

# Intel<sup>®</sup> Remote Management Module User's Guide

**A Guide for Technically Qualified Assemblers of Intel<sup>®</sup> Identified Subassemblies/  
Products**

Intel Order Number D48601-001

## **Disclaimer**

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

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

Intel, Intel Pentium, and Intel Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2006, Intel Corporation. All Rights Reserved

# Safety Information

---

## Important Safety Instructions

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 on the *Intel® Server Deployment Toolkit CD 2.0* and/or at <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>.

## Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warnung und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die Sicherheitshinweise zu Intel-Serverplatinen und Servergehäusen auf der *Intel® Server Deployment Toolkit CD 2.0* oder unter <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>.

## 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 *Intel® Server Deployment Toolkit CD 2.0* ou bien rendez-vous sur le site <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>.

## 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 *Intel® Server Deployment Toolkit CD 2.0* y/o en <http://support.intel.com/support/motherboards/server/sb/cs-010770.htm>.

## 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。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》)。

## Warnings

**Heed safety instructions:** Before working with your 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.

**System power on/off:** The power button DOES NOT turn off the system AC power. To remove power from system, you must unplug the AC power cord from the wall outlet. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

**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 tool you use to remove a jumper, or you may bend or break the pins on the board.

# Preface

---

## About this Manual

Thank you for purchasing and using the Intel® Remote Management Module (Intel® RMM). This manual provides information for configuring the Intel® RMM and for using the Intel® RMM to manage the server system into which it is installed.

This manual does not include instructions for installing the Intel® Remote Management Module or the RMM NIC. See the instructions that came with your Intel® Server Board to install these components, then return to this guide.

## Manual Organization

Chapter 1 provides a brief overview of the Intel® Remote Management Module. In this chapter, you will also find a list system requirements.

Chapter 2 provides instructions for configuring the Intel® Remote Management Module using the command-line utility.

Chapter 3 provides instructions for configuring the Intel® Remote Management Module using the Intel® Remote Management Module Web Console interface.

Chapter 4 provides instructions for managing your server using the Intel® Remote Management Module Web Console interface. The managed server must have the Intel® Remote Management Module and the RMM NIC installed.

Chapter 5 provides instructions for remotely managing your server using the Intel® Remote Management Module Virtual Server Control application. The managed server must have the Intel® Remote Management Module and the RMM NIC installed.

Appendix A provides tables that show the commands, Intel® RMM settings, and return status codes.



# Contents

---

<b>Safety Information</b> .....	<b>iii</b>
Important Safety Instructions .....	iii
Wichtige Sicherheitshinweise .....	iii
Consignes de sécurité .....	iii
Instrucciones de seguridad importantes .....	iii
Warnings .....	iv
<b>Preface</b> .....	<b>v</b>
About this Manual .....	v
Manual Organization .....	v
<b>Chapter 1: Product Overview</b> .....	<b>1</b>
Minimum Operating System Requirements .....	3
Server System .....	3
Client System .....	3
<b>Chapter 2: Using the Intel® RMM Command Line Utilities to Configure the Intel® RMM</b> .....	<b>5</b>
Connecting with the Intel® RMM the First Time .....	6
Command Line Options .....	7
MMCONFIG Utility Commands .....	9
<b>Chapter 3: Using the Web Console Interface to Manage the Intel® RMM</b> .....	<b>13</b>
Accessing the Remote Server .....	13
Configuring Network Settings .....	14
To Configure or Update Host Settings .....	14
To Configure or Update Network Settings .....	14
Configuring Session Settings .....	15
Configuring User Settings .....	16
To Add a New User .....	16
To Edit a User .....	17
To Delete a User .....	17
Configuring Privileges Settings .....	18
Updating Firmware .....	19
<b>Chapter 4: Using the Web Console Interface to Manage the Server</b> .....	<b>21</b>
Accessing the Remote Server .....	21
Verifying Communication through Ping .....	22
Rebooting, Cycling System Power, and Turning off the Remote Server .....	23
Checking Discrete Sensors .....	24
Checking Numeric Sensors .....	25

Field Replacement Unit (FRU) .....	26
Entering IPMI Commands .....	27
<b>Chapter 5: Using the Intel® Remote Management Module Virtual Server Control Application to Manage the Server .....</b>	<b>29</b>
Accessing the Remote Server .....	30
Interacting With the Server .....	31
Intel® Remote Management Module Virtual Media .....	33
Intel® Remote Management Module Virtual Media Dialog Box .....	33
Connecting a Generic Mass Storage Device .....	33
Connecting a CD-ROM or DVD-ROM Drive .....	34
Viewing the Connected Device Status .....	34
Operating the Device Remotely .....	34
<b>Appendix A: Command Syntax and Return Status Codes .....</b>	<b>35</b>
Command Syntax .....	35
Config Server Commands .....	36
Return Status Codes .....	45



# List of Tables

---

Table 1. Intel® Remote Management Module Features .....	2
Table 2. Video Resolutions / Refresh Rates .....	4
Table 3. Command Line Options .....	7
Table 4. Privileges .....	18
Table 5. Virtual Server Control Macro Options .....	32
Table 6. Command Syntax .....	35
Table 7. Config Server Commands .....	36



# List of Figures

---

Figure 1. Login Page .....	13
Figure 2. Network Page.....	14
Figure 3. Session Page .....	15
Figure 4. User Management Page .....	16
Figure 5. Privileges Page .....	18
Figure 6. Firmware Update Page .....	19
Figure 7. Login Page .....	21
Figure 8. Ping Device Page.....	22
Figure 9. System Power/Reboot Page .....	23
Figure 10. Discrete Sensors Page .....	24
Figure 11. Numeric Sensors Page .....	25
Figure 12. Field Replaceable Unit (FRU) Page.....	26
Figure 13. IPMI Page .....	27
Figure 14. Login Page .....	30
Figure 15. Remote Server Desktop Through Intel® RMM Virtual Server Control .....	31
Figure 16. Intel® RMM Virtual Media Dialog .....	33



# 1 Product Overview

---

This chapter describes the main features of the Intel® Remote Management Module (Intel® RMM) and provides information about the operating system requirements to configure the Module and manage the server with it.

The Intel® Remote Management Module is a component of a server system that consists of an Intel® server board and chassis and a RMM NIC. The Intel® Remote Management Module and the RMM NIC plug into connectors on the Intel server board, acting as components of the server board instead of as separate products.

The primary goal of the Intel® Remote Management Module and the RMM NIC is to create easy access to a server, even if it is at a remote location. These products provide a way to look at and operate the remote server's desktop in real-time. Mouse movements and clicks, and keyboard keystrokes are transmitted to the managed server from the remote workstation.

Using Virtual Media capabilities, it is also possible to run local media, such as a CD-ROM disk, on the remote server. For example, the user can insert a CD-ROM disk that contains an installation program in the local system and use a Virtual Media session to run the installation on the remote server.

The Intel® Remote Management Module and the RMM NIC use a dedicated network controller that is always on, as long as the server is attached to a power supply. This dedicated network controller is for server management purposes only. It is separate and independent from all other network controllers provided by the server. Since the Intel® Remote Management Module network controller is dedicated to management, it is not available to the operating system. Operating systems cannot see it.

Table 1 summarizes the major features of the Intel® Remote Management Module.

**Table 1. Intel® Remote Management Module Features**

Feature	Description
Graphical User Interface	Manage the remote Intel® Remote Management Module using the Intel® Remote Management Module Web Console, an embedded web-based graphical user interface that lets you perform many server configuration and management functions. It also lets you interactively use the keyboard, video, and mouse (KVM) functions of the remote server as if you were physically at the managed server.
Control of Virtual Media	The Intel® Remote Management Module Virtual Media functionality allows you to apply programs and data to the remote server, even when those programs and data are physically located at a client workstation. For example, you can run an installation program that is located on a client CD, DVD, floppy disk, USB device, or ISO images to install the program on the managed server. This feature enables you to install operating systems, recover hard drives, and back up servers, to name a few examples.
Reporting of Server Board Sensors	From the Intel® Remote Management Module Web Console, you can check the status of all server board sensors, discrete and numeric, allowing you to diagnose most problems remotely, as if you were physically at the managed server.
Control of System Power	The Intel® Remote Management Module Web Console allows you to cycle the power, power up, or power down a remote managed server.
Username and Password	The remotely managed server is user name and password protected. Access is prohibited until you enter a valid user name and password.
FLASH Upgrade	The Intel® Remote Management Module is upgradable through FLASH to ensure that it is always running with the most current firmware. The firmware upgrade ensures that the FLASH upgrades safely and correctly by running a series of checks throughout the download and installation process.

