联想万全慧眼 III 高级版 RMM2 用户手册 V1.0

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。

前言

关于手册

感谢你购买并使用联想远程管理高级卡（Lenovo Remote Management Module 2，以下简称 RMM2）。

RMM 主要针对系统维护工程师在一些日常工作中的问题提供提供支持与帮助，诸如，发现并处理故障，更新升级，修复管理高级卡等。该手册同时还提供产品的特性以及使用说明。

手册内容

第一章， Lenovo RMM2 产品简介，模块特性以及产品图；

第二章， 介绍如何利用 Psetup 工具查找 Lenovo RMM2 的 IP 地址以及配置方法。同时介绍如何设置 lenovo RMM2 恢复到出厂缺省值；

第三章， 介绍 Lenovo RMM2 WEB 接口；

第四章， 介绍如何连接到远程控制台（KVM）的步骤；

目　录

重要安全指导 2
前言 3
关于手册 3
第一章　简介 6
第二章 服务工具 8
Psetup 8
图形用户界面 8
Linux 命令行界面 10
第三章 WEB 页面 12
导 航 13
在线帮助 13
退出 14
远程控制 Remote Control 14
KVM 控制台 KVM Console 15
远程电源控制 Remote Power 16
虚拟介质 Virtual Media 16
Floppy Disk Image 16
驱动重定向 Driver Redirection 17
系统健康 System Health 18
系统信息 System Information 19
机箱控制 Chassis Control 20
传感器信息 Monitor Sensors 20
系统事件日志 System Event Log 21
用户管理 User Management 21
改变密码 Change Password 22
用户与组 Users & Groups 22
Permission 23
KVM 设置 KVM Settings 25
用户控制台 User Console 26
键盘/鼠标 Keyboard/Mouse 27
设备设置 Device Settings 29
网络 Network 29
动态 DNS Dynamics DNS 31
安全 Security 33
证书 Certification 34
USB 36
IPMI 37
日期与时间 Date And Time 37
认证 Authentication 38
SMTP 设置 SMTP Settings 40
事件日志 Event Log 40
SNMP 41

语言 Language.....43
维护 Maintenance.....43
设备信息 Device Information.....43
事件日志 Event Log.....44
更新固件 Update Firmware.....45
单元复位 Unit Reset.....46
第四章 远程控制台（KVM）.....47
主窗口.....47
远程控制状态条.....48
远程控制条.....48

第一章 简介

主要特性介绍

Lenovo RMM2 模块包含一个嵌入式的操作系统，该操作系统是独立于服务器操作系统之外的，从而可以为服务器提供一整套完整、稳定、有效的解决方案。作为系统管理工程师，你可以利用 Lenovo RMM2 独有的功能远程对服务器突发的紧急事件作出相应以及一些日常的维护工作。

Lenovo RMM2 通过专有的网络接口实现远程的 KVM（键盘，鼠标，显示窗口）的访问。它可以将远端服务器的键盘，鼠标，显示页面的信号实时捕获，数字化处理，压缩经网线镜像到本地的控制台端，你在本地控制台的操作就犹如你座在远端服务器前操作一样。远程的通道以及控制软件都在 Lenovo RMM2 上嵌入的处理器上运行，因而不会对服务器本身的操作系统以及网络性能造成影响。除此之外，Lenovo RMM2 还通过 IPMI 提供电源管理。具体 RMM2 的关键特性，请见下文：

- 嵌入式的 WEB UI－远程电源开/关，系统健康，系统信息，Lenovo RMM2 固件更新，事件日志（包括 Lenovo RMM2 模块自身的事件）
- 经由专有网口的 KVM 重定向，其专有的网口提供高效，同时并发的访问；
- USB2.0 介质重定向－支持远程介质引导启动；
- 安全－支持 SSL，LDAP，SSH，RADIUS 等方式；
- OEM 的定制；
- Lenovo RMM2 事件的 Email 告警；
- 对 Lenovo RMM2 事件，还可以采用 SMASH CLI/CLP,WS-MAN,SNMP 等方式；
- 经由 KVM 的软键盘模式（对多语言的支持）；
- 兼容 IPMI V2.0；
- 自动判断显示器的分辨率，以便将捕捉的屏幕效果最佳的呈现出来；
- 高效的鼠标追踪与同步；
- 可以远程查看操作系统启动之前的 POST 过程，并可以进入 BIOS 配置页面查看以及修改配置页面；

支持的操作系统

Lenovo RMM2 的运行是独立于服务器的，但是 RMM2 是将服务器端的键盘、鼠标、显示器内容传送到控制台端，使得你在控制台前的任何操作，都犹如在服务器前的操作。RMM2 不能保证在所有 OS 下的操作都能顺利执行，以下是 Lenovo 所支持的 OS 种类

被管理服务器端所支持的操作系统种类

• Microsoft Windows 2003* Server with Service Pack 1或更近的更新 or later and all recent updates

• Red Hat* Enterprise Linux Advanced Server 4

客户端所支持的操作系统种类

以下客户端的操作系统与网络浏览器的组合已经通过测试：

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

第二章 服务工具

Psetup

Psetup 能呈现 Lenovo RMM2 通过 DHCP 分配的 IP 地址，也可以修改原有的 IP 地址。甚至 IP 地址没有配置，也可以利用 Psetup 工具进入该卡的配置页面。

Psetup 可以通过远程或已经安装了 RMM2 卡的服务器本地进入到 RMM2 的配置页面。如果本地没有该工具，可以利用一个外接的 USB 设备连接上该模块。如果是远程方式，Psetup 可以发现该主机所在网段内所有外插 RMM2 的信息。如果更改 RMM2 卡的网络配置信息你需要输入作为超级用户的用户名及密码，修改才能有效。缺省的登陆用户名为“Admin”，密码为：Password。建议你在登陆后马上更改登陆密码。

图形用户界面

初次使用 Psetup 工具，它会扫描网内所有外插 RMM2 卡的信息。具体呈现在 MAC 地址栏中，通过 MAC 地址的下拉菜单你可以依次查看并配置每块卡的网络信息。如果想再次搜索，请点击”Refresh”（Linux）或者”Refresh Device”(Windows)。

Windows 版本下的 Psetup

Psetup 呈现的图形页面请见图 2-1

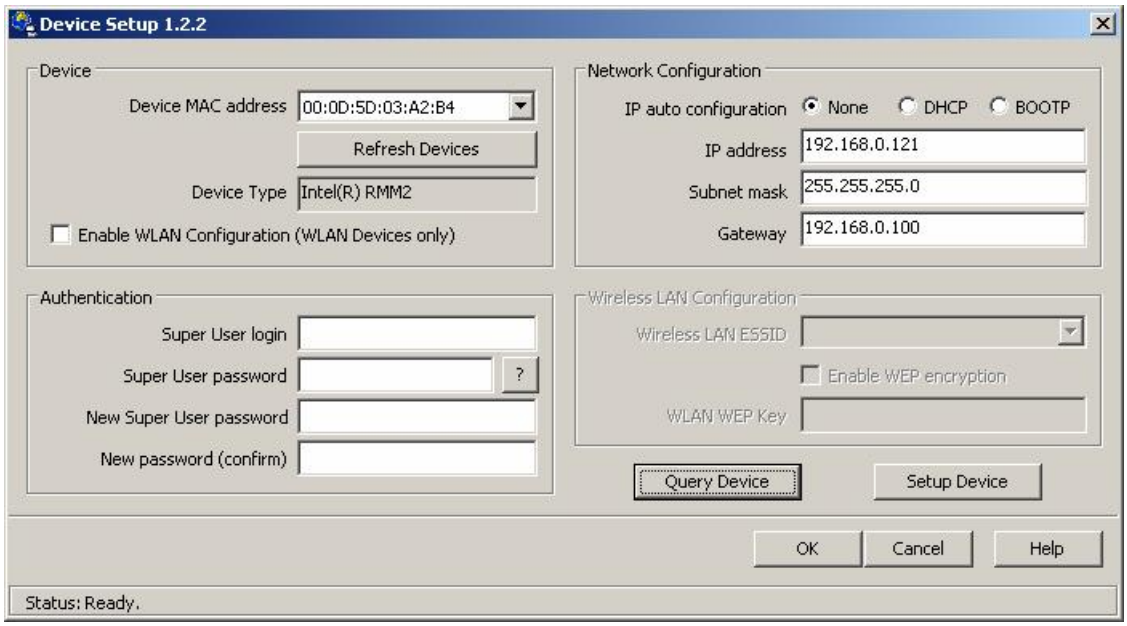


图 2-1：Windows 版 Psetup 配置页面

如图 2-1 所示，设备的 MAC 地址呈现在页面的左上角，其硬件的设备类型为 Intel RMM2。如果想再次搜索一遍设备，请点击“Refresh Device”按钮。点击“Query Device”会呈现该 MAC

地址对应的网络信息，诸如 IP 地址，子网掩码，网关等信息。

如果想改变登陆密码，请按照下列操作执行：
1、 确定你正在操作的 MAC 地址所对应的设备正是你所需要修改的设备；
2、 输入作为超级用户使用的用户名，缺省值为“Admin”；
3、 输入当前的用户密码，缺省值为“Password”；
4、 在”new Super user password”栏，输入新密码；
5、 重新确认新密码；
6、 点击“OK”保存设置；

更改网络配置值：
1、 确定你正在操作的 MAC 地址所对应的设备正是你所需要修改的设备；
2、 改变必要的网络配置值；
3、 输入有效的作为超级用户登陆的用户名；
4、 输入相应的登陆密码；
5、 点击“Setup Device”保存你的更改信息。

Linux 版本的 Psetup

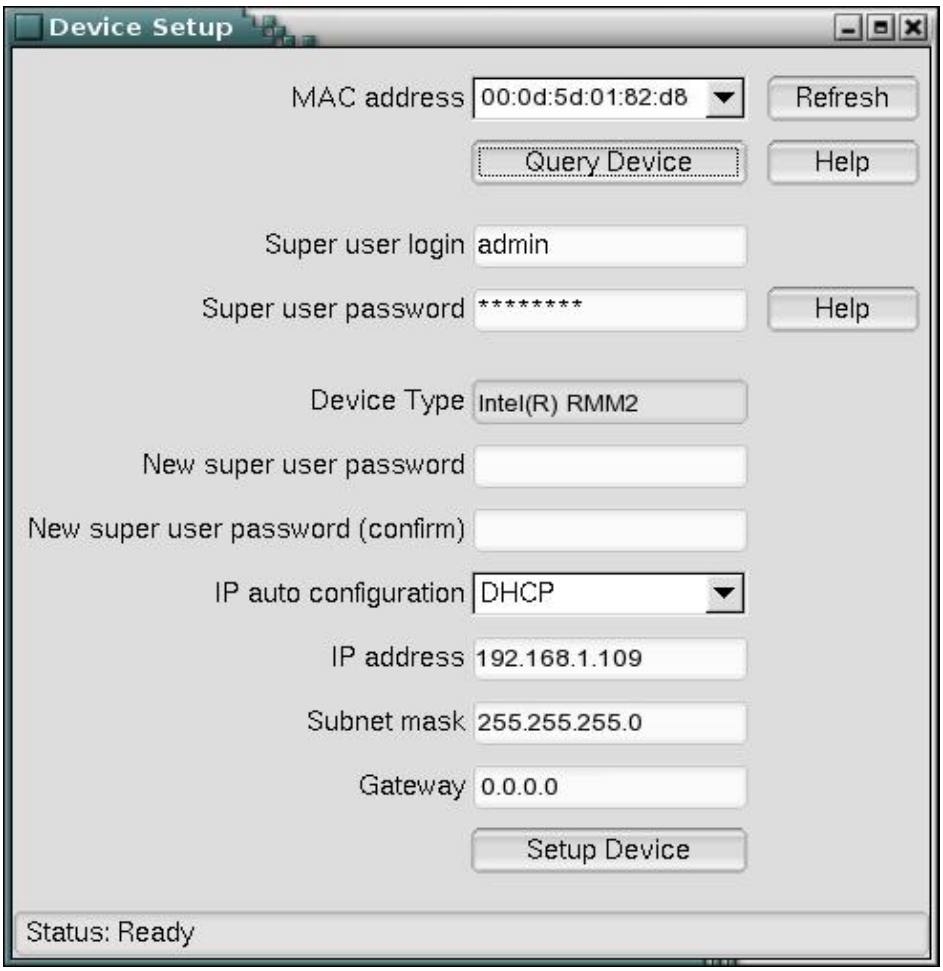


图 2-2：Linux 版的 Psetup 配置页面

具体图形界面请见图 2-2。设备的 MAC 地址呈现在页面的上部。如果需要重新搜索 MAC 地址信息，请点击“Refresh”。

更改密码：
1、 确定你正在操作的 MAC 地址所对应的设备正是你所需要修改的设备；
2、 输入作为超级用户使用的用户名，缺省值为“Admin”；
3、 输入当前的用户密码，缺省值为“Password”；
4、在”new Super user password”栏，输入新密码；
5、在”new Super user password （Confirm）”栏再次输入新密码；
6、 点击“Query Device”保存设置；

更改网络配置值：
1、 确定你正在操作的 MAC 地址所对应的设备正是你所需要修改的设备；
2、 改变必要的网络配置值；
3、 输入有效的作为超级用户登陆的用户名；
4、 输入相应的登陆密码；
5、 点击“Setup Device”保存你的更改信息。

Linux 命令行界面

Linux 下还可以在字符页面下使用 Psetup。下面列表 2-1 展示了命令行方式执行的句法以及使用方式。

表 2-1： Psetup 在 Linux 下的命令行

命令	使用方式	示例
-mac <device MAC address>	展示当前网络配置	命令: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78** 结果: **IP auto configuration: dhcp** **IP address: 192.168.5.135** **Subnet mask: 255.255.255.0** **Gateway: 192.168.5.1**
-ip <new IP address>	设置网络的IP地址	命令: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -ip 192.168.5.55 -login super -pw pass** 结果: **Device configured successfully.**
-ipacp <dhcp|bootp|none>	自动配置方式	命令: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -ipacp none -login super -pw pass**

