives the name of the log record.

8.14.1.3 CreationClassName

This property is a read-only property and gives the creation class name of the record.

8.14.1.4 RecordID

SEL Entries have a unique 'Record ID' field .This is the unique ID for the particular record. This is a read-only property.

8.14.1.5 MessageTimeStamp

This gives the time stamp of the record creation and this is a read-only property.

8.14.1.6 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.

8.14.1.7 identity

This property gives a brief explanation about the present target. This property is read only and cannot be changed.

8.14.2 Supported Verbs

The supported verbs of the Record target are as follows.

8.14.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.14.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.14.2.3 help

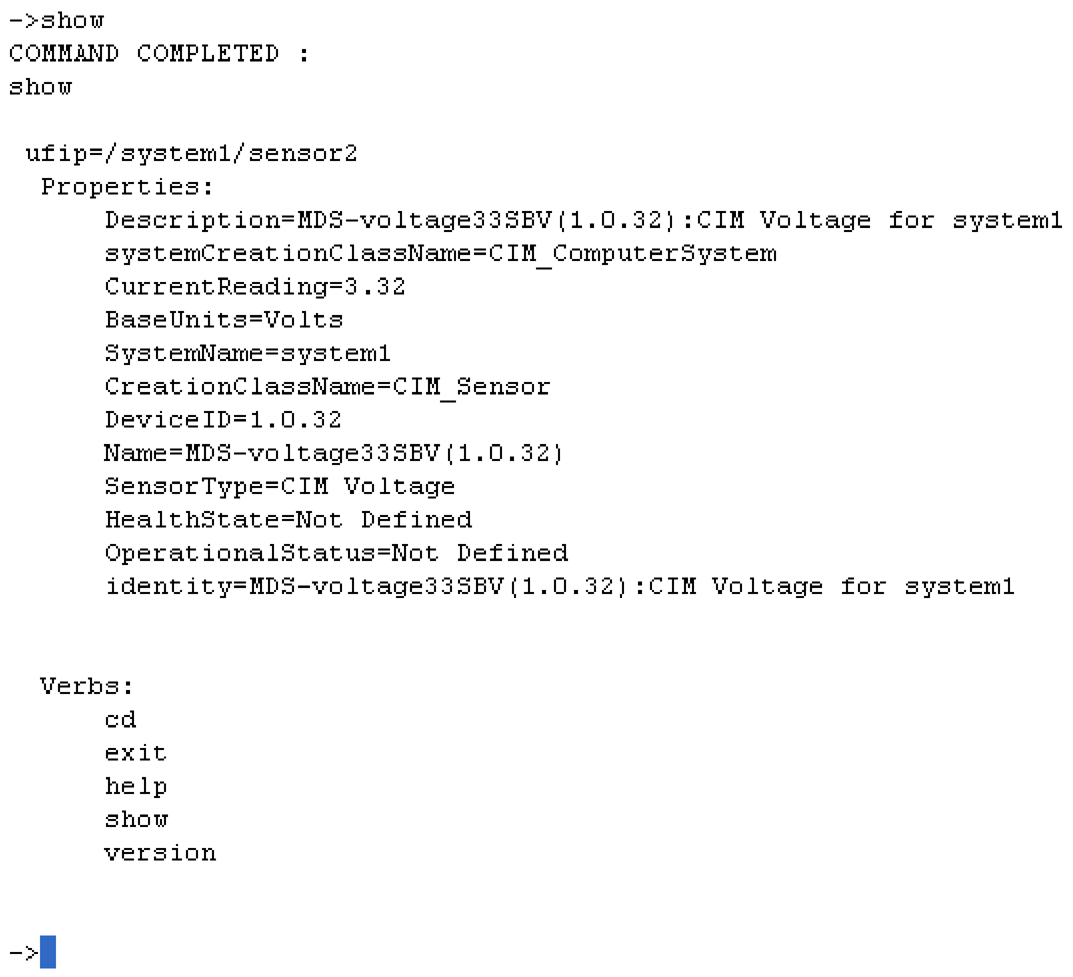
The verb help is used to provide information on using SMASH*.

8.14.2.4 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.14.2.5 version

The verb version is used to 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 57. RECORD1 Target

8.15 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 doesn't have any targets. All properties of this target are read-only properties.