# Minimum Operating System Requirements

## Server System

The following operating systems are supported on the managed server:

- Microsoft Windows\* 2003 Server with Service Pack 1 or later and all recent updates
- Red Hat\* Enterprise Linux Advanced Server 4

## Client System

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

- Red Hat\* Linux 4 ES with Firefox
- SuSE\* 9 Pro 9.1 with Mozilla
- Microsoft Windows\* XP Pro with Service Pack 2 and with Internet Explorer
- Microsoft Windows\* 2003 ES with Service Pack 1 and with Internet Explorer

The following video resolutions and refresh rates are supported:

**Table 2. Video Resolutions / Refresh Rates**

<b>Resolution</b>	<b>Refresh Rate</b>
640 x 480	60 Hz
	72 Hz
	75 Hz
	85 Hz
	100 Hz
800 x 600	60 Hz
	72 Hz
	75 Hz
	85 Hz
1024 x 768	60 Hz
	72 Hz
	75 Hz
	85 Hz
1280 x 960	60 Hz
1280 x 1024	60 Hz



## 2 Using the Intel<sup>®</sup> RMM Command Line Utilities to Configure the Intel<sup>®</sup> RMM

---

The Intel<sup>®</sup> RMM can be configured and updated with a set of command line utilities. The command line utilities locally use the USB interface of the server or remotely use the TCP/IP interface of the management NIC of the Intel<sup>®</sup> RMM. The utility programs run native on Windows and Linux.

The utility programs have the following basic features, all accessible from the command line:

- Read one or more settings and display them
- Write one or more settings from the command line
- Update the Intel<sup>®</sup> RMM firmware
- Reset all Intel<sup>®</sup> RMM settings to factory defaults

On each operating system platform, a single utility, called “mmconfig”, accomplishes the above functions. The utility provides access through either a local USB interface or through a remote SSL connection to the Intel<sup>®</sup> RMM. The mode of access (USB or remote) is determined by the first command on the command line. The default is local USB access, unless the first command is `-a`, followed by the IP address of the Intel<sup>®</sup> RMM NIC, indicating remote access. The `-a` command is only valid when specified as the first command on the command line.

# Connecting with the Intel® RMM the First Time

When the Intel® RMM is attached to an Intel server for the first time, the Intel® RMM will attempt to obtain an IP address for its built-in management NIC from a DHCP server attached to the network. If there is no DHCP server that the Intel® RMM can get its IP address from, or if the DHCP server fails to assign the Intel® RMM a valid IP address, then the Intel® RMM's IP address will default to 192.168.0.122. It is important to know the IP address associated with the Intel® RMM because it is with this IP address that a user can access the Intel® RMM with the remote utilities and the Intel® RMM Web Console.

Obtaining the IP address from the DHCP server is the factory default setting for the Intel® RMM. If the Intel® RMM is connected to a DHCP server and obtains its IP address from DHCP, then the user can use the mmconfig utility locally to find out the IP address assigned to the Intel® RMM by the DHCP server.

To connect with the Intel® RMM for the first time, boot the server to Windows or Linux.

- For Linux: Copy the Linux version of mmconfig in the root directory. At the root prompt, enter:

```
./mmconfig -g lan3/ipaddr
```

The mmconfig utility returns the IP address of the Intel® RMM.

- For Windows: Copy the Windows version of mmconfig into the C: directory. Open a DOS prompt window and navigate to the C: directory. At the C: prompt, enter:

```
mmconfig -g lan3/ipaddr
```

The mmconfig utility returns the IP address of the Intel® RMM.

This IP address can then be used to access the Intel® RMM Web Console remotely or to run the mmconfig utility remotely.

In addition to using the utilities, the Intel® RMM can be configured and updated through the Intel® RMM web console. Logging into the web server involves opening a browser on the client computer and typing the IP address of the Intel® RMM's NIC into the address bar. For example: If the IP address of the Intel® RMM NIC is 192.168.0.122, enter: <https://192.168.0.122/> in the address bar of the web browser to launch the Intel® RMM Web Console.

The Intel® RMM does not require user authentication for local utility USB access, but remote utility access always requires user authentication.

To connect to the utility remotely:

```
mmconfig -a 192.168.0.122 -u admin -p password -i
```

returns:

```
OK
00.00.79
```

00.00.79 indicates that the current version of Intel® RMM firmware is 79.

The remote command requires -a followed by the IP address of the Intel® RMM management NIC. The remote command also requires user authentication by “logging in” with a valid user name and password. In the example above, the user name and password used is the default: admin and password.

The equivalent command executed locally at the server is:

```
mmconfig -i
```

returns:

```
OK
00.00.79
```

Intel recommends that you change the password and that you write down the new username and password and store this information in a secure place.

**Note:** *If you lose your password, you can go to the server and run the mmconfig utility locally to reset the Intel® RMM to factory defaults with the command: mmconfig -s ctrl/default\_settings = 1. Then you can log into the Intel® RMM with the default user name and password “admin” and “password”.*

## Command Line Options

The following section defines the command line options. More than one option can be included on the command line. The options are processed in order. See “Return Status Codes” on page 45 for return status codes.

**Table 3. Command Line Options**

Function	Command-line Option
To test the host to Intel® RMM USB packet interface	-t {text string}
To specify a user name to login under	-u {username}
To specify a password (must follow the user name)	-p {password}
To set a value	-s {SettingName}={SettingValue}
To set value to that value’s default	-s {SettingName}=
To set all settings to factory defaults	-s CTRL/DEFAULT_SETTINGS=1
To display (get) a value	-g {SettingName}

**Table 3. Command Line Options**

Function	Command-line Option
To display the Intel® RMM's current firmware version information	-i
To upgrade the firmware on an Intel® RMM with a single command (this command performs a firmware image file upload to the RMM, verifies the integrity of the image file, writes the firmware update to the flash memory and reboots the Intel® RMM)	-f {ImageFileName}
To enable execution of subsequent commands in a local batch file if an error occurs (default mode is to discontinue subsequent commands)	-e
To disable responses from being sent to stdout during execution of subsequent options contained on the same command line, or subsequent command lines in a local batch file being executed (this is quiet mode; only the completion code will be returned)	-q
To cause subsequent commands in a batch file to be echoed to stdout before execution (noisy mode)	-n
To cause reboot of the Intel® RMM	-b
To run a script file on the local system (dash command-line format)	-x {FileName}
To check a firmware update file to verify that the file is the proper file type and format	-c {ImageFileName}
To specify an IP address and switch from the default USB transport to an SSL Sockets transport (note: this command is invalid unless it is the first command, and it will persist until the MMCONFIG utility terminates)	-a {IP address in dot-separated decimal form}
To maintain a persistent connection (the utility provides the command prompt)	-m
To close a persistent connection (utility exits)	-quit
To display version and build information of the command-line utility	-version
To display all command line options and switches (operator help function)	-h or -?

**Note:** User names, passwords and file names must not contain a leading dash character (“-“) to provide better syntax error checking.

# MMCONFIG Utility Commands

The Config Server is the firmware engine for setting and getting configuration parameters on the Intel® RMM. It implements the Get and Set portions of the CLI commands (-s and -g). In the appendix you will find list of commands a user can execute. See “[Config Server Commands](#)” on page 36.

All parameter values are treated as ASCII NULL terminated string values by the command line tool and USB interface. All commands are in the form of:

```
Mmconfig -option object/<instance>/attribute=value
```

Instance is usually optional and is only needed for user objects. Command strings are case-insensitive except for user names and passwords, which are case-sensitive. All filenames sent to the Intel® RMM Config Server are case-insensitive. “SUCCESS” or “OK” are the default successful replies and error reply messages begin with “ERROR:”

## Examples

A typical local (via USB) session to GET and then SET the IP Address of the management NIC on the Intel® RMM looks like:

```
MMConfig -g LAN3/IPADDR
```

Reply is

```
192.168.0.101
```

```
MMConfig -s LAN3/IPADDR=192.168.0.50
```

Reply is

```
OK
```

**Note:** *Changing the IP address of the Intel® RMM takes one minute after entering the command above.*

A typical remote (via TCP in which the Intel® RMM card IP Address is 192.168.0.101) session to GET and then SET the IP Address looks like:

```
MMConfig -a 192.168.0.101 -u admin -p password -g LAN3/IPADDR
```

Reply is:

```
OK
```

```
OK
```

```
192.168.0.101
```

```
MMConfig -a 192.168.0.101 -s LAN3/IPADDR=192.168.0.50
```

Reply is:

```
OK
```

```
OK
```

A typical session to add a user:

```
MMConfig -s USER/NAME=Bob
```

Reply is:

OK

```
MMConfig -s USER/Bob/NEW_PASSWORD=BobPassword
```

Reply is:

OK

To change user Bob to Bobby:

```
MMConfig -g USER/COUNT
```

Reply is

2

```
MMConfig -g USER/2/NAME
```

Reply is

Bob

```
MMConfig -s USER/2/NAME=Bobby
```

Reply is:

OK

A typical session to run the LAN3 self test looks like:

```
MMConfig -s SELF_TEST/SUBCOMPONENT=7
```

Reply is:

OK

```
MMConfig -s SELF_TEST/LAN_MODE=1
```

Reply is:

OK

```
MMConfig -s SELF_TEST/LAN_PEER_ADDR=192.168.1.15
```

Reply is:

OK

```
MMConfig -s SELF_TEST/CONTROL=1
```

Reply is:

OK

```
MMConfig -g SELF_TEST/STATUS
```

Reply depends on status and is:

0-4

```
MMConfig -g SELF_TEST/REASON
```

Reply depends on type of failure and is:

0-4

Changing or creating any user account settings remotely requires that a tool or a user log in using a username and password of an account that has ADMIN privileges, before any parameter value changes will be accepted. New account creation and deletion remotely is only allowed for accounts with the ADMIN privilege.