		结果: **Device configured successfully.**
-netmask <net mask>	设置子网掩码	Command: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -netmask 255.255.255.0 -login super -pw pass** Results: **Device configured successfully.**
-gateway <gateway address>	设置网关地址	Command: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -gateway 192.168.5.1 -login super -pw pass** Results: **Device configured successfully.**
-login <username>	输入具有Administrator权限的用户名，以使得修改的网络信息生效	Command: **test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -gateway 192.168.5.1 -login super -pw pass** Results: **Device configured successfully.**
-pw <password>	输入相应的密码	
-pw-new <password>	为选择的用户设置新密码	**test@teststation:~# /home/test/psetup -mac 00:0D:5D:00:65:78 -pw-new newpass -login super -pw pass** Results: **Device configured successfully.**

重新设置Lenovo RMM2恢复到出厂默认缺省值

利用Kiratool工具在本地将RMM2恢复到出厂设置的缺省值状态；
本地执行的命令：Kiratool –a –u admin –p <password> defaults

第三章 WEB 页面

RMM2 模块是一种嵌入式操作系统。它能提供各种标准化接口的应用。所有接口符合 TCP/IP 协议，可以通过内置以太网适配器或者调制解调器来访问。RMM2 支持下述接口：

- HTTP/HTTPS：使用标准的网络浏览器可以访问到 RMM2 管理环境。嵌入的网络服务提供 HTTP/HTTPS 两种方式。你可以根据实际情况选用适当的方式，如果可能请使用支持加密方式的 HTTPS 协议。
- Telnet：标准的 Telnet 客户端支持大多数 RMM2 的功能，包括字符模式控制端的重定向。当采用 Telnet 连接方式时，支持下述命令：Help，quit，version，terminal 以及 clp。
- SSH：A Secure Shell（SSH）客户端；

RMM2 模块主要使用的接口是 HTTP 接口。为了调用你管理主系统的远程控制窗口，浏览器需要安装 Java Virtual Machine 1.1 或者更高版本的 JavaVM 程序。如果浏览器没有 Java Virtual Machine 支持，你仍然可以使用浏览器本身显示的管理形式支持你的远程主系统。

注： 推荐安装 Sun JVM 1.4。

对于一种不安全联接到 RMM2 模块的方式，我们推荐如下网络浏览器：

- 在 WINDOWS 98，Windows ME，WINDOWS 2000 和 Windows XP 上微软的 IE3.0 或者更高版本。
- 在 WINDOWS 98，Windows ME, WINDOWS 2000，Windows XP，Linux 和其它 UNIX-的操作系统上的 Netscape 导航 7.0，Mozilla 1.6 和 Mozilla Firefox。

为了远程主系统能访问使用安全的带密码的联接方式，你需要浏览器支持 HTTPS 协议。该协议可以确保使用的密钥为 128 位。 一些旧的浏览器不支持 128 位译成密码的算法。 使用 Internet 浏览器，打开菜单进入“帮助/关于”菜单，浏览当前密钥长度。图 3-1 显示的是 Internet 6.0 的对话框。

图 3-1：IE6.0

打开 IE，有两种方式 HTTP 和 HTTPS 可以访问到 RMM2。如 http：// 192.168.81.66/或者 https：// 192.168.81.66/，根据实际需要选择适当的方式，输入 RMM2 模块的 IP 地址，回车。出现登录页面，输入用户名和密码后，单击 Login 按钮。具体如图 3-2；

初次登陆，使用缺省的用户名与密码。
缺省用户名＝admin
密码＝password
初次登陆后，系统管理员或 IT 专职人员可以改变密码，创建新用户并重新控制 RMM2。
注意：由于 RMM2 具有自己的处理器与内存。为了保证操作的相应时间，建议同时连接到 RMM2 的用户数不要超过 25 人。

导 航

登陆进入 RMM2 模块后，RMM2 的主页面呈现如下。整个页面分为三部分：

- 上部的按钮提供进入 Home 页面，控制台 Console 页面以及 Logout 页面。
- 左半部分包含了所有的导航功能条，以便于在各导航功能条之间进行切换。
- 右部页面内，会详细显示左边选定导航功能条的具体信息。

图 3-2：主页面

在线帮助

WEB 页面包含在线帮助。点击页面上的“？”，即可出现所点击部分的帮助说明。具体形势可参见下图。

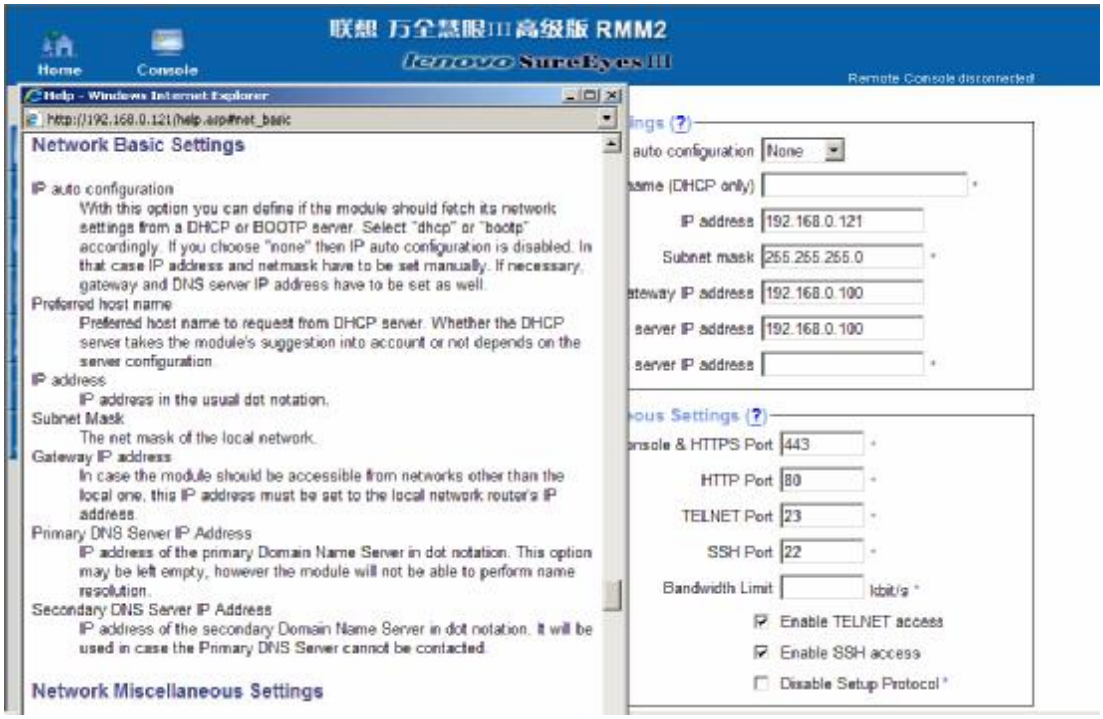


图 3-3:（online help）在线帮助

退出

点击 Logout 按钮，页面会再次弹出 login 页面。如果在 30 分钟内不做任何操作，WEB 页面也会自动退出。但是相关联的远程控制台（KVM）的连接不会相应也关闭，需要用户手动关闭。

注：如果点击 IE 页面上的刷新按钮，登陆页面会更新，同时相关联的远程控制台的连接也会相应关闭。

远程控制 Remote Control

远程控制台有两个选项：KVM 控制台与远程电源管理。详见图 3-4

图 3-4：远程控制

KVM 控制台 KVM Console

详见图 3-5。选择左半部分的 KVM 控制台或者点击右半部分呈现的远程 KVM 静态的图形，可以点击 refresh 查看更新的页面，即可进入远程的 KVM 控制台页面。具体介绍请见第四章的“远程控制台 P48（Remote Console（KVM））部分的介绍。

图 3-5：KVM Console

远程电源控制 Remote Power

远程电源是经由 IPMI 实现的，具体实现的功能有电源开启/关闭，重启。这些操作不会影响 RMM2 的操作。

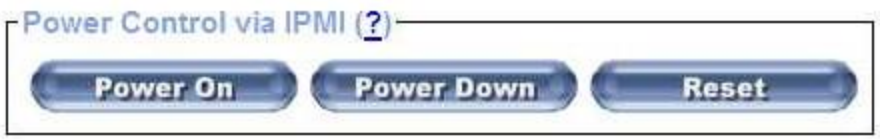


图 3-6：远程电源控制

虚拟介质 Virtual Media

该菜单有两个功能选项：Floppy disk Image，Driver Redirection，具体图列请参见图 3－7

图 3-7：虚拟介质

Floppy Disk Image

最大支持的软盘镜像文件为 4 个。具体加载形势见图 3－8，首先在 Virtual Driver 的选择框内选择需要添加的驱动号，再从 Floppy Image File 内填写需要添加的驱动文件，或者点击 Browse 按钮，从文件列表内选择需要添加的.img 文件。具体添加的.img 文件大小不能超过 1.44MB，选好文件后，点击“Upload” 该镜像文件将加载到 RMM2 模块内，如果想去除该

镜像文件，请点击“Discard”。如果点击 Logout 按钮或重新启动 RMM2，原有添加的镜像文件将不会有效保存。

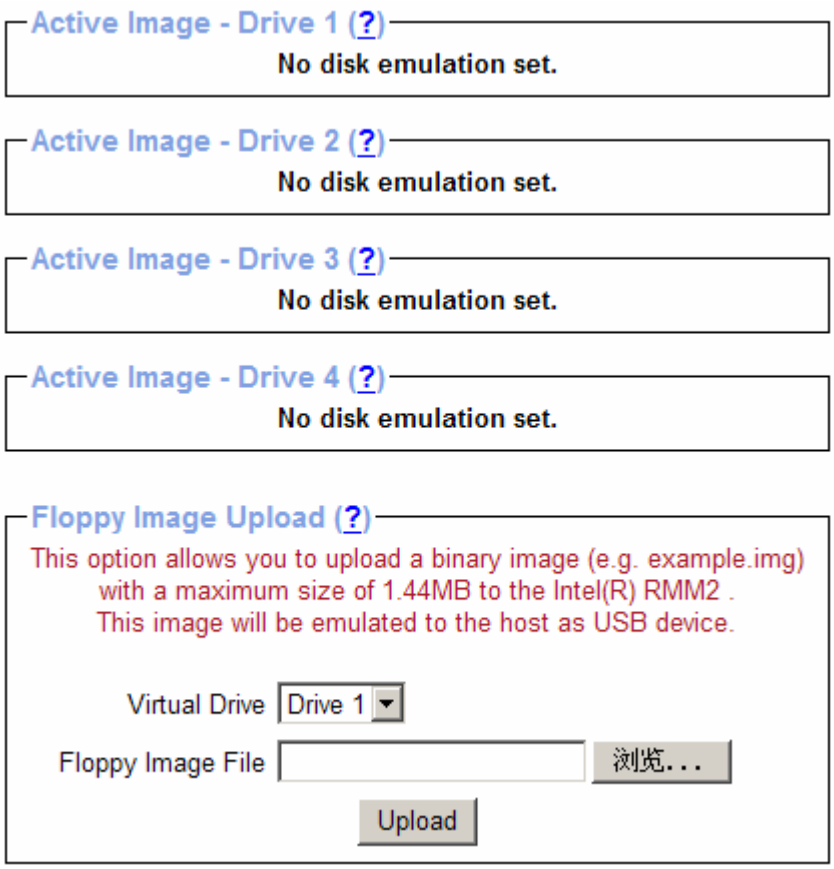


图 3-8：Floppy Image

驱动重定向 Driver Redirection

驱动重定向允许加载虚拟驱动至远程服务器端，从而代替镜像文件的使用。你可以将本地计算机上的软驱，CD-ROM，以及其它一些移动设备，诸如 USB 设备，通过 TCP 网络连接共享给远程的服务器。甚至于远端的服务器可以执行写操作，写数据到本地的驱动器。本页面只能呈现添加驱动的状态，如果想使用虚拟介质或驱动重定向过去的设备，你需要进入远程控制端的窗口。

使用驱动重定向需要小心，尤其是写操作。驱动重定向工作在操作系统层之下。本地与远程都不会意识到驱动已经重定向了。这在执行写操作时，可能会导致远端或者本地写数据到设备上时的数据不一致。如果写操作被允许了，远程服务器可能会破坏重定向设备上的数据或文件系统。如果本地的操作系统写数据到重定向设备上，而远程主机操作系统上的驱动缓存可能还包含一些旧数据，这可能会搞乱远程主机的操作系统。