8.15.1 Supported Properties

8.15.1.1 Description

This property describes the sensor and the target under which it is present. This property is read-only.

8.15.1.2 systemCreationClassName

This property gives the system creation class name and is a read-only property.

8.15.1.3 CurrentReading

This property gives the current reading shown by the sensor. This property is a read-only property.

8.15.1.4 BaseUnits

This property gives the units for the value given by current reading property. This property is a read-only property.

8.15.1.5 SystemName

This property gives the target name under which this sensor exists. This property is a read-only property.

8.15.1.6 CreationClassName

This property gives the creation class name of the sensor. It is a read-only property.

8.15.1.7 DeviceID

This property gives the device ID. This is a read-only property.

8.15.1.8 Name

This property gives the name of the current sensor. This property is a read-only property.

8.15.1.9 SensorType

This property gives the type of sensor. This property is a read-only property.

8.15.1.10 HealthState

This property gives the health status of the sensor. This property is a read-only property.

8.15.1.11 OperationalStatus

This property defines the operational status of the sensor. This property is a read-only property.

8.15.1.12 Identity

This property gives a brief explanation about the present target. This property is a read-only property and cannot be changed.

8.15.2 Supported Verbs

The supported verbs of the sensor target are as follows.

8.15.2.1 cd

The verb cd is used to change from one valid target path to any other valid target path.

8.15.2.2 exit

The verb exit is used to exit from the current SMASH* session.

8.15.2.3 help

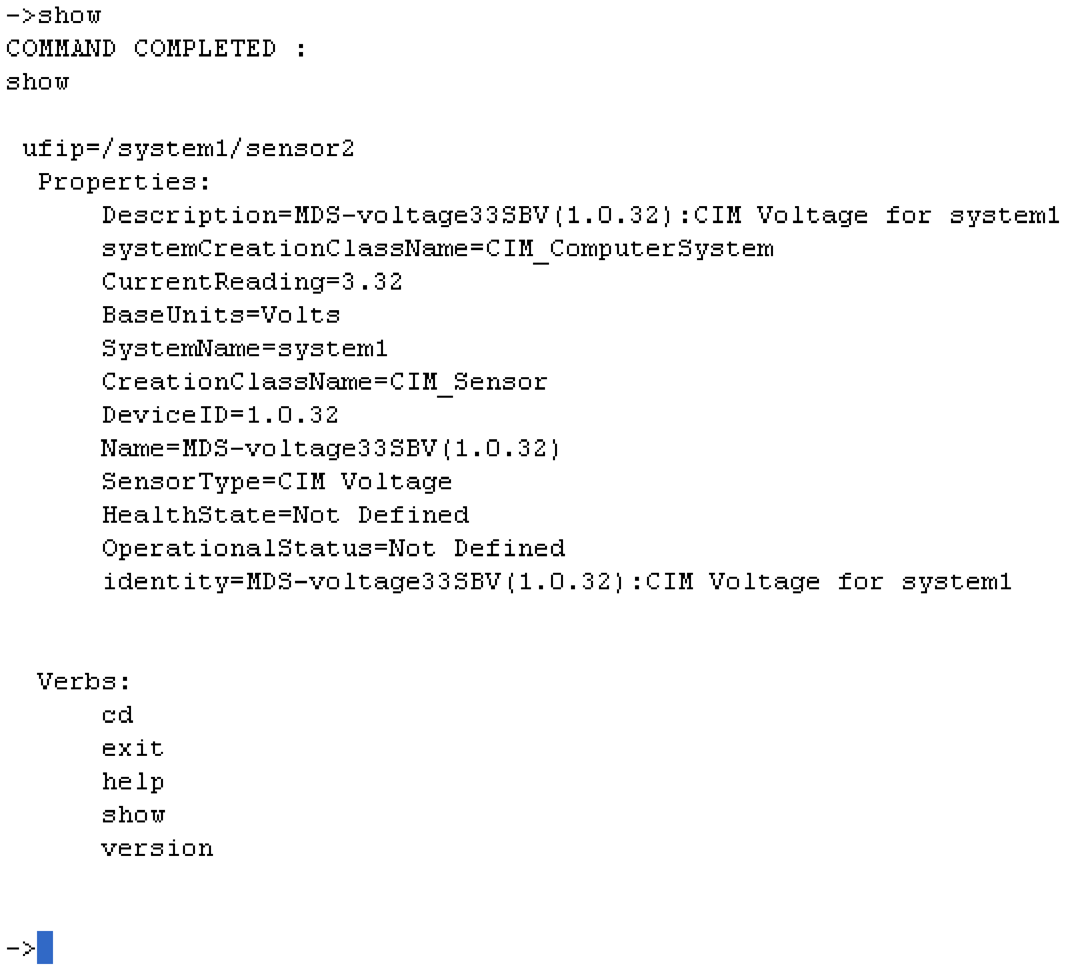
The verb help is used to provide information on using SMASH*.