One of the features of the Intel<sup>®</sup> RMM's local and remote utilities is the ability to invoke a self test of the Intel<sup>®</sup> RMM. The following interfaces are tested by the Intel<sup>®</sup> RMM Self Test:

- FML to the BMC
- IPMB
- USB
- DVO
- LAN

The Fast Management Link (FML) is a high speed (8 Mb/s) point-to-point interface between the Intel<sup>®</sup> RMM and the BMC within the Intel<sup>®</sup> 631xESB / 632xESB I/O Controller Hub. For the FML to the BMC self test, the Intel<sup>®</sup> RMM FML interface sends a "Status Request" to the BMC and waits up to one second for a reply. This test exercises the data and control signals of the FML interface. If a valid response is returned from the BMC in the allowed time, the test passes. If a valid response is not returned in time, then the test fails.

Testing the DVO interface involves a test to check if the internal KVM firmware is running. If the KVM firmware is running, then the self test will generate a signal that will be accepted by the KVM firmware. As a result of accepting the signal, the KVM firmware will create a file in the /tmp directory of the firmware's file system. The file will contain a "detected video" if the signal was detected. Otherwise, the test fails.

Testing the IPMB with the Intel<sup>®</sup> RMM's self test involves sending the BMC an IPMI command via the IPMB. If a response is received from the BMC, then the IPMB is working. Receiving no response from the BMC indicates that IPMB test failed.

The USB interface of the Intel<sup>®</sup> RMM is a "target only" to the USB host controller embedded in the Intel<sup>®</sup> 631xESB / 632xESB I/O Controller Hub. There is no way for the Intel<sup>®</sup> RMM to initiate USB traffic. Therefore, testing the USB interface consists of receiving a read request from the USB host controller over the USB and successfully responding to it. The Intel<sup>®</sup> RMM self test can keep track of this occurrence to indicate a

passing test. Within the MMconfig utility, the `-t echo` command can be used to initiate this read request traffic on the host. If the Intel® RMM successfully returns an echo, the USB interface is working correctly.

The self test for the Intel® RMM's LAN interface involves:

- Checking to see if the LAN interface can ping the internal loop back IP address of 127.0.0.1. If that address does not respond to the ping, the self test fails and returns an error code of 4.
- Checking to see if the Ethernet controller exists. Otherwise the self test fails and returns an error code of 3.
- Checking to see if the LAN interface can ping the external IP address assigned to the Intel® RMM's NIC. If that address does not respond to the ping, the self test fails and returns an error code of 2.
- Checking to see that the proper Ethernet interface firmware is running. If not, the self test fails and returns an error code of 1.

The second FML (NIC interface) is not tested because it is not used by the Intel® RMM. The serial interface is not tested because there is no way to force the system to output data to the serial port.



# 3 Using the Web Console Interface to Manage the Intel® RMM

---

You may perform almost all configuration functions through your web browser. This chapter discusses the following topics:

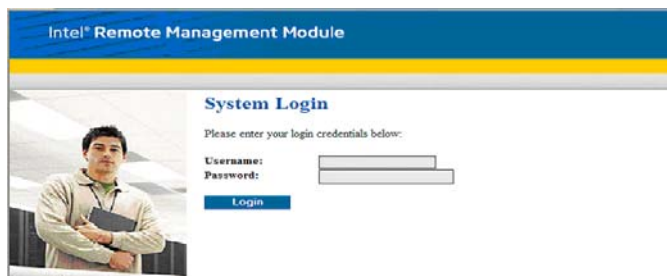
- “Accessing the Remote Server”
- “Configuring Network Settings”
- “Configuring Session Settings”
- “Configuring User Settings”
- “Configuring Privileges Settings”
- “Updating Firmware”

## Accessing the Remote Server

You can access the Intel® RMM remotely through your web browser, making it possible to do almost any configuration or management task as if you were physically present at the server.

To access the Intel® RMM through your browser:

1. Open your web browser.
2. Enter the server's URL into the address bar. For example, enter https://192.168.0.122. The Intel® Remote Management Module displays the login page.



**Figure 1. Login Page**

3. Enter your User Name and Password in the appropriate fields and click Login. The Intel® RMM displays the System Summary page.

## Configuring Network Settings

Through the web interface, you can configure the host and network settings that the remote Intel® RMM will use. You may use a static IP address, or have the DHCP automatically assign an IP address. If you have multiple servers on the same network, each with an Intel® RMM, you may want to rename the host name to a unique name so that the DNS can associate each server.

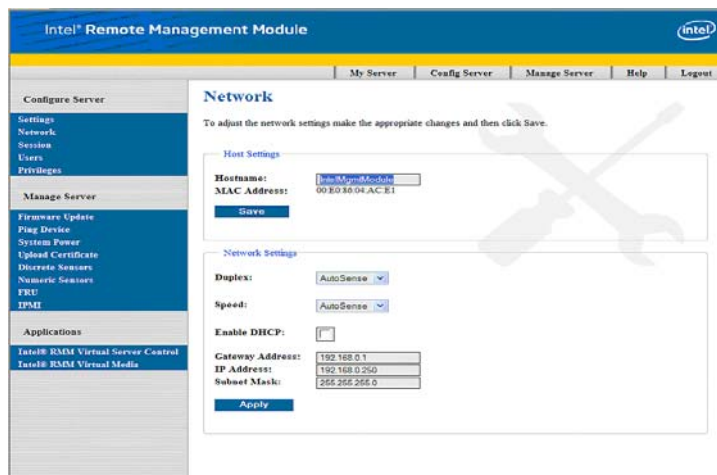


Figure 2. Network Page

### To Configure or Update Host Settings

1. Under Configure Server on the left side of the System Summary page, click Network. Your browser displays the Network page.
2. Enter the host name of the Intel® RMM in the Host Name field. The default name is IntelRMM. The MAC address for your individual Intel® RMM is in the MAC address field.
3. Click Save.

### To Configure or Update Network Settings

1. Under Configure Server on the left side of the System Summary page, click Network. Your browser displays the Network page.
2. In the Duplex field, select AutoSense, Full, or Half from the drop-down menu.
  - Full refers to allowing network traffic in both directions simultaneously.
  - Half refers to allowing network traffic in both directions, but only one direction at a time.
  - Autosense will automatically select a setting.

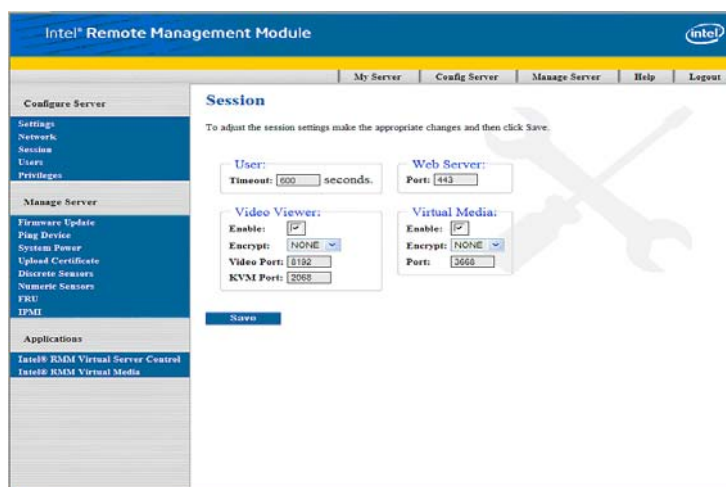
**Note:** If you have previously changed the IP address from the default through DHCP, mmconfig, or the Network Settings web page, and the DHCP server subsequently fails to assign an IP address, the Intel® Remote Management Module defaults to IP address 192.168.0.122.

3. In the Speed field, select the LAN speed: Autosense, 100mb, or 10mb from the drop-down menu. Autosense will automatically select a setting.
4. DHCP (Dynamic Host Configuration Protocol) is enabled by default, allowing your remote Intel® RMM to automatically retrieve an IP address if your subnet has a DHCP server. If you would like to disable this feature and assign a network address for the Intel® RMM yourself, uncheck the Enable DHCP box. The Gateway Address, IP Address, and Subnet Mask Address fields will become activated for you to enter your choices manually.

**Note:** If your Intel® RMM is on a subnet that has no DHCP server, the Intel® RMM defaults to the static IP address of 192.168.0.122. If you select disable DHCP and then enable it again after you click Apply, your new IP address will display in the address bar. This IP address will replace your previous IP address.

## Configuring Session Settings

Through the web interface, you can choose to adjust settings for User Timeout, Web Server, Video Viewer, and Virtual Media sessions. These adjustments include port numbers and enable/disable toggles. This page is important because some networks may block the usage of certain ports. Since the ports used by the Intel® RMM are reconfigurable, they can be changed to port numbers accessible in your environment.



The screenshot shows the Intel Remote Management Module web interface. The top navigation bar includes 'My Server', 'Config Server', 'Manage Server', 'Help', and 'Logout'. The left sidebar lists various configuration categories: 'Configure Server' (Settings, Network, Session, Users, Privileges), 'Manage Server' (Firmware Update, Plug Device, System Power, Upload Certificate, Discrete Sensors, Numeric Sensors, FRU, IPMI), and 'Applications' (Intel® RMM Virtual Server Control, Intel® RMM Virtual Media). The main content area is titled 'Session' and contains the following settings:

- User:** Timeout: 600 seconds.
- Web Server:** Port: 443.
- Video Viewer:** Enable: ; Encrypt: NONE; Video Port: 5192; KVM Port: 2068.
- Virtual Media:** Enable: ; Encrypt: NONE; Port: 2668.