在驱动重定向的页面内，图 3—9 有两个选项。

- 禁止驱动重定向：如果选定，则驱动重定向处于不可获得状态；
- 强制只读连接：如果选定该功能，则写支持不可用。即不能通过驱动重定向设备进行写操作。

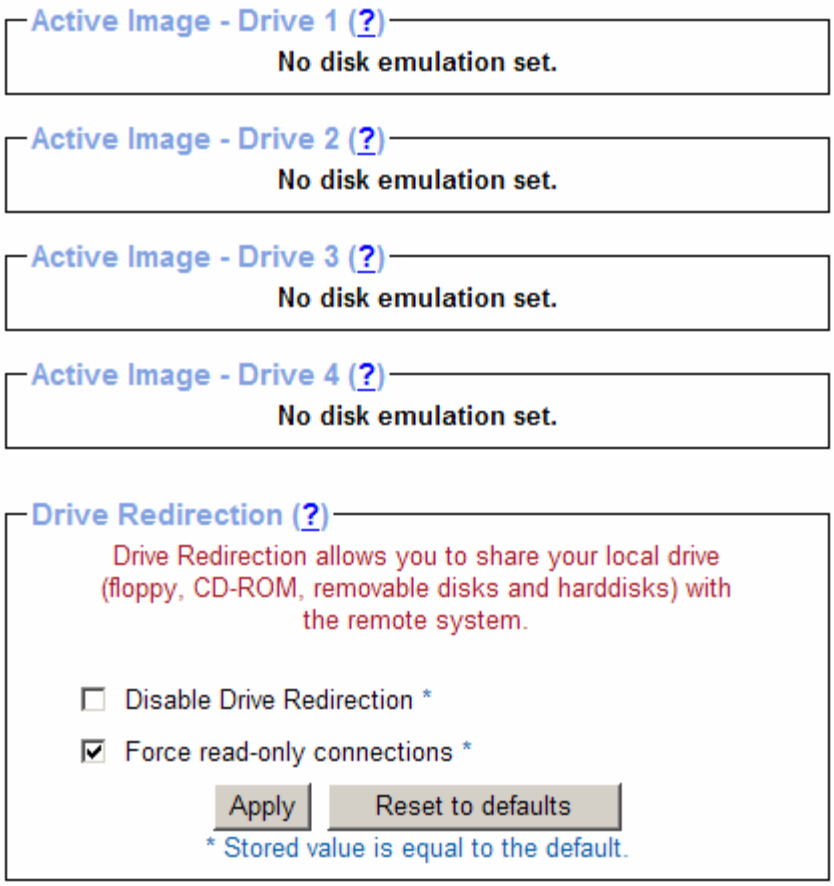


图 3-9：Driver Redirection

系统健康 System Health

该菜单包含四部分：

- 系统信息
- 机箱控制
- 传感器信息
- 系统事件日志

RMM2 可以通过智能管理平台接口（IPMI）对远程的主机执行电源开关，硬重启等。还可以查看远程主机的硬件事件日志，系统硬件健康信息，诸如获取主机上的温度。

图 3-10： System Health

系统信息 System Information

该页呈现主机系统上的基本信息，具体请参见图 3-11。

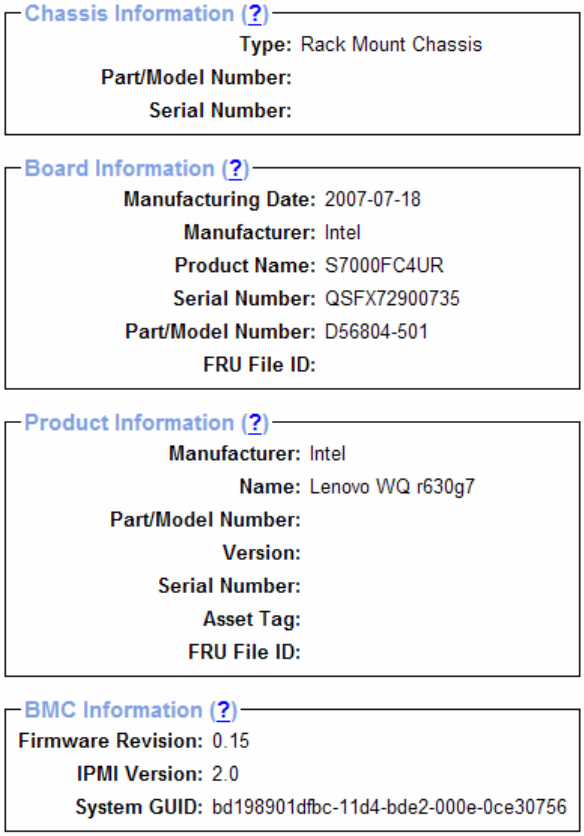


图 3-11：System Information

机箱控制 Chassis Control

机箱控制可以获得当前机箱的状态，进行远程电源控制，以及点亮蓝色的系统 ID 灯。请见图 3-12。

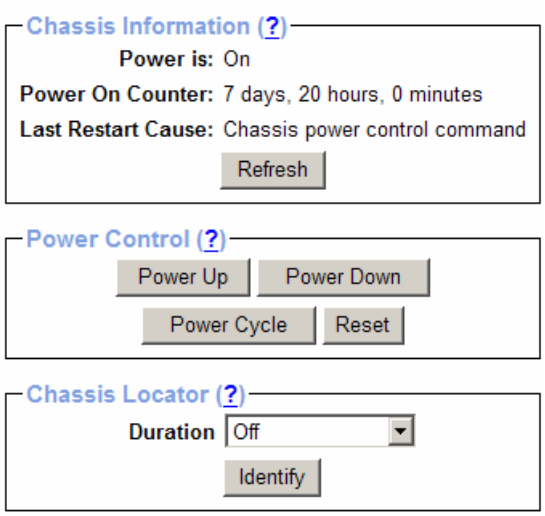


图 3-12：Chassis Control

传感器信息 Monitor Sensors

该页面提供当前获取的传感器状态与具体读值。如果传感器的读值超过了预先设定的阈值，传感器的状态会变成红色，否则呈现的状态为绿色。具体状态请参见图 3－13

Monitoring Sensors (?)

Type	Name	Status	Reading
Temperature	BB Temp	Ok	35 (+/- 1.500) degrees C
Temperature	FP Temp	Ok	26 (+/- 1.500) degrees C
Temperature	Mem Brd A Temp	Ok	29 (+/- 8.500) degrees C
Temperature	Mem Brd B Temp	Ok	31 (+/- 8.500) degrees C
Temperature	Mem Brd C Temp	Ok	28 (+/- 8.500) degrees C
Temperature	Mem Brd D Temp	Ok	29 (+/- 8.500) degrees C
Temperature	Mem A-B Agg Marg	Ok	-39.000 (+/- 1.500) degrees C
Temperature	Mem C-D Agg Marg	Ok	-12.000 (+/- 1.500) degrees C
Fan	System Fan 1	Ok	2310 RPM
Fan	System Fan 2	Ok	2310 RPM
Fan	System Fan 3	Ok	2331 RPM
Fan	System Fan 4	Ok	2289 RPM
Fan	Memory Fan 1	Ok	3840 RPM
Fan	Memory Fan 2	Ok	3872 RPM
Fan	Memory Fan 3	Ok	3840 RPM
Fan	Memory Fan 4	Ok	3872 RPM
Temperature	PS1 Temp	Ok	34 degrees C
Temperature	PS2 Temp	Ok	34 degrees C
Temperature	P1 Therm Margin	Ok	-53.000 degrees C
Temperature	P1 Therm Ctrl %	Ok	0 unspecified
Temperature	HSBP Temp	Ok	0 (+/- 1) degrees C
Power Unit	Pwr Unit Redund	Fully Redundant	
Physical Security	Physical Scrty		

图 3-13：Monitor Sensor

系统事件日志 System Event Log

该页面呈现主机系统的硬件事件日志。该页面的下部有一个 Clear 按钮，点击该按钮，可以清除所呈现的事件日志。请注意不要将该日志与记录 RMM2 的管理日志混淆。

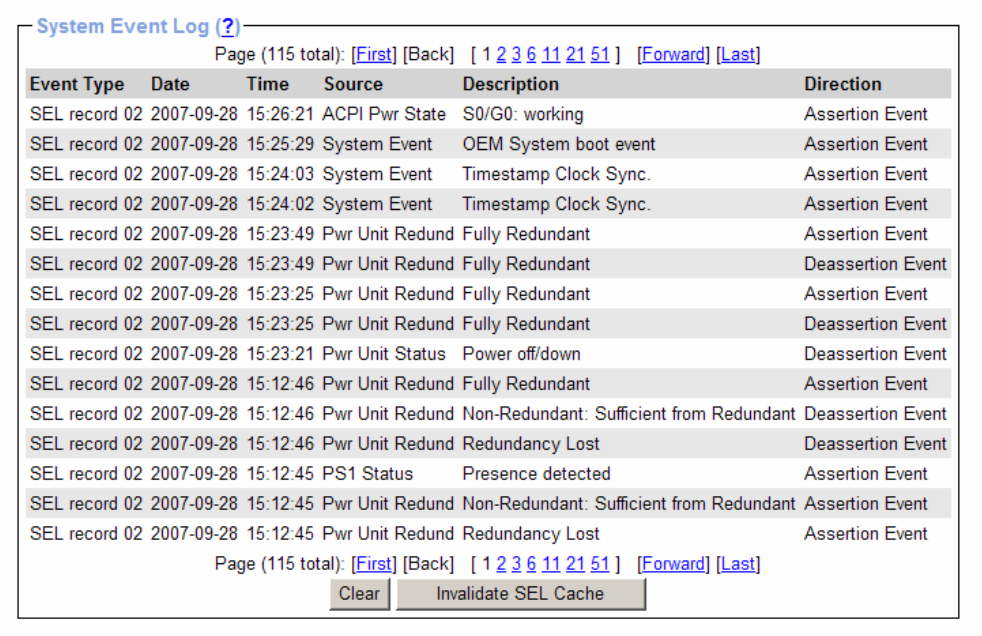


图 3-14：System Event Log

用户管理 User Management

该菜单包含三个选项：

- 改变用户密码
- 建立用户与组
- 权限

RMM2 预先设置一个管理员/超级用户。超级用户的登录名称为“Admin”， 超级用户具有所有权限，并能够执行 RMM2 所有的功能。

RMM2 预先设置了如下群组：

Admin：组内的用户都是 Administrator/superuser.

Unknown：该群组的用户没有特定的组，而且其权限受限。

None：表明该用户没有组，并且其获得的权限是私有权限。

作为超级用户可以删除预定义的组，并且能创建、删除其它组。

图 3-15：User Management

改变密码 Change Password

改变密码的操作步骤：

1、 在 Old Password 选项框内，输入当前密码。

2、 在 New Password 选项框内，输入新密码，密码长度至少 4 位。

3、 在 Confirm New Password 选项框内，再次输入新密码。

4、 点击“ Apply”，生效新密码。

图 3-16：Change Password

用户与组 Users & Groups

用户管理

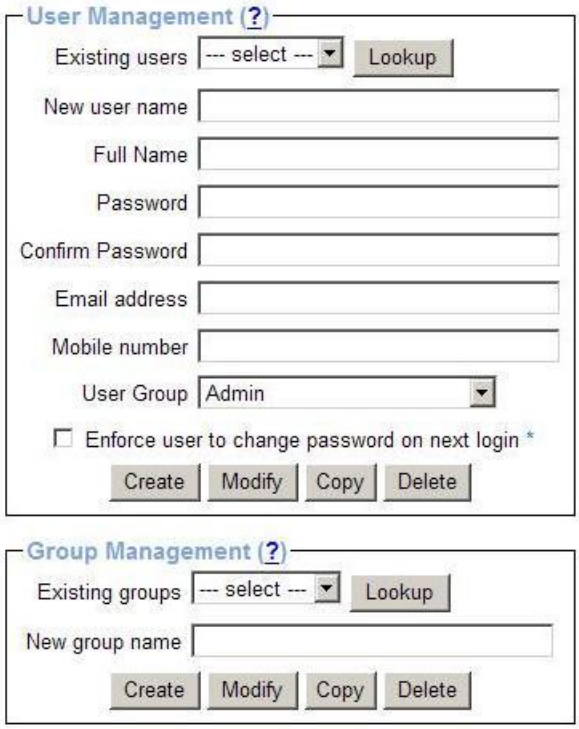


图 3-17:User&Group

- 存在的用户（Existing users）：选择存在的用户列表以进行修改。一旦选好用户，点击 Lookup 按钮，会出现用户的具体信息。
- 新用户名称 New User name：可以输入新用户名称。
- 密码 Password：配合登陆用户名的密码。
- 确认密码 Confirm password：确认上述密码。
- 电子邮件地址 Email address：可选项。
- 移动电话号码：这个信息以供选择。