8.15.2.4 show

The verb show is used to show all the targets, properties, and verbs supported by this target.

8.15.2.5 version

The verb version is used to 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 58. SENSOR2 Target

8.16 Targets Creation

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.

Appendix A. Intel® Server Issue Report Form

Issue Report Form (Rev 3.5)

NOTE: Filling out this form completely is required for any escalation.

Customer Contact Information:

Customer Support Case #:

Intel® Server Board or System:

(Example : S5000PSL or SR6850HW4)

Server Chassis:

(Example SC5400. If third party chassis used, indicate make and model.)

Base Board Information: (some information maybe found by accessing BIOS & going through the Server Management menu -> System Information)

Baseboard PBA/TA/AA # (Example: 123456-789):

- can be found on the white sticker label on the baseboard

System BIOS Version:

Intel® Remote Management Module Firmware Version (if applicable):

Intel® Management Module BMC Revision (if applicable) :

BMC/mBMC Version:

FRU/SDR Version:

HSC Version:

Has the latest BIOS been tried? (Yes/No):

Has the latest BMC/mBMC been tried? (Yes/No):

Has the latest IMM BMC been tried? (Yes/No):

Has the latest RMM Firmware been tried? (Yes/No):

Has the latest FRU/SDR been tried? (Yes/No):

Has the latest HSC been tried? (Yes/No):

Processor information:

	Type	Speed	sSpec	Thermal Solution
Processor 1				
Processor 2				
Processor 3				
Processor 4				

Thermal solution (Heatsink) examples:
(1U, Passive w/air ducting, Active w/fan, etc.)

Memory:

Manufacturer	Part Number	DRAM Part Number	On Intel tested list?

Add-in adapters (Example: NICs, Management Adapters, Serial Expansion Cards, PCI-Express* Adapters, RAID Controllers, SCSI Controllers, etc.):

Type	Slot	Manufacturer	Model	Firmware

Other third part hardware (Example: Example: KVM, Chassis, etc):

Description/Use	Manufacturer	Model	Firmware

Storage Devices (Example: SCSI, SATA, SAS, USB, Tape, etc.):

Manufacturer	Model	Type	Size	Firmware	In Hot Swap Bay?

Operating System Information (Example: RedHat* Enterprise Linux, Microsoft* Windows* Server 2003, Service pack 1, OEM CD):

Manufacturer:

Version:

Language version (English, Arabic, Chinese (Simplified)):

Service Pack Level or Kernel Revision:

Distribution (OEM/Retail):

Intel® RAID Controller: (Example SRCU42E)

RAID controller part number (PBA number):

RAID controller firmware version:

Has the latest RAID firmware been tried? (Yes/No):

RAID driver version:

Has the latest RAID driver been tried? (Yes/No):

RAID volumes configuration (disks & RAID level):

RAID volume use (Boot device/Data Volume):

Is BBU (Battery Backup Unit) installed? (Yes/No):

BBU part number:

Detailed description of issue:

Troubleshooting tried:

Steps to replicate the issue:

Issue impact statements:

Do you have any potential Intel system, or component purchases that this issue is holding up? If yes, please provide a brief description below.

Do you have systems already purchased that are not being delivered to your customers because of this issue? If yes, please provide a brief description below.

Have you returned systems or components to your place of purchase because of this issue? If yes, please provide a brief description below.

*All other brands and names are property of their respective owners.