A 'Save' button is located at the bottom of the configuration area.

Figure 3. Session Page

To configure Session settings:

1. Under Configure Server on the left side of the Server Configuration page, click Session. Your browser displays the Session page.
2. Select Enable for each of the types of sessions you would like to use and select the appropriate port number. On the Video Viewer and Virtual Media, you may also choose to encrypt the data.
3. Click Save.

## Configuring User Settings

Through the web interface, you can add and edit users, and administer the passwords and privilege levels of each.

**Note:** You should change the default username, “admin” and the default password, “password” as soon as possible.

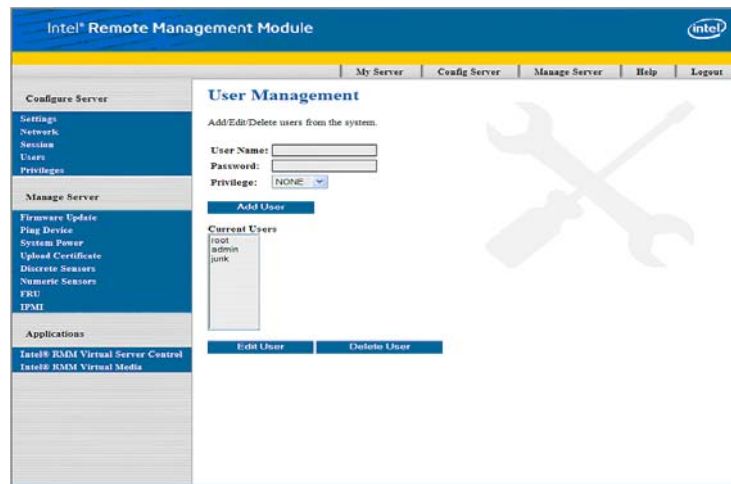


Figure 4. User Management Page

## To Add a New User

1. Under Configure Server on the left side of the Server Configuration page, click Users. Your browser displays the User Management page.
2. Enter the name of a new user in the field provided.
3. Enter the password of the new user in the field provided.
4. From the drop-down menu, select a privilege level.
5. Click Add User.

## To Edit a User

1. Under Configure Server on the left side of the Server Configuration page, click User. Your browser displays the User Management page.
2. Under Current Users, select an existing user.
3. Click Edit User. The user's name will appear in the User Name field.
4. If you would like to change the password, enter a new password in the field provided.
5. If you would like to change the privilege level of user, from the drop-down menu, select a privilege level.
6. Click Update User.

## To Delete a User

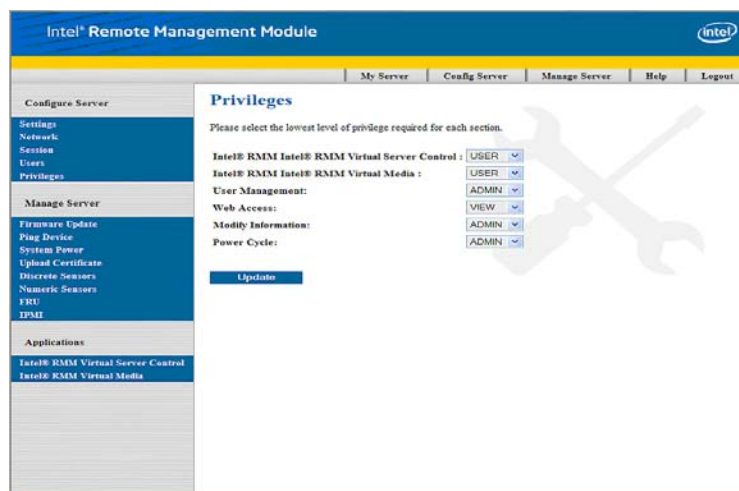
1. Under Configure Server on the left side of the Server Configuration page, click User. Your browser displays the User Management page.
2. Under Current Users, select an existing user. The user's name will appear in the User Name field.
3. Click Delete User.

# Configuring Privileges Settings

Through the web interface, you can add and edit users, and administer the passwords and privilege levels.

**Table 4. Privileges**

Privilege	Description
ADMIN	Administrator level users are allowed. No restriction on allowed commands.
USER	Commands that change users configuration are restricted.
VIEW	Commands are restricted to read-only access of system information.
NONE	Setting this privilege level to a feature, disables the feature.



**Figure 5. Privileges Page**

To set privileges for web interface capabilities:

1. Under Configure Server on the left side of the Server Configuration page, click Privileges. Your browser displays the Privileges page.
2. For each of the web interface's capabilities, enter the lowest level of privilege you would like. For example, if you would like to allow all users for the Video View, select User from the drop-down menu; if you want to restrict that capability to administrators, select ADMIN from the drop-down menu.
3. Click Update.

# Updating Firmware

You can easily update your Intel Remote Management Module's firmware to keep it current.

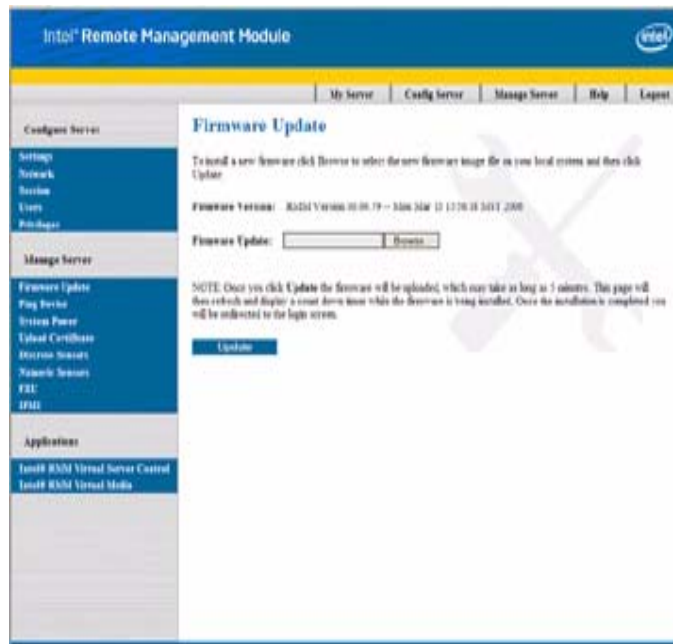


Figure 6. Firmware Update Page

1. Using your web browser, download the most recent firmware update from the Intel web site.
2. Under Manage Server on the left side of the Server Configuration page, click Firmware Update. Your browser displays the Firmware Update page.
3. Click Browse to find the firmware file that you downloaded.
4. Click Update. Your local system will download the firmware update to the remote system. When the installation process begins, the installation program will display a timer. Once the installation is complete, you will be redirected to the login screen.

The Firmware Update program ensures that the update has not been corrupted: it checks the update repeatedly through the process. If, however, there is a power interruption while the update is being written to the The Intel<sup>®</sup> Remote Management Module, the board may be damaged.





# 4 Using the Web Console Interface to Manage the Server

---

You may perform almost all configuration functions through your web browser. This chapter discusses the following topics:

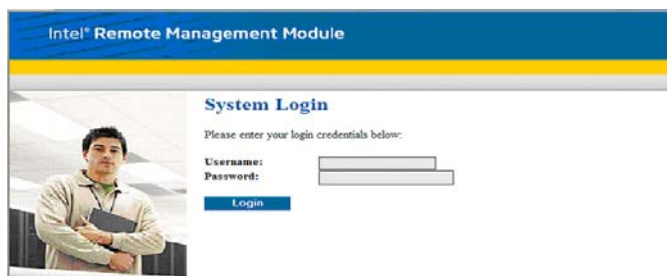
- “Accessing the Remote Server”
- “Verifying Communication through Ping”
- “Rebooting, Cycling System Power, and Turning off the Remote Server”
- “Checking Discrete Sensors”
- “Checking Discrete Sensors”
- “Checking Numeric Sensors”
- “Field Replacement Unit (FRU)”
- “Entering IPMI Commands”

## Accessing the Remote Server

You can easily access the Intel® Remote Management Module remotely through your web browser, making it possible to do almost any configuration or management task as if you were physically present at the server.

To access the Intel® RMM through your browser:

1. Open your web browser.
2. Enter the server's URL into the address bar.

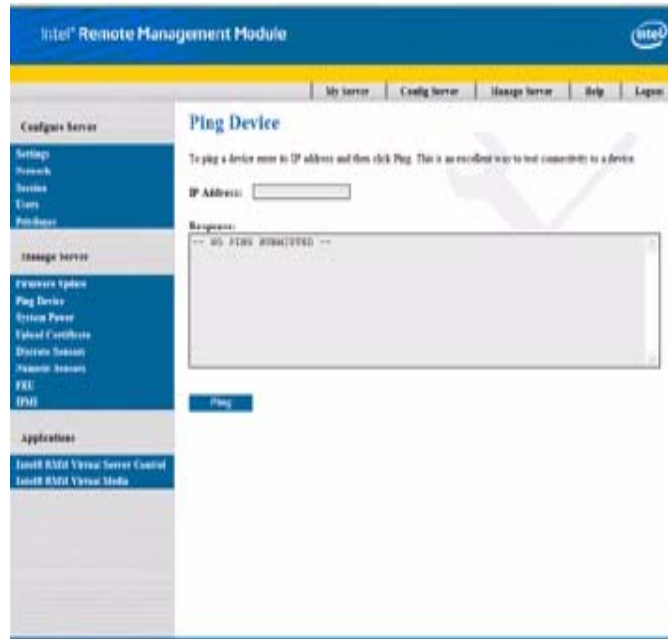


**Figure 7. Login Page**

3. Enter your User Name and Password in the appropriate fields and click Login. The management module displays the Server Configuration page.