组管理

每个用户都是一个组的成员--或者是管理人员，或者是一个常规用户。可以从组的下拉菜单中选择希望的组。

如果想建立一个用户点击按钮“Create”。 点击“Modify”修正已经设定的用户。点击“Delete”删除一个用户。

Permission

该页面允许对每个组以及组中的成员设置权限，每个用户的权力来自于组的权力，对没有组的成员，可以分别设置他们的权限。

具体配置：

1、 选择具体的组或无组的用户从下拉的菜单中。你所选择的条款将影响它的权限。

2、 点击各个条款设置允许或禁止。这部分的设置要先于远程控制台的设置。

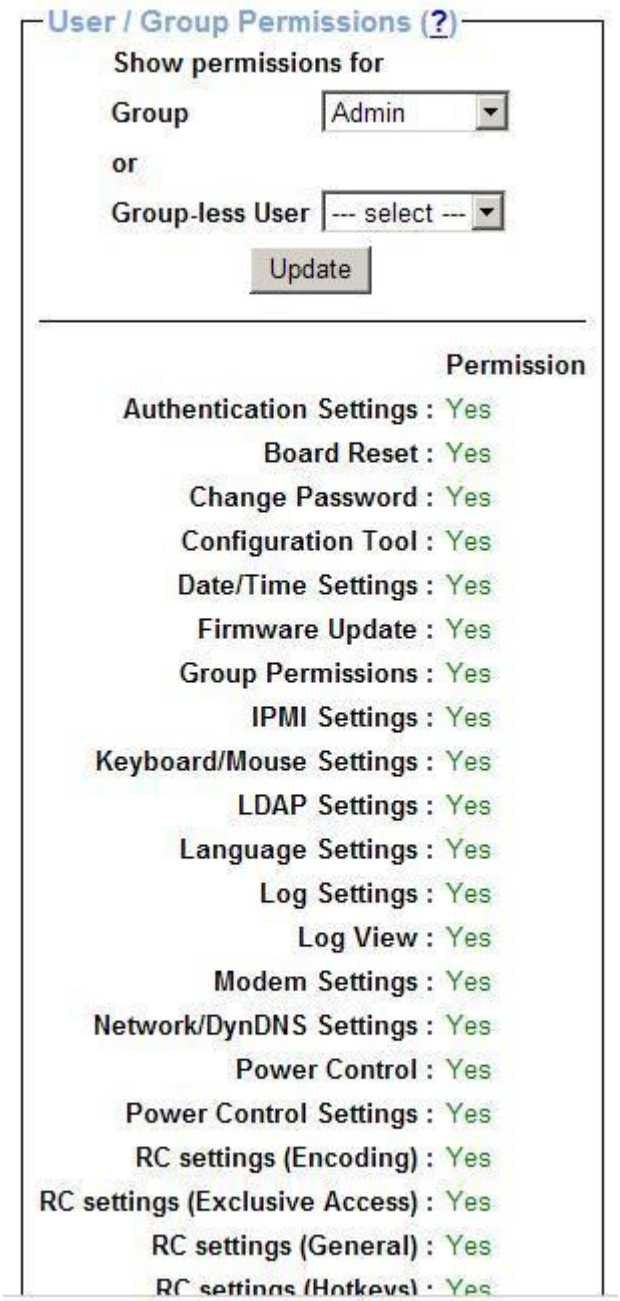


图 3-18：Permissions

KVM 设置 KVM Settings

本菜单有 2 个选项：用户控制台，键盘/鼠标

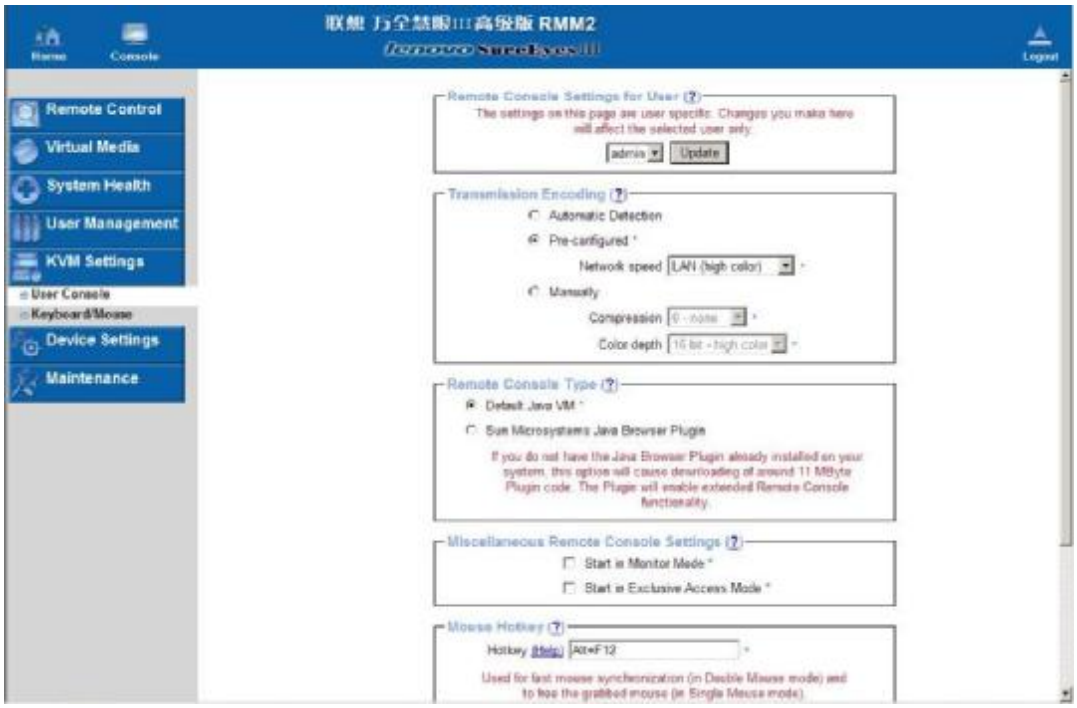


图 3-19：KVM Setting

用户控制台 User Console

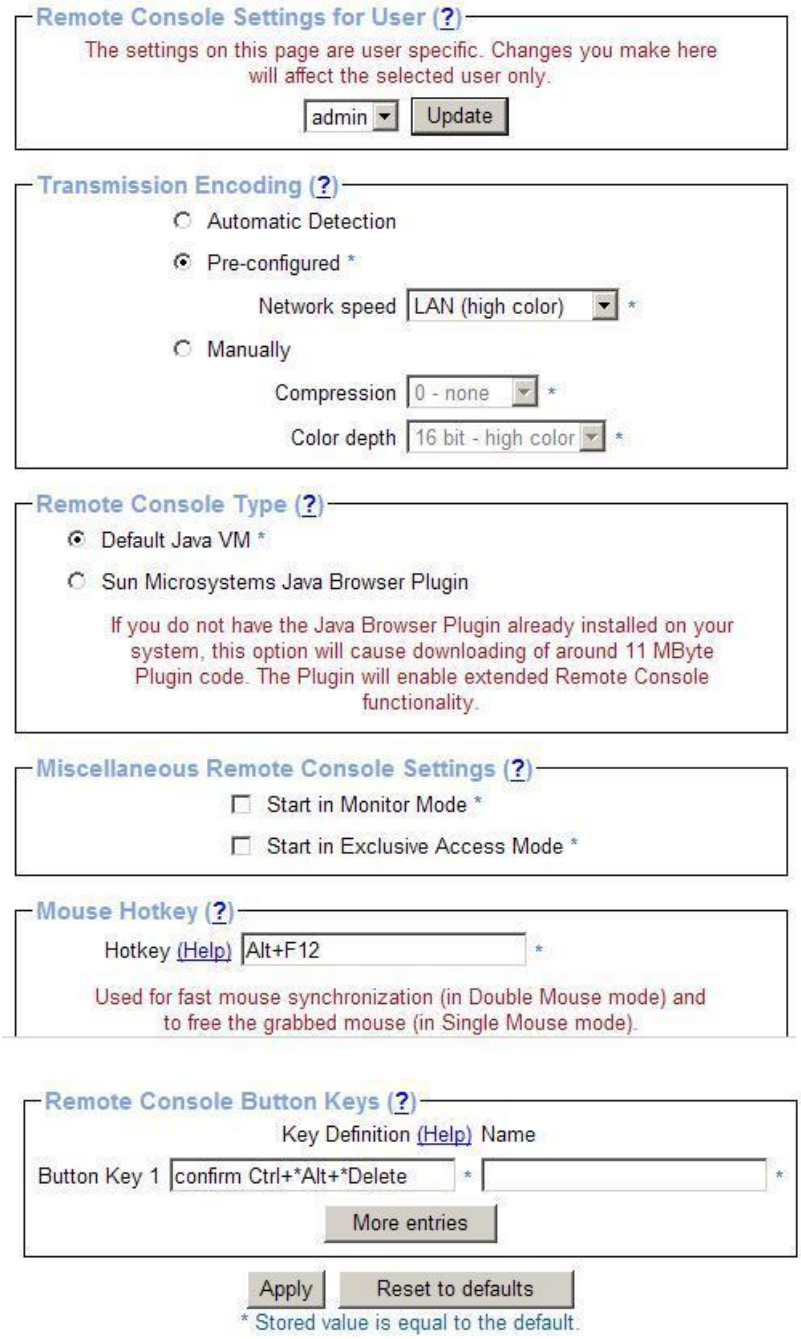


图 3-20：User Console

Remote Console Settings for User

用户的远程控制设置，从下拉菜单中选择期望的用户形式，并且压按钮“更新”。这一改变只影响所选用户。

注意：你能更改其他用户的设置，表明你具有这个权限。对于一个普通用户没有权限修改其它用户的设置。

Transmission encoding

视频信号传输到远程控制台窗口是通过图像编码算法实现的，编码传输设置允许改变视

频数据传送图像的编码算法。这种优化取决于同时工作的用户数以及联接线(调制解调器，ISDN，DSL，LAN 等)的带宽。

- Automatic detection：通过当前可供使用的带宽和视频图像的内容自动确定编码和压缩水平。
- Pre－configure：预设置想获得的最好结果，需要优化调整压缩比和颜色深度，这些取决于网络速度。
- Manually：允许手动个别调整压缩率和颜色深度。在 RMM2 卡和远程控制台之间的数据流传送选择压缩方式可以节省带宽。当多个用户同时访问 RMM2 时，由于高的压缩率十分耗时间，这时不推荐使用压缩方式。

标准的颜色深度是 16 位(65536 种颜色)。其它颜色深度旨在于较缓慢的网络联接。为了较快传输数据，0 级(没有压缩)压缩水平仅使用 16 位颜色深度。在低带宽模式下，典型的桌面推荐 4 位(16 种颜色)和 2 位(4 个灰度)模式。 对于象照片的图片想要具有最好的效果，配备 4 位(16 个灰度)。1 位颜色深度(黑/白)仅应用于极缓慢的网络联接。

Remote console type 远程控制台类型

指明使用那种方式浏览远程控制台

- Default Java Virtual Machine (JVM)：缺省的浏览方式采用 Java VM(JVM)。如果选择该方式，这可能是微软 JVM 或者 SUN 公司的 JVM。对 SUN 公司 JVM 的使用也可以是下述情况。
- Sun Microsystems Java Brower Plug-in：表明你的管理控制系统使用的是 Sun 公司的 Microsystems Java virtual machine。如果系统没有安装 Java VM 插件，在第一次进入此对话框时，它会自动下载并且安装此插件。当然，在安装过程中的对话框中，你只能回答“是”。以安装此插件，该插件代码大约 11 Mbytes。Sun 公司的 JVM 具有良好的稳定性并能适应各种不同的平台。

各种各样的远程控制台设置

- 以监视器方式开始：设置了监视器模式的初值。缺省模式是“disable”状态。为防止你打开它，远程控制台窗口仅以“读”方式开始。
- 以专有权模式开始：一打开远程控制台立即使能专有权模式。这种模式强迫关闭了所有其它用户打开远程控制台的能力。直到关闭该特性或者注销该能力。

鼠标热键

在同步鼠标或单一鼠标模式下，允许特殊的热键组合进行远程控制，“Ctrl+Alt+Del”即是一个典型应用。

键盘/鼠标 Keyboard/Mouse

当使用远程控制台时，需要对键盘鼠标的模式进行选择。

Windows 2000*,2003*,XP(各种版本)：在 USB 鼠标类型选项中选择 “MS Windows 2000 or newer”，在 Windows 的控制面板选项中禁用“增强精度的指针”。

Linux：在 USB 鼠标类型选项中选择“Other Operating Systems”。其鼠标速度选择“Auto”。该选择适配 USB 与 PS2 两种鼠标。

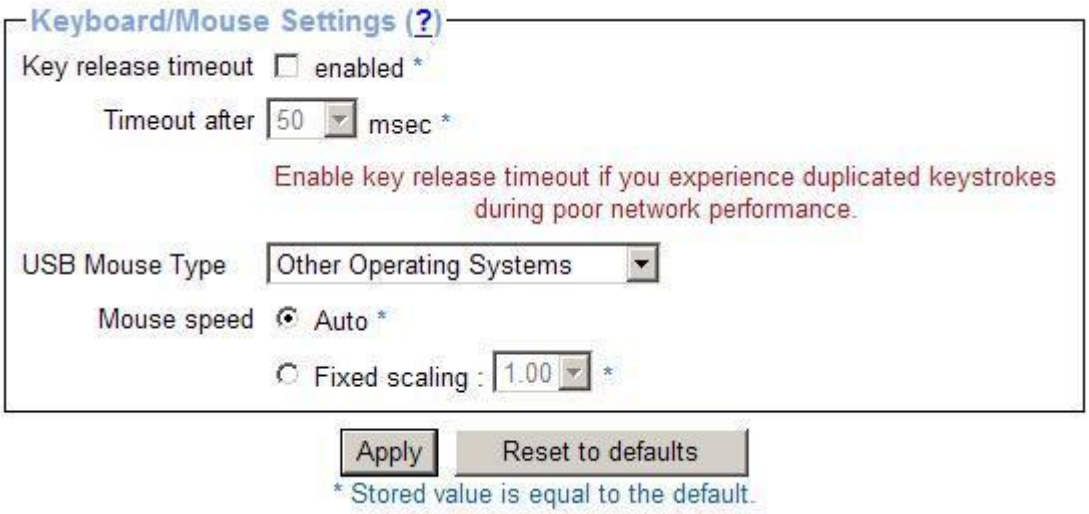


图 3-21：Keyboard/Mouse

- 键盘释放超时 Key Release Timeout：如果登陆 RMM2 的网络很慢或者正发生拥塞，建议选中“enabled”选项。在正常情况下，当你按压了键盘，网络会将按压的键打包传送至 RMM2。当你释放该键时，RMM2 相应也会收到释放该键的网络包。当网络很慢时，这个传送的过程可能会很长，从而导致 RMM2 一直重复处在该键的按压状态，就犹如你一直按压该键一样。而如果选中了该选项，当时间到达设置的等待时间后，RMM2 会自动释放该键，而不必一定要收到释放的传送包，同时也避免无意识的多次按压。
- USB 鼠标类型 USB Mouse Type：使能 USB 鼠标类型。从选择框内选择相应的选项。针对 MS Windows 2000，2003 Server，XP，请选择“MS Windows 2000 or newer”。针对 MS Windows NT*，Linux 或 OS X.，请选择“Other Operating Systems”。在“MS Windows 2000 or newer”的模式下，远程鼠标总是会与本地鼠标保持同步。
- 鼠标速度自动 Mouse Speed Auto：鼠标速度设为自动。如果服务器主系统的鼠标使用了增强加速设置，RMM2 模块会自动加速以保持与鼠标同步。
- 鼠标速度固定比例 Mouse Speed Fixed Scaling：固定鼠标速度。在本地与远程的鼠标指针之间采用直接传送鼠标移动的模式。你可以设定一个固定的比例尺决定远程鼠标移动的量，诸如本地鼠标每移动一个象素点，远程鼠标指针也开始移动一个象素点。这种选项仅在主系统的鼠标设置在现象状态才可用。

所有选项选好后，单击按钮“Apply”生效。

设备设置 Device Settings

图 3-22：Device Settings

本菜单包含 12 个选项：

- 网络 Network
- 动态 DNS Dynamic DNS
- 安全 Security
- 证书 Certificate
- USB
- IPMI
- 日期/时间 Date/Time
- 认证 Authentication
- SMTP 设置 SMTP Settings
- 事件日志 Event Log
- SNMP 设置 SNMP Settings
- 语言 Language