## Verifying Communication through Ping

If you are experiencing a problem communicating with the remote server, you may verify the connectivity by pinging the device. With this tool you may also ping any other device as well.



**Figure 8. Ping Device Page**

To verify communication with the remote server by pinging it:

1. Under Manage Server on the left side of the Server Configuration page, click Ping Device. Your browser displays the Ping Device page.
2. Enter the IP address of the remote server you wish to ping into the IP Address field.
3. Click Ping. The server's response will display in the Response field.

# Rebooting, Cycling System Power, and Turning off the Remote Server

You can easily reboot Intel® Remote Management Module, cycle the power, or turn off the remote server.

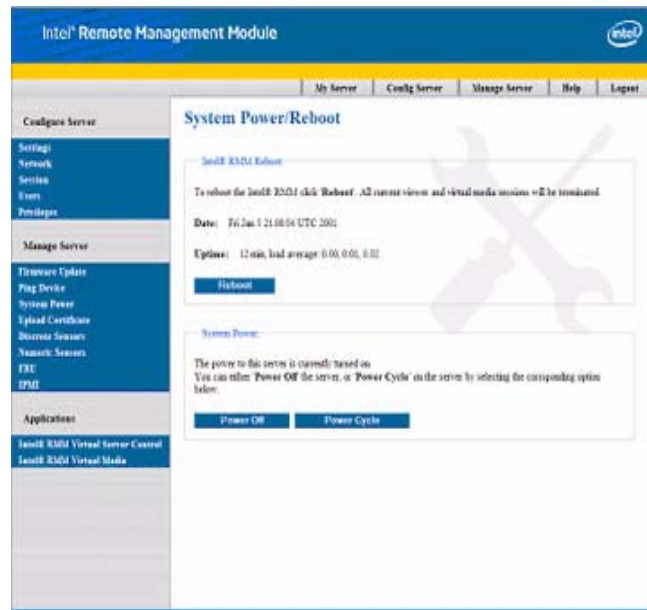


Figure 9. System Power/Reboot Page

To reboot the Intel® RMM, cycle the power, or to turn on or off the remote server:

1. Under Manage Server on the left side of the Server Configuration page, click System Power. Your browser displays the System Power/Reboot page.
2. Execute the desired task:
  - Click Reboot to restart the Intel® RMM.
  - Click Power Cycle to turn the server's power off and turn it on again, (hard reboot).
  - If the server is powered on, click Power Off to turn off the power on the remote server.
  - If the server is powered off, click Power On to turn on the power on the remote server.

**Note:** If you want to reset the server (not just the Intel® Remote Management Module), then through the video viewer session and KVM features, you can use the desktop functionality of the server, (see [Chapter 5, “Using the Intel® Remote Management Module Virtual Server Control Application to Manage the Server”](#)).

# Checking Discrete Sensors

Discrete sensors tell you about the health of the remote server with which you are communicating. (For a list of the sensors supported by the Intel<sup>®</sup> Remote Management Module, see the Technical Product Specification).

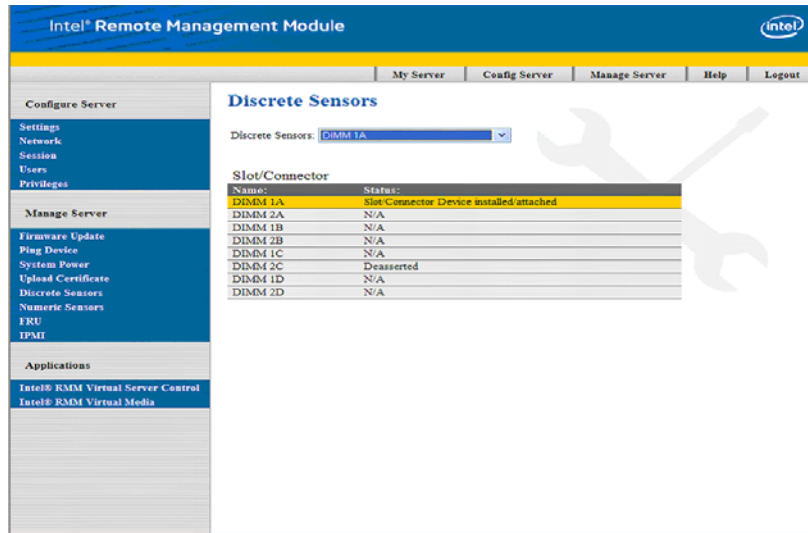


Figure 10. Discrete Sensors Page

To check discrete sensors:

1. Under Manage Server on the left side of the Server Configuration page, click Discrete Sensors. Your browser displays the Discrete Sensors page.
2. Choose a sensor for the Discrete Sensors drop-down menu. The status of the sensor you chose will display on the Discrete Sensors page beneath the menu.

# Checking Numeric Sensors

Numeric sensors tell you about the health of the remote server with which you are communicating. (For a list of the sensors supported by the Intel<sup>®</sup> Remote Management Module, see the Technical Product Specification).

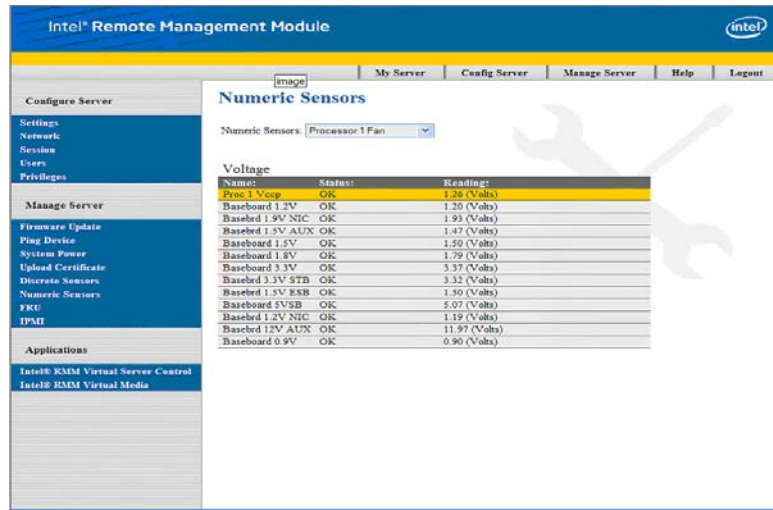


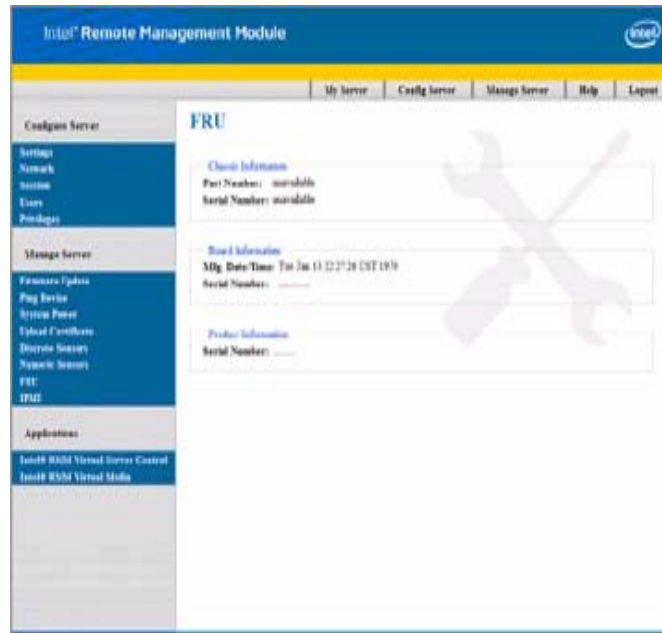
Figure 11. Numeric Sensors Page

To check numeric sensors:

1. Under Manage Server on the left side of the Server Configuration page, click Numeric Sensors. Your browser displays the Numeric Sensors page.
2. Choose a sensor for the Numeric Sensors drop-down menu. The status of the sensor you chose will display on the Numeric Sensors page beneath the menu.

# Field Replacement Unit (FRU)

You may check FRU information for the remote unit with which you are communicating. This information includes chassis and server board information, such as the part number, the serial number, the manufacture date and time, and the board language.



**Figure 12. Field Replaceable Unit (FRU) Page**

To check Field Replacement Unit (FRU) information:

Under Manage Server on the left side of the Server Configuration page, click FRU. Your browser displays the FRU page. The Field Replacement Unit information is displayed.