网络 Network

网络设置面板如图 3-23 所示，在该页面允许用户自行更改所需要的网络配置参数。具体参数设置如下所述。 一旦单击“Apply”，新的网络设置将立即生效。

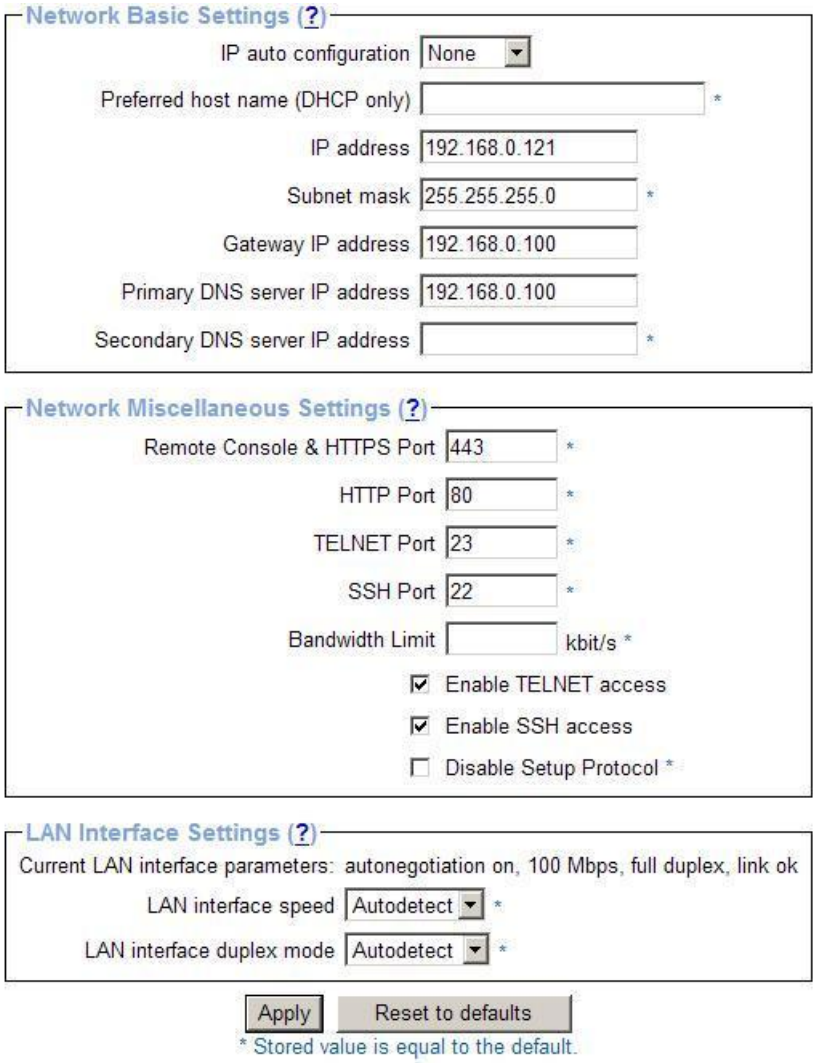


图 3-23：Network Settings

警告：改变 RMM2 模块的网络设置可能会导致与它失去联系。所以改变设置时要确保你所输入的数字是正确的，你还能登陆进入 RMM2 控制页面。

基本的网络设置 Basic Network Settings

- IP 自动配置 IP auto configuration：利用网络的 DHCP 或者 BOOTP 服务器功能自动获得 IP 地址。相应的，在 DHCP 栏中选择“dhcp”BOOTP 选项中选择“bootp”。如果选择“none”，则禁止 IP 自动配置能力。
- IP 地址 IP address：IP 地址以点符号“.”来间隔。
- 子网掩码 Subnet Mask：本地网络的网络掩码。
- IP 地址的网关 Gateway IP address：RMM2 模块要能由除本地之外的网络访问，这个 IP 地址要设为本地网络路由器的 IP 地址。
- 首选 DNS 服务器 IP 地址 Primary DNS Server IP Address：IP 地址以点符号“.”间隔，该选项可以为空。
- 备选 DNS 服务器 IP 地址 Secondary DNS Server IP Address：IP 地址以点符号"."间隔，它主要防止首选 DNS 服务器没连上的备选方案。

其它网络设置 Miscellaneous Network Settings

- Remote Console And HTTPS port ：该端口呈现的是 Lenovo RMM2 模块的远程控制服务和 HTTPS 服务正在接收信号的端口。缺省端口号为 443。
- HTTP port：RMM2 模块的 HTTP 服务接听端口。 缺省端口号为 80。
- Telnet port： RMM2 模块的 Telnet 服务端口，缺省端口号为 23。
- SSH port：RMM2 模块的 SSH（安全页面）服务监听的端口，缺省端口号为 22。
- Bandwidth Limit 带宽限制：通过 RMM2 模块以太网设备产生的最大网络流量。 单位 Kbit/s。
- Enable Telnet：允许 Telnet 客户端模式。
- Enable SSH：允许 SSH（Secure Shell）客户端模式。
- Disable Setup Protocol：选中该选项，将禁止 RMM2 模块设置协议。

Lan 接口设置 Lan interface setting

该条呈现了 RMM2 模块在以 Ethernet/LAN 作为接口的设置，你可以选择自动协商和固定设置两种方式，如果选择固定模式需要在下列“interface speed”和“duplex mode”的下来菜单中进行选择。

- LAN interface speed ：LAN 的接口速度取决于网络，你可以选择一个合适的速度值。为了调整接口你可以选择“autodetect”(缺省值)。如果选择的结果不符合该接口，你可以选择其它数值，接口将以那个固定速度传输数据。
- LAN interface duplex mode：LAN 接口双工模式，如果必要你也可以选择具体的双工模式。 缺省值设为“autodetect”，它将按照你的网络自动选择双工模式。作为一种变通，你可以明确设定接口为“半双工”和“全双工”模式。

动态 DNS Dynamics DNS

通过服务商动态指定的 DSL 路由的 IP 地址，可以访问 RMM2 模块。因为管理员不知道由服务商指定的 IP 地址，RMM2 模块定时与特定的动态 DNS 服务器连接并注册自己的 IP 地址。管理员也可以连接服务器获得属于本卡的相同的 IP 地址。管理员必须为将和动态 DNS 服务器一起提供服务的 RMM2 模块注册并指定一个确定的主机名。注册过程中会得到一个别名与密码。为了确定已注册的 RMM2 模块的 IP 地址，需要这个帐户的信息和主机名。为了使用动态 DNS，必须按照以下步骤操作：

1. 确保 RMM2 的 LAN 接口已被适当配置。
2. 进入图 3－24 所示的动态 DNS 设置对话框。
3. 使能动态 DNS 并根据你的需要改变设置。
   - 启动动态 DNS Enable Dynamic DNS：打开动态 DNS 服务。要求一个已配置的 DNS 服务器 IP 地址。
   - 动态 DNS 服务器 Dynamic DNS server：这是 RMM2 模块定时注册自己的服务器名。当前，由于仅有 dyndns.org 支持，这是一个固定设置。
   - 主机名 Hostname：这是由动态 DNS 服务器提供的 RMM2 模块的主机名。(使用包括域名的全名，例如 testserver.dyndns.org)。
   - 用户名 Username：在手动注册到动态 DNS 服务器时，你已经注册了这个用户名。在别称中不允许空格。

- 口令 Password：当你在手工注册到动态 DNS 服务器时已用了这个口令。
- 检查时间 Check time：RMM2 模块注册自己到动态 DNS 服务器的时间。
- 检查间隔 Check interval：这是 RMM2 模块再次注册到动态 DNS 服务器的时间间隔。

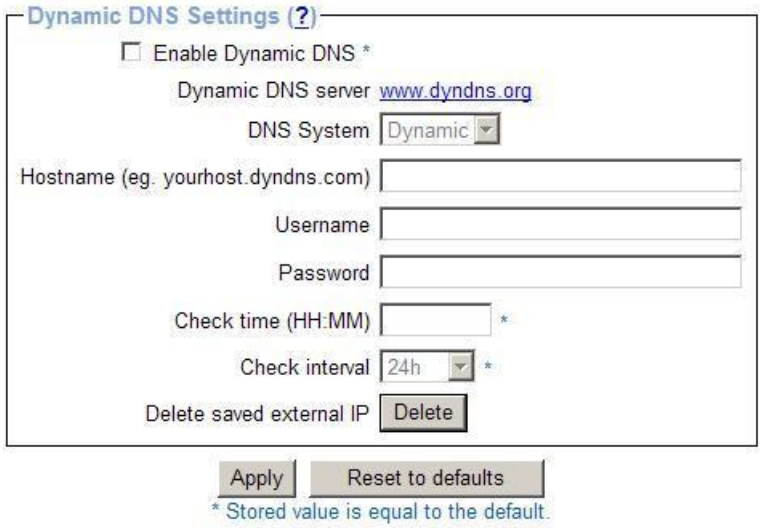
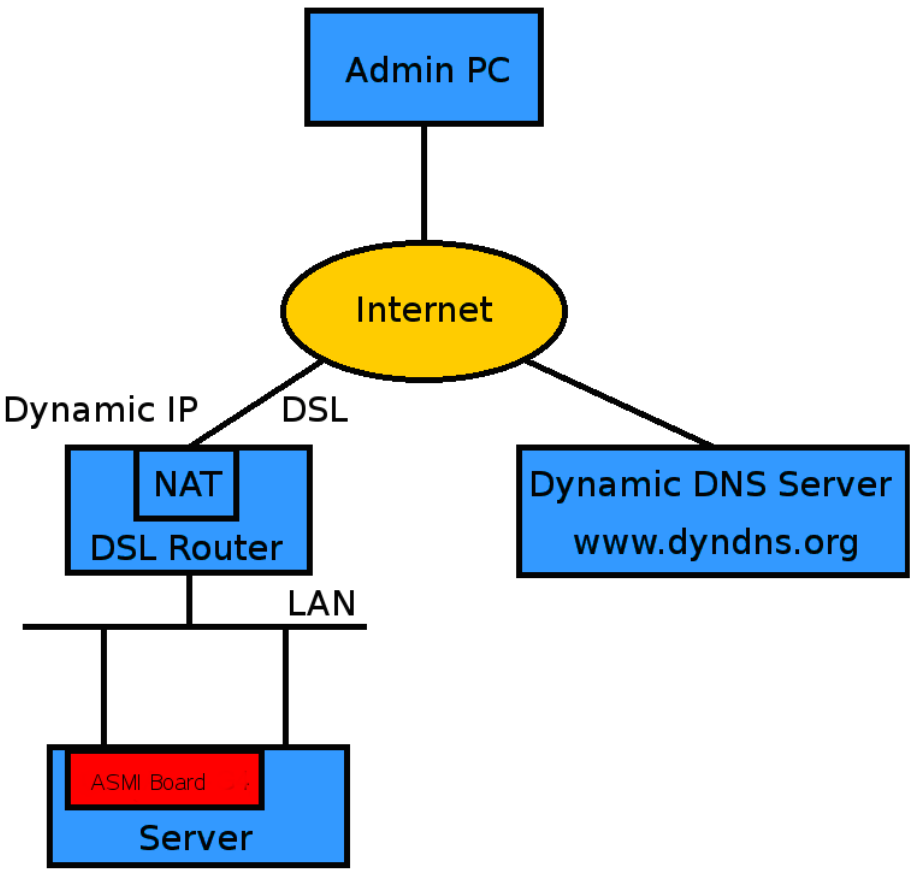


图 3-24：Dynamic DNS Settings

注意：*RMM2 有其自己独立的时钟。确保 RMM2 的时间设置是正确的。*

如果想设定一个动态 DNS 服务（dyndns.org），可参考如下设定方式。



安全 Security

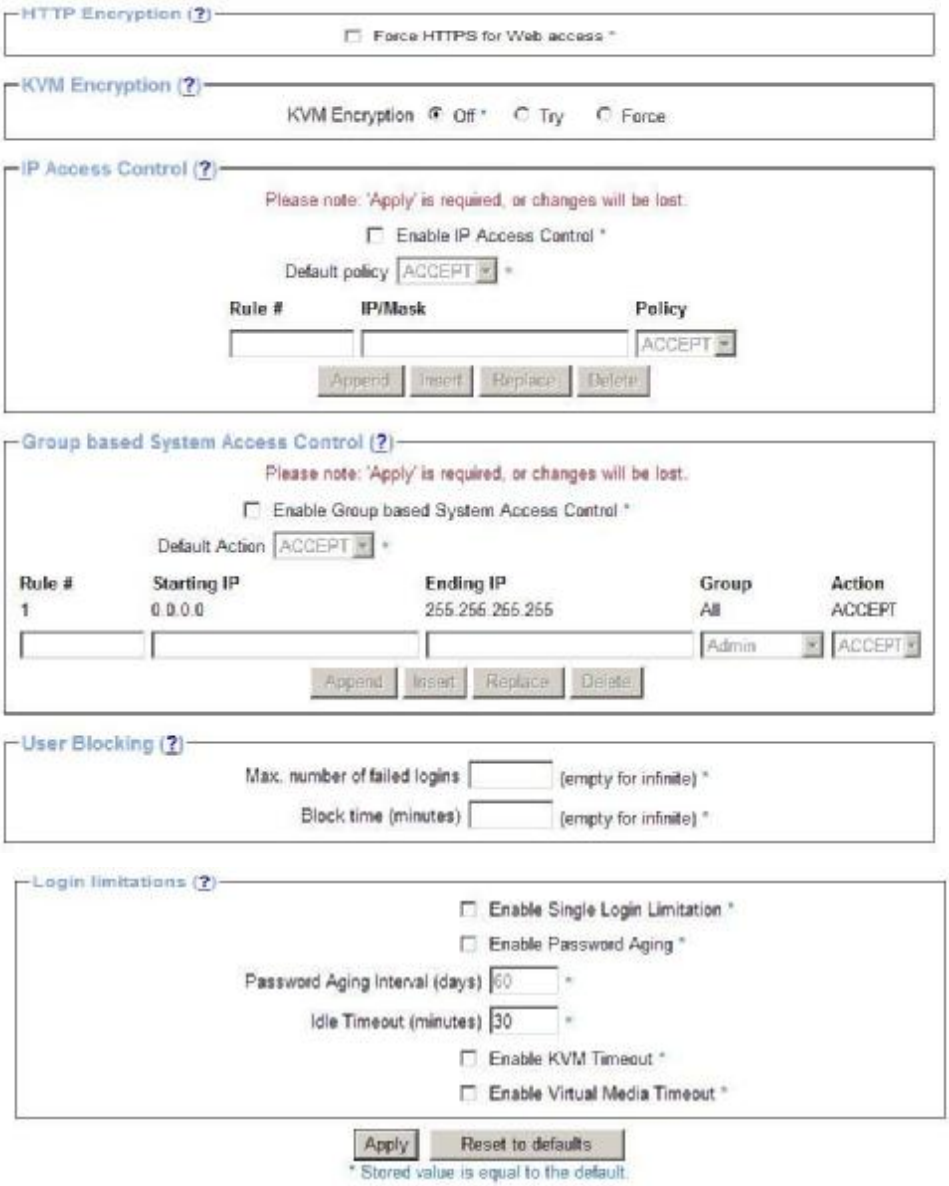


图 3-25：Security

HTTP 加密 Http Encryption

Force HTTPS For Web access：如果选择本选项，只能用 HTTPS 来访问网络端口。RMM2 卡将不再侦听 HTTP 端口上的连接。并产生你自己的 SSL 证书来识别当前使用的 RMM2。具体见“Certificate”页面 P36。

KVM 加密 KVM Encryption

本选项控制 RFB 协议的加密。控制台应用 RFB 把屏幕数据传递到管理员的机器并把键盘和鼠标数据传回到主机。

- Off：则不用加密。

- Try：Java 程序 applet 将尝试建立加密连接，如果不能建立加密连接，可以使用非加密连接方式。
- Force：applet 将建立加密连接，如果连接建立失败，会产生错误提示。

IP 通道的控制 IP Access Control

允许 IP 通道控制：如果选中，防火墙允许或阻拦某些特定客户机上的 IP 地址访问。

如果缺省的策略定为“Drop”，则所配置的 IP 地址或者地址段列表可以作为例外而被接受。如果缺省的策略定位“Accept”，IP 地址或 IP 地址段被配置为下拉异常。

网络或地址范围需要配置为 CIDR（Classless Inter-Domain Routing）符号，例如，192.168.1.0/24.它是由一个 IP 地址跟随“/”符合以及属于网络或地址段的数据组成。

基于组的系统通道控制 Group Based System Access Control

使能 IP 通道控制：

用户使用区

- 最大的失败登陆次数：允许用户尝试登陆 RMM2 的次数。每次失败的登陆都会被记录下来。缺省值为空。
- 封杀时间（分钟）：当用户超出允许尝试的登陆次数后，RMM2 将封杀用户登陆的时长。缺省值为空。

登陆限制

- 允许单用户登陆的限制：规定只有一个用户可以登陆到 RMM2。
- 密码老化限制：用户需要更改密码的时间间隔。

证书 Certification

RMM2 模块用安全链入层协议在自己和连接的客户机之间建立加密网络传输。在连接建立期间，RMM2 模块用密码证书向客户机显示自己的身份。在发行时，所有 RMM2 模块的证书和底层密钥是相同的，这不能和由用户为 RMM2 模块设定的网络设置匹配。证书的底层密钥也可用于 SSL 握手。 因此，这是一种安全风险(但是远比没有加密好)。 然而，可以生成和安装对于每一特定 RMM2 模块的唯一 base44 x.509 证书。为了实现它，RMM2 模块能生成一个新的密钥和需要认证机构认证的关联证书签字请求。认证机构核实你的身份和签字并为你颁发一个 SSL 证书。

为 RMM2 模块创建 SSL 证书，需要以下几步：

1. 填充证书签署要求页面上需要的选项。
2. 点击“Creat”按钮将生成开始证书签字请求。
3. 点击“CSR Download”下载 CSR 到你的管理机器上。
4. 发送存储的 CSR 到一家认证机构。经过较为复杂的传统认证程序（取决于认证机构），你将从认证机构得到新的证书。
5. 点击“Upload”按钮上载证书到 RMM2 模块上。

完成这些步骤之后，RMM2 模块拥有用于向客户机标识本模块的自己的证书。

警告： *如果你破坏了 RMM2 模块上的 CSR，将无法恢复！你必须按照上述步骤重新操作。*

图 3-26：Certificate Signing Request

- 通用名 Common name：这是当安装到用户的网络时，RMM2 模块的网络名称（通常是完整的有效域名）。它和通过浏览器访问 RMM2 模块时的名称一致，只是没有前缀“http：//”。 在此处给的名字和实际网络名字不同时的情况下，当用 HTTPS 访问 RMM2 模块时，浏览器将弹出安全警告。
- 单位 Organizational unit：本项用于具体说明本 RMM2 模块属于机构组织中的具体的部门。
- 组织 Organization：RMM2 模块属于的组织名称。
- 位置与城市 Locality/City：组织处于的城市。
- 州/省 State/Province：组织处于的州或省。
- 国家(ISO 代码)：组织所处国家。这是采用两字母 ISO 代码表示，例如，德国是 DE，美国是 US 等。
- 盘问口令 Challenge Password：有些认证机构要求一个盘问口令来授权对证书的后续修改（例如：废弃证书）。本口令的最短长度为 4 个字母。
- 确认盘问口令 Confirm Challenge Password：验证盘问口令。
- 电子邮件 Email：负责 RMM2 模块和其安全性的联系人的电子邮件地址。
- 密钥长度 Key length（bits）：1024 或 2048 字节。

使用如下步骤安装 SSL 证书：

1、 点击“ Download”去下载 CSR 到你的管理系统。
2、 发送存储的 CSR 到一家认证机构。经过较为复杂的传统认证程序（取决于认证机构），你将从认证机构得到新的证书。
3、 点击“Upload” 去上载证书到 RMM2。

完成这些步骤之后，RMM2 模块拥有用于向客户机标识自己模块的证书。

图 3-27 Install SSL

USB

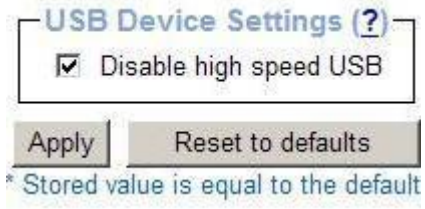


图 3-28：USB Device Settings

在该选内，可以禁止 USB 的高速模式以兼容 BIOS 对一些 Linux 操作系统的兼容性问题。然而，此项改变可能会降低虚拟设备仿真的速度。

IPMI

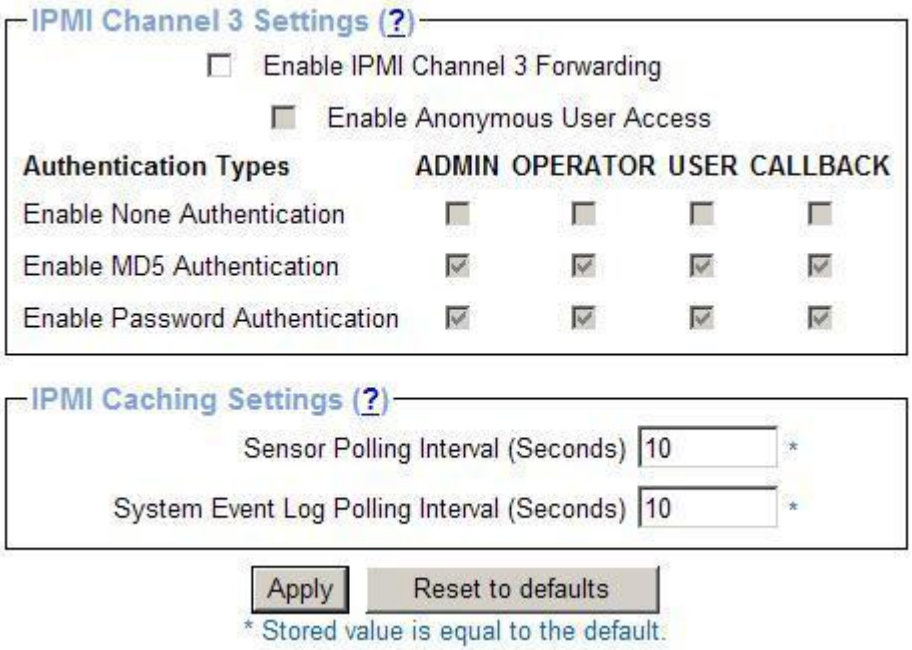


图 3-29：IPMI

在该页面内，可以设置 IPMI 的通道以及每次显示缓冲池更新的时间间隔。

日期与时间 Date And Time

本页可以设置 RMM2 的内部实时钟(参见图 3-30)。 你可以人工调整钟或者使用 NTP 时间服务器。没有时间服务器，你的时间设置将不一致，当 RMM2 卡掉电超过几分钟时，你不得不再次调整时间。为避免这个，你可以使用自动设定内部时钟到当前 UTC 时间的一个 NTP 时间服务器。 因为 NTP 服务器时间总是 UTC，可以允许设定静态偏移值来得到你的当地时间。

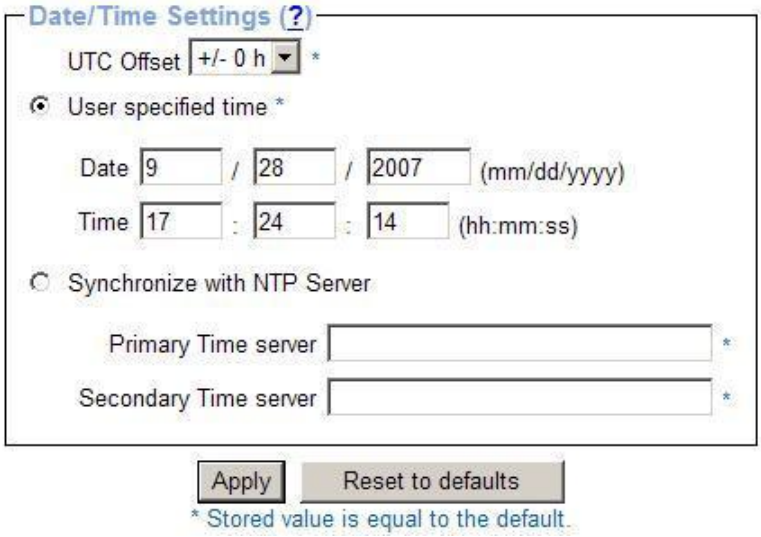


图 3-30：Date/Time

认证 Authentication

在该页面，您可以指定那些认证的用户可以进入 RMM2。本地认证要求在 RMM2 上产生用户信息以及相应在 RMM2 上认证的用户/组的信息。LDAP 与 RADIUS 允许你提供特定的 LDAP 或者 RADIUS 服务器名单用于登陆认证。

RMM2 使用 LDAP 或 RADIUS 仅用于密码的验证。用户的专有权以及私有设置是已经存储在 RMM2 里了。在用户经由 LDAP 或 RADIUS 登陆之前，其用户的帐号必须在 RMM2 上已经生成。所有的专有权设置必须在 RMM2 的用户管理里完成。

RADIUS 没有支持挑战/响应功能。

使用 RADIUS 协议访问一个远程设备时，首先您必须登录。 然后输入您的用户名和密码。RADIUS 服务器读取您的输入数据(认证)，RMM2 会寻找相应的配置信息(认证)。 配置信息定义了(或限制)您的行为，并且可能由于您的具体情况不同而不同。 如果没有这样的配置信息，您通过 RADIUS 的访问将被拒绝。 以远程行为机制方式通过 RADIUS 登陆就如同远程控制台一样。

如果半小时内没有动作发生，那么到 RMM2 的连接将会被终止并关闭。

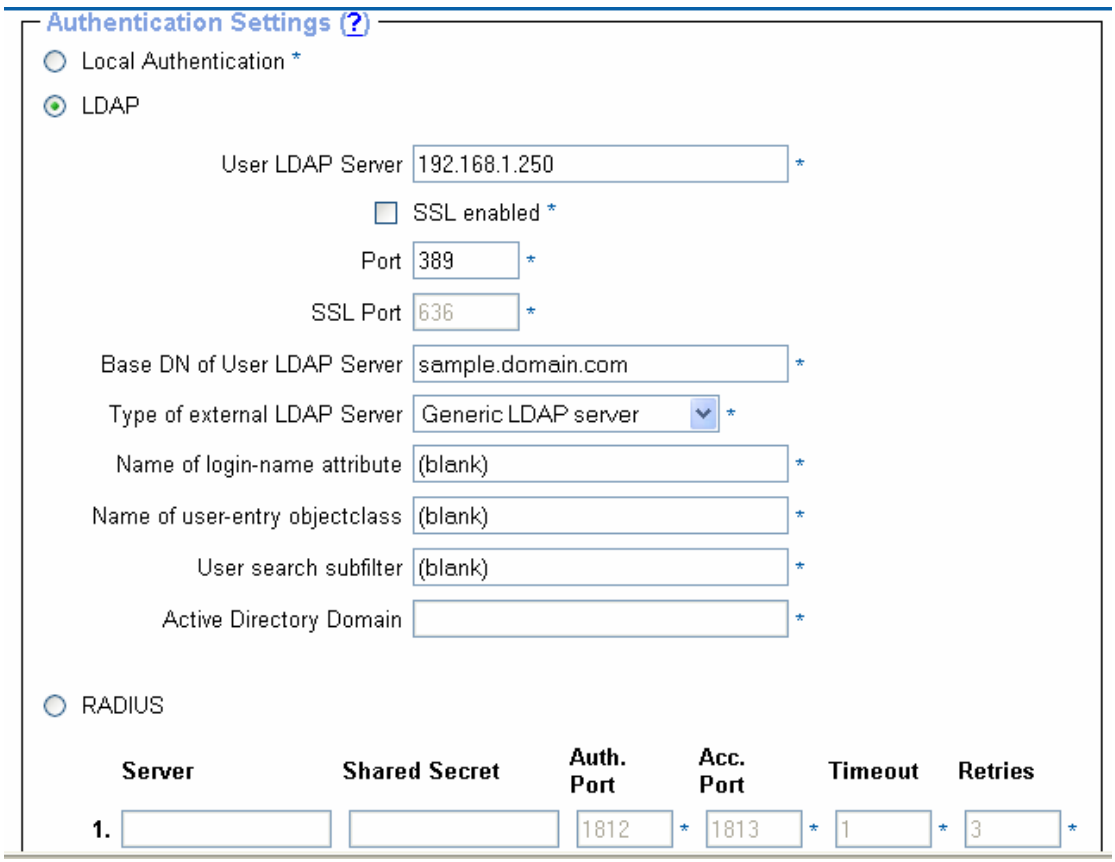


图 3-31：Authentication

LDAP

- 用户 LDAP 服务器：在这里，您输入 LDAP 服务器的名字或 IP 地址。如果您选择了一个名字而不是 IP 地址，那么您需要在网络设置中配置 DNS 服务器。
- 用户 LDAP 服务器的基本 DN（辨别名）：在用户 LDAP 服务器中，您在目录树开始的地方指定辨别名（DN）。
- 外在 LDAP 服务器的类型：用这个选项您设置了外部 LDAP 服务器的种类。因为一些服务器类型要求特别处理，因此这是必须的。另外，为采用 LDAP 策略适当地设置缺省值。 您能在一台通用的 LDAP 服务器， Novell 目录服务和微软激活目录之间选择。然后如果您既没有 Novell 目录服务，又没有微软激活目录，那么就选择一台通用 LDAP 服务器并编辑已用过的 LDAP 策略。
- 登陆名属性名称：这是包含整个用户登陆名属性的名称。如要使用默认的设置，此处保留空白。默认的设置取决于所选的 LDAP 类型。
- 用户登录权对象类的名字
- 这是在 LDAP 目录辨认一名用户的对象类。 要使用缺省，留此处为空。 缺省取决于选择的 LDAP 服务器类型。
- 用户搜索子过滤器：您可以在此处为用户提炼搜索结果，并且这些结果应当让高级管理卡知道。