# Entering IPMI Commands

Under normal conditions, you do not need to enter IPMI commands. However, in some circumstances, you may be directed by an Intel support technician to use this feature. For a list of the IPMI hex commands, see the Technical Product Specification for your server board / chassis, and the Intelligent Platform Management Interface Specification.

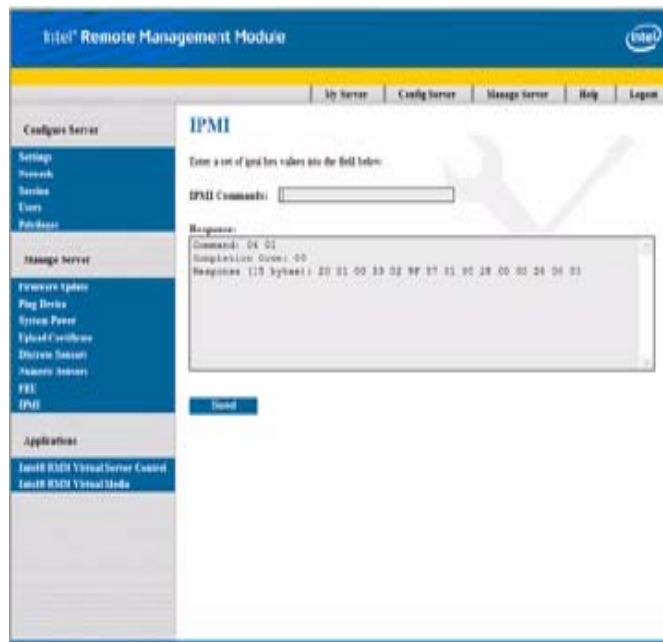


Figure 13. IPMI Page

To enter IPMI commands:

1. Under Manage Server on the left side of the Server Configuration page, click IPMI. Your browser displays the IPMI page.
2. Enter the IPMI command into the IPMI Commands field.
3. Click Send. The system will return a response in the Response field.

## Example

To get Device ID information, enter: 06 01 and the Response field will have the IPMI Device ID information of the BMC.





# 5 Using the Intel<sup>®</sup> Remote Management Module Virtual Server Control Application to Manage the Server

---

The Intel<sup>®</sup> Remote Management Module allows you to manage servers and media such as CD's from a remote location. Using the Intel<sup>®</sup> Remote Management Module Virtual Media dialog box in conjunction with the Intel<sup>®</sup> Remote Management Module Virtual Server Control viewer, you can operate virtual media sessions that allow you to boot from a remote disk, perform recovery operations, and manage operating system installation, to name a few examples.

You may perform almost all configuration functions through your web browser. This chapter discusses the following topics:

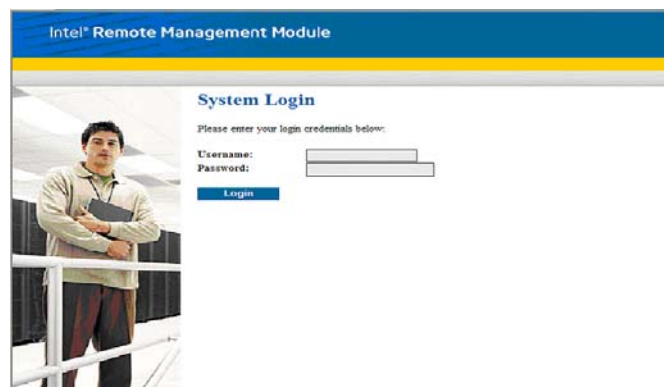
- [“Accessing the Remote Server”](#)
- [“Interacting With the Server”](#)
- [“Intel<sup>®</sup> Remote Management Module Virtual Media”](#)
- [“Intel<sup>®</sup> Remote Management Module Virtual Media”](#)

## Accessing the Remote Server

You may easily access your remote server through your web browser, making it possible to do almost any configuration or management tasks as if you were physically present at the server.

To access the remote server through your browser:

1. Open your web browser.
2. Enter the IP address of the Intel® Remote Management Module into the address bar. (For example, type https://192.168.0.2). The Intel® Remote Management Module displays its login page.



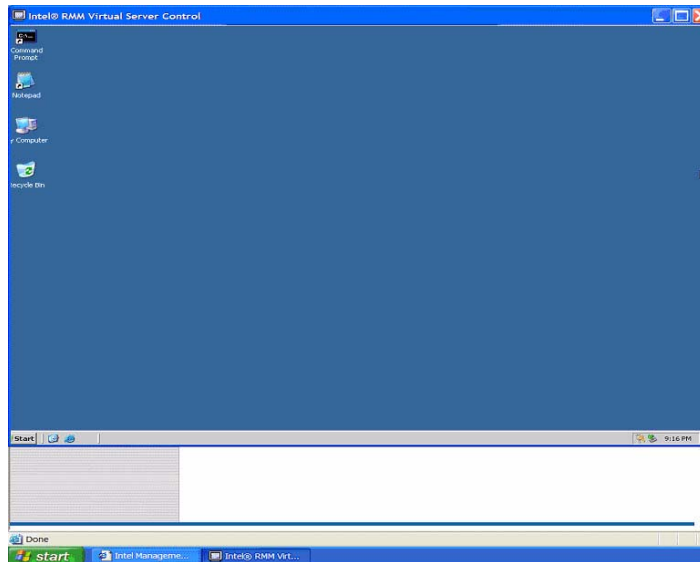
**Figure 14. Login Page**

3. Enter your User Name and Password in the appropriate fields and click Login. The management module displays the Server Configuration page.
4. Under Applications on the left-hand side of your screen, click the Intel® RMM Virtual Control button. The Intel® Remote Management Module displays the remote server's desktop in a window on your screen.

**Note:** You must have Java Runtime environment (JRE) 1.4.2 or higher on your client.

## Interacting With the Server

Once you have connected to the server, you will see its desktop on your screen. This desktop opens in a separate window where you will see two cursors: your client's cursor and the remote server's cursor. You control both cursors through your local mouse. Using the menu to substitute some keyboard operations through keyboard macros, such as Alt and Ctrl keys, you will be able to access all of the functions of this server as if you were physically present at the server.



**Figure 15. Remote Server Desktop Through Intel® RMM Virtual Server Control**

On the remote server's desktop, you will find a menu bar at the top of the screen. This menu bar allows you to use your mouse to make selections.

To access the remote server through your browser:

1. Click on the menu, using the remote server's cursor. The menu will drop down.
2. Make any selection, using the remote cursor.

To perform commands on the remote server, use the keyboard macros on the macros menu, (the most common choices of which are repeated on the menu bar for your convenience) or the quick keys associated with the macros. For example, if you press the <Ctrl><Alt> and <Delete> on your keyboard, you will act on your local system; to perform this same function on the remote system, click <Ctrl><Alt><Delete> on the macros menu, or use the quick keys that represents that macro, (<Alt><Print Screen>).

Other functions from the menu bar perform other operations on the remote server. Listings of all of the menu choices follow:

**Table 5. Virtual Server Control Macro Options**

<b>Macro</b>	<b>Macro</b>
<Ctrl><Alt><Delete>	<Alt><Print Screen>
<Alt><Tab>	<F1>
<Alt><Escape>	<Pause>
<Ctrl><Escape>	<Tab>
<Alt><Space>	<Ctrl><Enter>
<Alt><Enter>	<SysRq>
<Alt><Hyphen>	<Alt><SysRq>
<Alt><F4>	<Alt><Left Shift><Right Shift><Esc>

# Intel® Remote Management Module Virtual Media

## Intel® Remote Management Management Module Virtual Media Dialog Box

The Intel® Remote Management Module Virtual Media dialog box allows you to connect a floppy device, a USB device or a CD/DVD device to a target server. When you have connected a device, you will be able to see it from the remote console through the Intel® RMM Virtual Server Control. To access a server:

Under Applications on the lower left side of the Configuration page, click Intel® RMM Virtual Media application. The Intel® Remote Management Module displays the Virtual Media dialog.

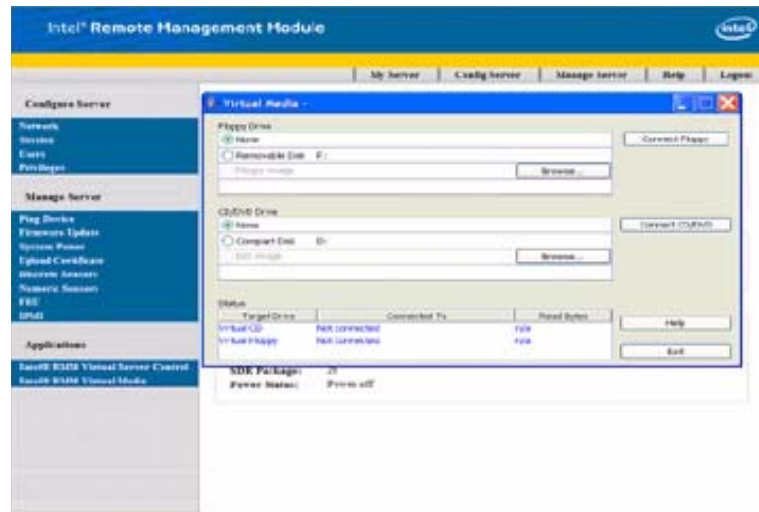


Figure 16. Intel® RMM Virtual Media Dialog

## Connecting a Generic Mass Storage Device

The Floppy Drive panel allows you to select a floppy or USB device from a list of all client floppy and removable USB drives. You can also select the Floppy Image option that allows you to browse to the location of your chosen floppy image file. If you do not want to select either of these options you can select the None option.