- 激活目录域：这个选项说明激活目录域在微软的激活目录服务器中已经配置了。这个选项仅仅在你已经选择了微软的激活目录作为 LDAP 服务器类型是才生效。

Remote Authentication Dial In User Service (RADIUS)

- 服务器：可以输入 RADIUS 服务器的 IP 地址或是主机名来进行连接。使用主机名的话，DNS（动态域名服务器）必须得配置并开启。

- 共享密匙：一个共有密匙是指在 RADIUS 客户端和服务器端作为密码的一个文本字符串。在这个例子中，RMM2 作为 RADIUS 客户端。一个共有密匙是用来确认 RADIUS 消息时被 RADIUS 驱动的被配置拥有相同密匙的设备发送的，以及确认 RADIUS 消息在传输过程中未被修改（消息完整性）。对于共有的密匙，您能使用其中任一标准字母数字和特殊字符。一个共有密匙共由 128 个字符组成。

- 认证端口：RADIUS 服务器用于侦听认证请求的端口。缺省值为＃1812。

- 帐号端口：RADIUS 服务器侦听帐号请求的端口。缺省值为＃1813。

- 超时：请求有效的秒数。该时间主要用于等待一个请求的完成。如果请求工作没有在规定的时间内完成，该请求将被取消。缺省的时间为 1 秒。

- 重试：允许一个请求重试的次数。缺省的次数为 3 次。

- 全球认证类型：认证协议。可以使用非加密 PAP 协议（Password Authentication Protocol）或者加密 CHAP 协议（Challenge Handshake Authentication Protocol）。

SMTP 设置 SMTP Settings

本页面为事件日志配置邮件服务器和发送邮件的源地址。如果 RMM2 内部事件允许通过 Email 方式发送通知，需要在事件页面中使能 SMTP。具体设置页面参见图 3－32

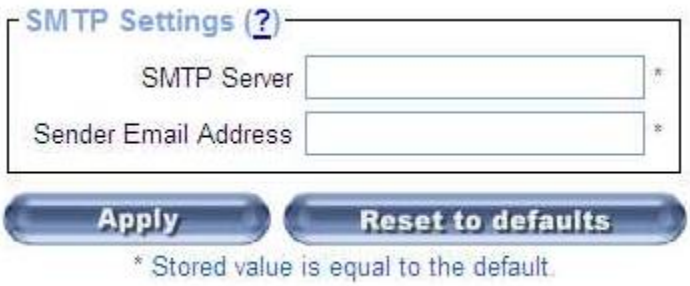


图 3-32：SMTP Settings

事件日志 Event Log

RMM2 内部事件，如登陆失败或某一固件更新，将被记录在选定的地方（参见图 3－33）。每个事件属于一个能被单独激活的事件组。

在事件日志设置中，你可以选择每页显示多少条记录。另外，你可以在此清除日志文件。

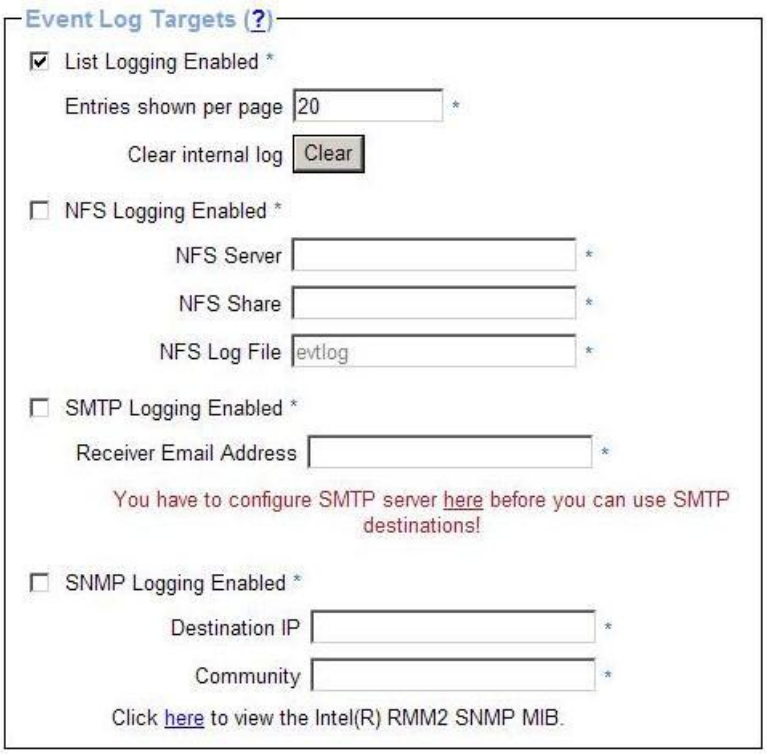


图 3-33：Event Log

事件报告对象 Event Log Targets

- 使能日志列表 List logging enabled：你可以用 RMM2 卡的内部日志列表记录事件。因为 RMM2 卡的系统内存用来存储所有信息，受限于 RMM2 系统内存的大小，最大记录的条数为 1000。超过这个限制的每条记录将会自动覆盖最老的一条记录。
- 使能 NFS 日志 NFS Logging enabled：为了将所有数据写入指定位置的文件，指定 NFS 服务器，在 NFS 服务器上存在输出指向的目录或静态连接。可以将一个以上的 RMM2 卡的日志数据写入一个 NFS 共享，但必须为每一个卡定义一个唯一的文件名。当改变 NFS 设置并按“Apply”按钮，NFS 共享将立即加载。这意味着 NFS 共享和 NFS 服务器必须均有效，否则将得到出错信息。
- 使能 SMTP 日志 SMTP Logging enabled：应用本选项，RMM2 卡能发送电子邮件到事件日志设置中电子邮件地址域中提供的邮件地址。这些邮件包括与内部日志文件相同的描述字串，邮件主题是当前发生的日志事件的事件组。为了应用这一日志指定，你必须指定可以从 RMM2 卡访问的 SMTP 服务器，不需要任何认证。(<serverip>:<port>)。
- 使能 SNMP 日志 SNMP Logging enabled：如果本项被激活，每当日志事件发生，RMM2 卡将向一个特定 IP 地址发送一个 SNMP 托盘。如果接收者要求串，你可以在相应文本域中设定。大多数事件托盘仅包含一个日志事件信息的描述串。只有认证和主机电源事件有包括自己的托盘类，该类由包含发生事件详细信息的几个域构成。为接收 SNMP 托盘，可以用任何 SNMP 托盘侦听。

事件日志指派 Event Log Assignment

你可以选择 RMM2 的何种动作将被存入日志文件。选定相应的框并点击"Apply"确认你的选择。

SNMP

通过 SNMP，您可以获得以下信息：

- 系列号
- 固件版本号
- MAC 地址 / IP 地址 / 子网掩码 / 局域网接口的网关
- 服务器的电源状态

- 服务器 POST 代码

通过 SNMP，您可对以下行为进行初始化：
- 重设服务器
- 开启/关闭服务器电源
- 重启 RMM2 模块

以下事件会被 RMM2 经由 SNMP 报告出来：
- 登陆 RMM2 失败
- 登陆 RMM2 成功
- 拒绝接入一个特定的行为
- 服务器重启
- 服务器被重新开/关电源
- 使能 SNMP 客户端：如果设置了此项，那么 RMM2 将会回应 SNMP 的请求。

提醒：如果某一选项没有设置，那么您将不能进行相应的请求操作。例如，如果您不想禁止重启 RMM2 通过 SNMP 的功能，那么就不要设置写功功能项。

图 3-34：Enable SNMP

- 读功能项：这是 SNMP 功能，它允许您通过 SNMP 收回信息。
- 写功能项：这个功能允许您设置选择项并且通过 SNMP 重设 RMM2 卡或者主机。例如，所有影响主机的功能或 RMM2 卡。
- 系统定位：输入一个描述主机物理位置的信息，这个信息将被用来回复 SNMP 请求“sysLocation.0.”。
- 系统联系人：为主机输入一个联系人，这个参数将被用于回复 SNMP 请求 "sysContact.0.”。
- 点击此处查看 SNMP MIB：从 Web 浏览器上查看或保存 SNMP MIB 文件。当一个 SNMP 客户端与 RMM2 进行通信时，该文件可能需要。

语言 Language

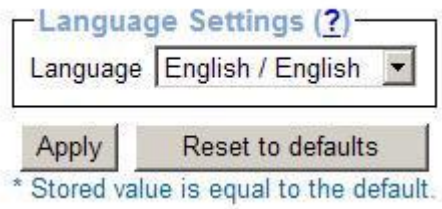


图 3-35：Language

在该菜单下可以选择需要的语言，目前提供的语言有：英文，德文两种语言界面；

维护 Maintenance

该菜单包含 4 个选项：

- Device Information 设备信息
- Event Log 事件日志
- Update Firmware 更新固件
- Unit Reset 单元重启

图 3-36：Maintenance

设备信息 Device Information

图 3－37 显示了 RMM2 的概要信息并允许你对该模块进行重启。

图 3-37：Device Information

连接的用户 Connected User：从左到右显示了已连接的用户，它们的 IP 地址(用户来自的主机)和其活动状态。“RC”意味着远程控制台是开放的。

事件日志 Event Log

图 3-38：Event Log

图 3－38 显示了事件日志列表。它包括 RMM2 保存的事件，以及事件的时间，事件的简短描述和请求来自的 IP 地址。你可以用“前页”和 “后页”来浏览数据。

- 点击“Prev”与“Next”分别浏览前页与后页的数据信息；
- 点击“Clear”清除所有日志信息；

更新固件 Update Firmware

为了添加新的功能和特殊性能，RMM2 的固件可以被远程更新。新的固件更新可以通过电子邮件发送给你或通过 Lenovo 网站上下载相应的更新固件文件。

警告：*固件的更新是不可逆转的，同时需要花费几分钟时间。在更新过程中，不要对远程电源进行操作。*

图 3-39：Firmware Upload

更新固件的步骤：

1、 下载需要更新固件的文件；
2、 在上载页面上，点击右侧的“浏览”按钮选择相应的 FW 文件。
3、 点击“Upload”，固件文件将传送到 RMM2 上。在上载过程中，会检查固件文件的有效性以及是否发生传送错误。任何错误如果被识别出来，上载将终止。
4、 如果上载顺利完成，在出现的更新固件窗口中会显示当前运行的固件版本以及新上载的固件版本号。点击“upload”按钮，将会替代旧版本。
5、 等待 RMM2 自动重启。页面会自动回到登陆页面，输入用户名与密码后会再次登陆。

单元复位 Unit Reset

图 3-40 Unit Reset

这部分允许你重启某些特殊设备。其中重启键盘/鼠标，USB，视频引擎仅需要几秒钟的时间。不会对当前的连接造成影响。

设备自重启主要是满足更新固件的需要。该选项将关闭所有连接并需要花费大约 30s 的时间。

注意：*只有作为“Admin”的用户才能重启 RMM2。*

第四章 远程控制台（KVM）

远程控制台是将 RMM2 所在主机的键盘，鼠标，显示页面重定向。

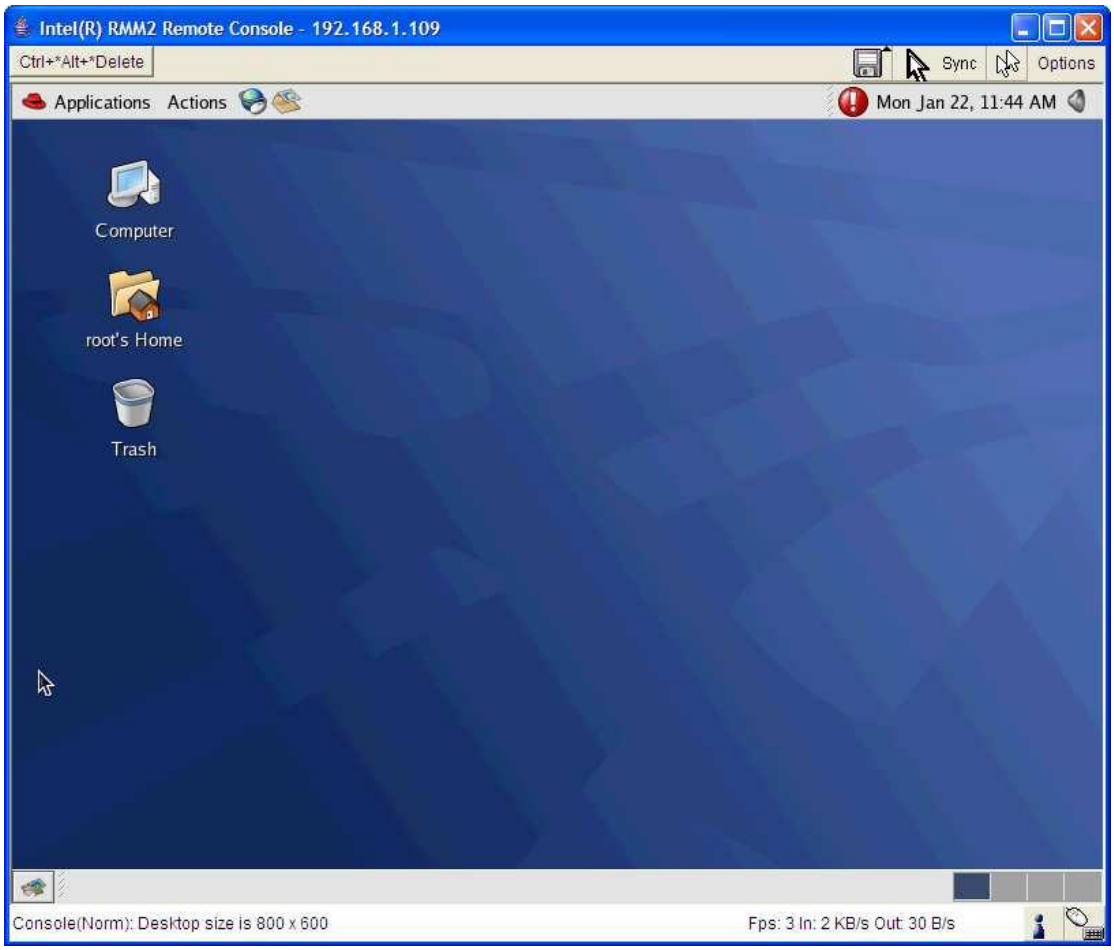


图 4-1：Remote Console Page

远程控制台窗口是一个基于 Java 的程序，它通过 TCP 连接到 RMM2。运行这一连接的协议既不是 HTTP，也不是 HTTPS，它是 KVM 专有的协议。该协议使用的端口为＃443。所以本地的网络环境必须允许该连接。诸如，你的防火墙，以及为了避免你的私有的内部网络，你的 NAT（Network Address Translation）设置不得不进行配置。

主窗口

远程控制即将会打开一个新窗口显示远端服务器屏幕上的内容。远程控制执行的动作就犹如你直接坐在远程主系统的屏幕前执行的效果，也就意味着键盘和鼠标能以通常的方式应用。只是键盘和鼠标的动作会有一点轻微的延迟，具体延迟程度取决于你连接 RMM2 所占用的带宽情况。

远程控制台窗口将以最优的尺寸显示远端的屏幕。它将识别远程服务器端屏幕的分辨率

大小并跟随它的分辨率大小，从而使显示窗口为最优的效果。如果对显示效果不满意，还可以在控制端调整远端显示窗口的分辨率，直至符合要求。

远程控制状态条

远程控制台底部为状态，它显示控制台的连接状态。括弧中的值描述远程控制的连接.“Norm”意味着一种没有加密的标准连接，“SSL”表明使用了 SSL 的一种安全连接。

图 4-2：Status Line

状态行中的数字表示刷新缓冲帧数（“Fps”）与输入(“In:”)与输出(“Out:”)的网络压缩传输率（KB/s）。

状态行右部图标表示的意义为：

 一个用户连接到 RMM2 的远程控制台

 多于一个用户连接到 RMM2 的远程控制台。

 你所独有的专有通道。任何其它用户不能通过远程控制台访问远程主系统，除非你关闭该选项。

 另一个远程用户正以专有权方式进入。你不能通过远程控制台访问远程主系统，除非那个远程用户关闭该选项。

 “Monitor Only”选项被禁止，键盘/鼠标还是可以有效执行。

 “Monitor Only”选项处于使能状态。

远程控制条

远程控制窗口上部包含了一个控制条。使用它的元素你能看到远程控制台的状态和本地远程控制设置的影响。每部分执行的功能如下所述：

一些控制选项仅在 KVM Settings：Keyboard/Mouse 页面中选择“Other Operating System”才可见。详细介绍请见 P29“Keyboard/Mouse”.

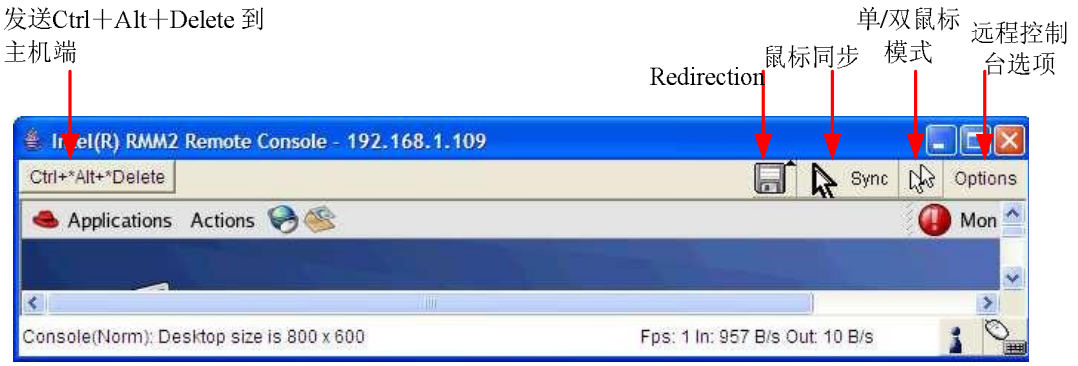


图 4-3 Remote Console’s control button

Ctrl + Alt +Del

该图标是发送“Ctrl+Alt+Del”组合键信息到远程主系统(也可见第 3 章中 KVM Settings 部分定义新的按钮键)。

注：对“超级”用户这个键是缺省存在的。 其它用户需要自己定义此按钮。

Redirection

点击该按钮，会出现重定向画面，在该菜单下，可以重定向本地的驱动（只在 Windows 下可用）或者 ISO CD/DVD-ROM 的镜像文件。

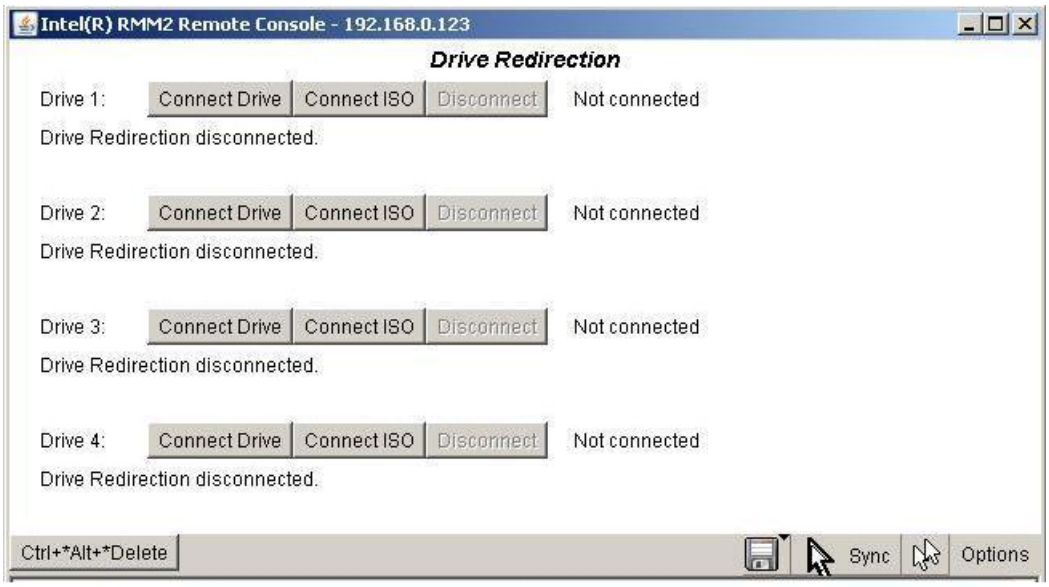


图 4-4：Redirection

同步鼠标 Sync

点击同步鼠标将会使本地的鼠标同远程的鼠标指针保持同步。当主机系统采用鼠标加速的设置时选择该选项尤其必要。通常这里不需要改变鼠标的设置。该选项只在 KVM Settings: Keyboard/Mouse 中选择“Other Operating System”时才会显示出来。

单/双鼠标模式

选择单鼠标模式将只显示远程的鼠标指针，而双鼠标模式将显示本地与远程鼠标，选择双鼠标模式，鼠标指针需要同步。如果选择 SUN*JVM，单鼠标模式需要 SUN 的 JVM 1.4 或更高版本的支持。

在单鼠标模式，按动 ALT＋F12 将会获取本地的鼠标指针。

远程控制选项

远程控制选项包含如下选项。

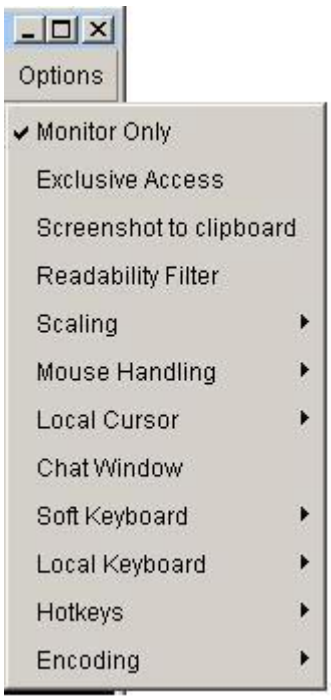


图 4-5：Option

- Monitor Only：打开/关闭监控过滤。当监控过滤处于开的状态，远程控制台交互不可用，远程监控的屏幕只能被查看。
- Exclusive Access：专有权通道，如果用户获得该权限，他能强迫关闭所有其它使用远程控制台的用户，并且其他用户不能打开远程控制台，直到专有用户关闭这一特殊权限或者注销退出。
- Screenshot to clipboard：捕获获远程控制台的屏幕页面。如果需要截图，只需点击该选项，RMM2 会讲截图放置在剪切板上。
- Readability Filter：打开/关闭可读滤波器。当选为“开”状态时，滤波器会保留屏幕上大多数细节，即便是减小了原有屏幕的缩放比例。该选项仅在 JVM1.4 或更高版本上才能应用。

  在状态行里可以改变通道模式，更多详细信息参见远程控制状态行。
- Scaling：可以调整远程控制台呈现的屏幕尺寸的缩放比例。你仍然能使用鼠标和键盘，但是缩放的算法并不保留所有显示的细节。
- Mouse Handling：当使用软鼠标模式时，同步本地与远程的鼠标指针。该选项仅在 KVM Setting：Keyboard/Mouse 中的操作系统类型中选中“Other Operating Systems”才会显示，具体请见 P29 页内的“Keyboard/Mouse”部分。

  －快速同步：仅是固定斜率的暂时正确；

  －智能同步：如果快速同步不能生效或者主系统的鼠标设置已经发生改变时，选用此功能；

  －单/双鼠标模式：单鼠标模式，即只显示远程鼠标指针，本地鼠标不会呈现，直接利用远程鼠标进行操作。如果想跳出该模式，需要按动鼠标切换的快捷键 “Alt＋F12”，该快捷键方式可以自定义设置，该选项仅在选择 KVM settings：Keyboard/Mouse 的操作系统种类中选择“Other Operating Systems ”才会显示出来。具体请参见 P29 页内的“Keyboard/Mouse”部分。

- Local Cursor：Local Cursor 提供一个列表以供选择，以区分本地鼠标指针。选择的形式将被保留下来，并在下次用户登录远程控制台时激活。具体可供使用的形状取决于 Java Virtual Machine 的版本提供的列表。
- Chat Windows：打开一个聊天窗口，可以直接与其他登陆到 RMM2 卡的用户直接进行通讯交流。
- Soft Keyboard：仿真远程系统的键盘。使用软键盘发送键码与键盘的顺序到远程系统。如果远程系统使用的是不同语言与国家的键盘映射，该功能尤其有效。

  在软键盘的使用中，发送单一键就是通过点击软键盘上的键，就会立刻生效。如果发送特殊的键值，诸如 Ctrl，Shift 或其它功能键，需要点击这些键两次。第一次点击代表“键被按压”，第二次点击代表“按压的键被释放”。在第一次按压，按压的键改变颜色表明键被按压下了，在第二次点击键返回正常颜色，表明该键已经被释放。

  举例来说：

  发送组合键 Ctrl＋C：

  - 点击“Ctrl”一次，屏幕上该键会改变颜色。
  - 点击“C”一次，因为“C”不是特殊键，因而 Ctrl 与 C 键同时被释放，该组合键会被发送到远程系统中。两个键会返回到正常颜色。

  发送组合键 Ctrl＋F5

  - 点击“Ctrl”一次。屏幕上的键会改变颜色。
  - 点击“F5”两次。最后一次点击会同时释放两个键并将该组合键发送至远程系统。这两个键返回正常颜色。

  发送组合键 Alt＋Shift＋F4：

  - 点击“Alt”一次，屏幕上的该键改变颜色。
  - 点击“Shift”一次，屏幕上的该键改变颜色。
  - 点击“F4”两次。最后一次点击释放这三个键，并同时将该组合键发送至远程系统。这三个键返回正常颜色。

  －Show：显示软键盘。

  —Mapping：选择相应国家与语言的软键盘图。
- Local Keyboard：改变运行在远程控制台系统上的语言映射关系。正常情况下，远程控制台 Applet Java 运行程序会自动适配正确的语言。但是 JVM 与浏览器设置可能需要手动修改。举例来说：一个德国人的本地系统使用一个 US－英文的映射键盘。
- Hotkeys：呈现一个之前定义的热键列表。在发送到远程主系统之前，会弹出一个确认框进行确认。
- Encoding：调整压缩率与颜色深度的代码级别。这些仅在采用自动传送方式时才会获取。

  －Compression Level：可以在数值 1 到 9 之间进行选择。压缩品质越低，意味着传送的数据越多，整个图形页面的传送时间会更长。

  级别 0 表示关闭视频压缩。级别 1 使能压缩，级别 9 代表最大的压缩率。

  最好的压缩级别是网络带宽与两个单显示器交换数据量的折衷。如果网络带宽比较小，采用较高的压缩级别。压缩级别越高，每一边连接到显示器需要压缩与解压缩的时间会更长。而压缩品质主要取决于显示画面。

  －Predefined Compression：有损失的压缩可能会导致页面品质的下降。

  －Lossy Compression：显示事先调整的压缩选项。

－Color Depth：设置期望的颜色深度。颜色深度越高，需要被捕获和传送的显示信息越大。在 8-bit 或 16-bit 之间，选择对应压缩级别 0，在 1-bit 或 8-bit 之间，选择压缩级别 1 到 9。