**Note:** Only one option from the Intel® Remote Management Module Virtual Media panel can be selected at any one time. The selected generic mass storage device is not connected until you click Connect.

## Connecting a CD-ROM or DVD-ROM Drive

The CD/DVD Drive panel allows you to select a CD-ROM or DVD-ROM device from the attached CD-ROM / DVD-ROM drives. You can also select the ISO image option to select a single CD-ROM / DVD-ROM image file. If you do not want to select either of these options you can select the None option.

**Note:** *Only one option from the CD/DVD Devices or Filesystem panel can be selected at any one time. The selected generic mass storage device is not connected until you click Connect.*

## Viewing the Connected Device Status

The Intel<sup>®</sup> Remote Management Module Virtual Media panel lists the generic mass storage and CD/DVD devices that are currently connected. For each connected device, the target drive letter, where the target drive is connected, and the number of bytes read for that device are displayed.

## Operating the Device Remotely

Once the device has been connected, operate it remotely through the Intel<sup>®</sup> Remote Management Module Virtual Server Control viewer. (See [“Interacting With the Server” on page 31](#)).

# Appendix A: Command Syntax and Return Status Codes

---

## Command Syntax

**Table 6. Command Syntax**

To Perform this Action	Use this Syntax
To test the host / Intel® Remote Management Module USB packet interface.	-t {text string}
To specify a user name (login).	-u {username}
To specify a password (must follow username).	-p {password}
To set one value.	-s {SettingName}={SettingValue}
To set one value to its default.	-s {SettingName}
To set all settings to defaults.	-s CTRL/DEFAULT_SETTING=1
To display (get) one value.	-g {SettingName}
To display the Intel® Remote Management Module's current firmware version information.	-i
To upgrade the firmware on an Intel® Remote Management Module with a single command. This performs a firmware image file upload to the Intel® Remote Management Module, verifies the image file integrity, flashes the firmware update, and reboots the Intel® Remote Management Module.	-f {ImageFileName}
To enable execution of subsequent commands in a local batch file if an error occurs (default is to discontinue subsequent commands).	-e
To disable responses from being sent to stdout during execution of subsequent options contained on the same command line, or subsequent command lines in a local batch file being executed. This is quiet mode - only the completion code will be returned).	-q
To cause subsequent commands in a batch file to be echoed to stdout before execution (noisy mode).	-n
To check a firmware update file to verify it is the proper file type and format.	-x {FileName}
To run a script file on the local system (dash command-line format).	-c {ImageFileName}
To maintain persistent connection (utility provides command prompt).	-m

**Table 6. Command Syntax**

To close a persistent connection (utility exits).	-quit
To display version and build information on the command-line utility.	version -h or -?

## Config Server Commands

**Table 7. Config Server Commands**

Setting Name	Description	Type	Default Value (First in the List) and (Format)
ENCRYPT/KVM	Encryption algorithm and strength.		NONE AES DES
ENCRYPT/VMEDIA	Encryption algorithm and strength.		NONE AES DES
LAN/ INTERFACE_PICK_COUNT	The number of records contained in the PICK_LIST variable.	Read-only	Appropriate to installed hardware



Setting Name	Description	Type	Default Value (First in the List) and (Format)
LAN/ INTERFACE_PICK_LIST	Interface instantiations that are available for use as the management LAN.	Read-only	<p>&lt;Index=3, Tag=LAN3, Desc=Management Module LAN3&gt;</p> <p>&lt;Index=2, Tag=LAN2, Desc=Baseboard Management LAN2&gt;</p> <p>&lt;Index=1, Tag=LAN1, Desc=Baseboard Management LAN1 &gt;</p> <p>If an interface is not available, then it should not be listed in this pick list by the Intel® RMM. Index values may be skipped; they do not need to be packed. (Hence internally, the list can have a fixed index, and records dropped when absent).</p> <p>General format is:</p> <p>&lt;Index, Tag, Description&gt;</p> <p>&lt;Index, Tag, Description&gt;</p> <p>and so on.</p> <p>The Tag fields must correspond with the prefix of the corresponding parameter for that LAN channel. For example, LAN1, LAN2, LAN3 as S/W will use the tag to determine which other variables control the LAN settings.</p> <p>The index value is used directly in the INTERFACE_SELECT field to select which interface is the active Intel® RMM interface.</p>

Setting Name	Description	Type	Default Value (First in the List) and (Format)
LAN/INTERFACE_SELECT	Chooses and enables the interface that will be used by the Intel® RMM to send and receive management traffic.	Read-write	<p>The default is selected via a policy based on detected hardware. The Intel® RMM will determine if IPMI management is enabled on the Intel® 631xESB / 632xESB I/O Controller Hub-embedded NIC using IPMI commands. If only LAN1 or LAN2 is enabled, then that interface shall be used, and the static/fixed setting in place will be adopted by the Intel® RMM.</p> <p>If both LAN1 and LAN2 are enabled, then LAN1 shall be the default.</p> <p>If neither LAN1 nor LAN2 are enabled, then the Intel® RMM's own NIC shall be selected as the default when the Intel® RMM is initially installed.</p> <p>LAN1 in the Intel® 631xESB / 632xESB I/O Controller Hub is the default.</p>
LAN3/INTERFACE_TYPE	Interface type for this LAN interface.	Read-only	<p>Types:</p> <ul style="list-style-type: none"> <li>• 0 = MM-MII</li> <li>• 1 = MM-UMP-MII</li> <li>• 2 = MM-RMII</li> <li>• 3 = MM-UMP-RMII</li> <li>• 4 = MM-DUAL-RMII</li> <li>• 5 = MM-DUAL</li> <li>• 6 = UMP_RMII</li> <li>• 7 = Chipset-MII</li> <li>• 8 = Baseboard-MII</li> <li>• 9 = Chipset-FML</li> <li>• 10 = TCO-FML</li> <li>• 11 = Baseboard-FML</li> <li>• 12-255 Reserved</li> </ul> <p>Intel® 631xESB / 632xESB I/O Controller Hub systems will only have:</p> <ul style="list-style-type: none"> <li>• MM-MII</li> <li>• Chipset-FML</li> </ul>
LAN3/ADDR_TYPE	IPv4	Read-only	IPv4

Setting Name	Description	Type	Default Value (First in the List) and (Format)
LAN3/ENABLED	Interface enabled.	Read-write	TRUE FALSE
LAN3/NETWORK	Network IP Address, Netmask, Gateway - sets all three before restarting the LAN interface. Needed for remote configuration utilities.	Read-write	192.168.0.122 255.255.255.0 192.168.0.1
LAN3/IPADDR	Network IP Address.	Read-write	192.168.0.122
LAN3/GATEWAY	Network Gateway.	Read-write	192.168.0.1
LAN3/NETMASK	Network Mask.	Read-write	255.255.255.0
LAN3/SPEED	LAN Speed.	Read-write	AutoSense 100mb 10mb
LAN3/DUPLEX	LAN Duplex.	Read-write	AutoSense Full Half
LAN3/DHCP	DHCP Enable.	Read-write	True, DHCP enabled False, Static
INFO/DATE	Intel® RMM date.	Read Only	12-17-2004
INFO/TIME	Intel® RMM time.	Read Only	23:00:00
DHCP/DEFAULT_IP_ADDR	This address is used when DHCP client requests fail, or when a static IP address is selected, but the user specified address is an invalid IP address per TCP/IP rules.	Read-write	192.168.0.122
USER/COUNT	Returns number of user accounts.	Read Only	1 to thousands
USER/TIMEOUT	Set/Get the number of seconds between commands before a user needs to login again.	Read-write	600

Setting Name	Description	Type	Default Value (First in the List) and (Format)
USER/<number>/NAME	The SET version is used to add a user. The <number> is not needed or used for the ADD operation. The read operation enumerates users. (1-based indexing).  First get the USER/COUNT, and then get their names via this command. To add a user, e.g. USER/NAME=Bob.	Read-write	User Name.  Up to 8 ASCII bytes.
USER/<username>/DELETE	Delete a user.	Write-only	User Name.  Up to 8 ASCII bytes.
USER/<username>/PASSWORD	Existing password input for validating user authentication prior to executing a password or privilege change. Also used for normal login operations.	Write-only	User Name and Password.  Up to 8 ASCII bytes.
USER/<username>/NEW_PASSWORD	Password input for selecting a new password value on a password change.	Read-write	User Name = Password.  Up to 8 ASCII bytes.
USER/<username>/PRIVILEGE	Set/Get a user's management access level.	Read-write	USER VIEW NONE ADMIN
PRIVILEGE/KVM_OP	Required privilege level for KVM operations	Read-write	USER ADMIN
PRIVILEGE/MEDIA_OP	Required privilege level for Media Redirection operations.	Read-write	USER ADMIN
PRIVILEGE/USER_OP	Required privilege level for User Account and Password operations.	Read-write	ADMIN (USER and other levels are not allowed to be set.) Trying to set returns an error.  This is a value so that users can display the requirement via CLP tools.
PRIVILEGE/CLP_DISPLAY	Required privilege level for CLP operations that do not allow setting values.	Read-write	ADMIN USER VIEW
PRIVILEGE/CLP_CHANGE	Required privilege level for any CLP operations that allow setting and changing values.	Read-write	ADMIN USER

Setting Name	Description	Type	Default Value (First in the List) and (Format)
PRIVILEGE/WEB_DISPLAY	Required privilege level for Web server display pages.	Read-write	ADMIN USER VIEW
PRIVILEGE/WEB_CHANGE	Required privilege level for Web server pages actions that change parameters or effect command actions.	Read-write	ADMIN USER
PRIVILEGE/ POWER_CYCLE	Required privilege for Web server Power cycling operations.	Read-write	ADMIN USER
PRIVILEGE/ SYSTEM_RESET	Required privilege level for Web server Reset operations.	Read-write	ADMIN USER
CTRL/SYSTEM_RESET	When set to reset, this causes a system reset.	Write Only	Reset
CTRL/ SYSTEM_POWER_STATE	When set to Request_PowerDown, causes the system to power down. The Intel® RMM will change the value of its current operating state to Off on completion of a Request_PowerDown request or to Operating on completion of a Request_PowerOn request.	Read-write	Operating Off Request_PowerDown Request_PowerOn
CTRL/MANAGEMENT _RESET	When set to Reset, this affects a reset in the Intel® RMM itself. This is restored to Operating when the Intel® RMM recovers from its reset.  If set to Operating, this is ignored without error by the Intel® RMM. Only setting to Reset results in any action.	Read-write	Operating Reset

Setting Name	Description	Type	Default Value (First in the List) and (Format)
CTRL/SERIAL_MUX_STATE	Value decides how the Intel® RMM will program the serial mux on the server board.	Read-write	Auto: Defaults to server board routing, unless a connection request comes in via Telnet or SSH2, and then the Intel® RMM auto selects mux to itself via IPMI to IPMB, and on a connection loss, sets the mux back to server board.  Intel® RMM: Intel® RMM sets mux to always select the RMM connector.  Baseboard: Intel® RMM sets the mux to always select the server board logic.
CTRL/DEFAULT_SETTINGS	Forces all settings to factory defaults	Write only	1: Set all settings to factory defaults.
HTTPS/ENABLED	If page serving using the HTTPS protocol is enabled.	Read-write	True, Enabled, default False, not enabled.
HTTPS/PORT	IP Port to enable HTTPS serving on.	Read-write	443
KVM/ENABLED	KVM Server allows KVM sessions to start.	Read-write	True, enabled. False, not enabled.
KVM/KVM_PORT	KVM Server keyboard and mouse signals port number	Read-write	5900
KVM/VIDEO_PORT	KVM Server video signal port number	Read-write	5901
INFO/FIRMWARE_VERSION	String describing the firmware revision level	Read-only	
INFO/SDR_VERSION	String Describing the SDR revision level.	Read-only	
INFO/PXA_VERSION	String describing the Intel PXA processor version.	Read-only	
INFO/WEB_CONTENT_VERSION	String describing the Web server file system content version.	Read-only	
INFO/BOOTLOADER_VERSION	String describing the installed boot loader version	Read-only	
INFO/HARDWARE_REV	String describing the hardware revision level	Read-only	
INFO/MAC_TYPE	Hex representation of the MAC_TYPE bits.	Read-only	

Setting Name	Description	Type	Default Value (First in the List) and (Format)
SELF_TEST/CONTROL	<p>Initiate the self test when set from 0 to 1. When test is complete, the Intel® RMM sets the flag from 1 to 0.</p> <p>Writing a 0 has no effect. Set SELF_TEST / SUBCOMPONENT to something other than 0 before setting this attribute to 1.</p>	Read-write	<p>0 = Test-Not-Running</p> <p>1 = Initiate-Self-Test</p> <p>1 = BUSY. (Same as test is running).</p>
SELF_TEST/STATUS	<p>Shows results of current or last self test. If the test is running then a 1 is returned. Only the SELF_TEST / SUBCOMPONENT attribute is accurate, showing what subcomponent is currently executing in the self-test. If the STATUS attribute is not 1, then the test results are final. A zero value means the test passed. A non-zero value means the test failed, in which case the CONTROL and REASON values are set.</p>	Read-only	<p>0 = Test complete; no errors.</p> <p>1 = Test still running, subcomponent field is valid.</p> <p>2 = Test failed, unknown cause, unknown component.</p> <p>3 = Test failed with unknown cause on known subcomponent shown in the subcomponent field.</p> <p>4 = Test failed with identifiable cause reflected in the “reason” self test field in subcomponent identified in the subcomponent field.</p>
SELF_TEST/LAN_MODE	<p>Sets the testing mode for the LAN on the self test.</p> <p>When set to 1, on systems that support this function, the self test will assume a valid external connection on the LAN, and hence Link testing and a ping (ICMP) test to the test peer address can be performed.</p>	Read-write	<p>0 = No external wire testing. (Test peer is not needed).</p> <p>1 = External Peer connectivity test shall be executed.</p>
SELF_TEST/LAN_PEER_ADDR_TYPE	<p>Sets the IP version used in the LAN ping test (ICMP).</p>	Read-write	0 = IPv4
SELF_TEST/LAN_PEER_ADDR	<p>IP Address of another host to ping. Address can be any valid host computer, router or gateway that supports ping.</p>	Read-write	IPv4 IP Address

Setting Name	Description	Type	Default Value (First in the List) and (Format)
SELF_TEST/ SUBCOMPONENT	Sets which system subcomponent is under test. Defaults to NONE. Set this attribute before setting SELF_TEST/CONTROL to 1 (which starts the self test).	Read-write	0 = NONE Under Test 1 = FML Channel 1 3 = IPMB 6 = DVO (digital video) 7 = LAN3 8 = LAN2 (not supported in this release)  The USB interface of the Intel® RMM is tested by the mmconfig -t command when performed on the host console.
SELF_TEST/REASON	Reason a test failed in a subcomponent. The reason codes vary per subcomponent.	Read-only	FML: <ul style="list-style-type: none"> <li>• 0 = No error.</li> <li>• 1 = Send Failed.</li> <li>• 2 = Send &amp; Receive Failed.</li> </ul> IPMB: <ul style="list-style-type: none"> <li>• 0 = No error.</li> <li>• 1 = IPMB Failed to send.</li> </ul> DVO: <ul style="list-style-type: none"> <li>• 0 = No error, no video signal detected.</li> <li>• 1 = No error, video signal detected.</li> <li>• 2 = Error, not running.</li> </ul> LANx: <ul style="list-style-type: none"> <li>• 0 = No error.</li> <li>• 1 = NIC to PHY link not established (MII not working)</li> <li>• 2 = PHY self test failed.</li> <li>• 3 = NIC self test failed.</li> <li>• 4 = NIC internal loop back failed.</li> </ul>



## Return Status Codes

Return Status Name	Explanation	Value
SUCCESS	Operation successful and Intel® RMM present	0x00
ERR_RMM_NOT_PRESENT	No Intel® RMM detected	0x01
ERR_INVALID_CMD_SWITCH	A dash command line switch or option is not valid	0x02
ERR_ILLEGAL_PARAMETER	A command parameter or value is not valid or missing	0x03
ERR_SYNTAX_ERROR	A syntax error occurred not covered by the two above error codes	0x04
ERR_INVALID_FW_FILE	A file designated by the -f switch is not a valid firmware file	0x05
ERR_FW_UPDATE_FAILED	An -f command (FW upgrade) failed for reasons besides the above	0x06
ERR_RMM_FILE_NOT_FOUND	A file was not found in the Intel® RMM directory during open (read)	0x07
ERR_RMM_FILE_NOT_CREATED	A file was not created in the Intel® RMM directory during open (write)	0x08
ERR_RMM_FILE_READ	An error occurred while reading a file from the Intel® RMM	0x09
ERR_RMM_FILE_WRITE	An error occurred while writing a file to the Intel® RMM	0x0A
ERR_HOST_FILE_NOT_FOUND	Requested file was not found in the current host directory	0x0B
ERR_HOST_FILE_NOT_CREATED	Requested file was not created in the current host directory	0x0C
ERR_HOST_FILE_READ	An error occurred reading a file in the host directory	0x0D
ERR_HOST_FILE_WRITE	An error occurred writing a file to the host directory	0x0E
ERR_FILE_VERIFY	A verify mismatch was detected between a file on the host and a file with the same name on the Intel® RMM	0x0F
ERR_WIN32_EXEC_ON_DOS	An attempt was made to execute the Win32 utility under DOS	0x11
ERR_RMM_SEND_REQUEST	An error was encountered sending a request to the Intel® RMM	0x12
ERR_RMM_RECV_RESPONSE	An error occurred while receiving a response from the Intel® RMM	0x13
ERR_INSUFFICIENT_PRIVILEGE	An error occurred attempting a function without adequate privileges	0x14
ERR_INVALID_USER_OR_PSWD	A login was attempted with either an invalid username or password	0x15
ERR_INVALID_IP_ADDR	IP address entered is invalid or in invalid format	0x16
ERR_UNDEFINED	An undefined error was encountered	0x18

