OPMA M3-G4
User Manual

Contents

Contents ... iii

Tables ... vi

Figures ... vii

Preface ... ix
- Copyright ... ix
- Document Version and Date ... ix
- Trademarks ... ix
- About the OPMA Module ... x
- Limited Warranty ... x
- Limitations of Liability ... x
- Technical Support ... x

Chapter 1: The Quick Start Guide ... 1
- About the OPMA M3-G4 Module ... 1
- Connecting the OPMA Module to the Host System ... 1
- Initial Network Configuration ... 2
- Web Interface ... 2
- The Remote Console ... 3

Chapter 2. Introduction ... 4
- General Information ... 4
- Features ... 4
- OPMA add-on Card System Components ... 5
- When the Server is up and running ... 5
- When the Server is dead ... 5

Chapter 3. OPMA Installation Guide ... 7
- About the OPMA add-on card ... 7
- Connectors ... 7
  - Connecting the OPMA add-on card to the Host System ... 7
  - Connecting the Ethernet ... 8
  - 10 Mbps Connection ... 8
  - 100 Mbps Connection ... 8

Chapter 4. OPMA Modul Configuration ... 9
- Initial Configuration ... 9
- Initial Configuration via DHCP Server ... 9
- Initial Configuration via Serial Console ... 9
- Web Interface ... 12
- Mouse and Keyboard Configuration ... 12
  - Remote Mouse Modes ... 12
  - Remote Mouse Settings ... 13
  - Auto Mouse Speed and Mouse Synchronization ... 13
  - Host System Mouse Settings ... 14
  - Single and Double Mouse Mode ... 15
  - Recommended Mouse Settings ... 15
  - Video Modes ... 15
- Resetting the OPMA module to its Factory Settings ... 16
  - Using the Serial Interface ... 16
  - Using KiraTool ... 16

Chapter 5. OPMA Module Usage 17
Prerequisites 17
Login and Logout to the OPMA Module 18
Login into the OPMA Module 18
Navigation 19
Logging out of the OPMA Module 20
The Remote Console 20
General Description 20
Main Window 21
Remote Console Control Bar 21
Remote Console Options 24
Remote Console Status Line 30
Optimizing the Video Picture 31
Using the OPMA module with low bandwidth 32

Chapter 6. Menu Options 33
Remote Control 33
KVM Console 33
Virtual Media 34
Floppy Disk 34
CD ROM 35
Drive Redirection 39
Options 44
Creating an Image 45
System Health 47
Chassis Control 47
Monitor Sensors 48
System Event Log 49
System Alert Management 50
User Management 52
Change Password 52
Users And Groups 53
KVM Settings 56
User Console 56
Keyboard/Mouse 59
Device Settings 61
Network 61
Dynamic DNS 64
Security 66
Certificate 71
USB Device Settings 74
Date And Time 75
Authentication Settings 76
Event Log 79
SNMP 82
Maintenance 85
Device Information 85
Event Log 86
Update Firmware 87
Unit Reset 88

Appendix A: Troubleshooting 90

Appendix B. Glossary 92

Appendix C. KiraTool Commands 94
Supported Operating Systems 94
Supported Interfaces 94
Supported Functionality 94
Usage 94
Return Code 97

Appendix D. Configuring the RADIUS Server 98
Prerequisites 98
Add and configure a RADIUS client 98
Setup a custom remote access policy 99

Appendix E. Key Codes 101

Appendix F. Pin Assignment 103
OPMA Connector 103
RJ45 Connetcor Ethernet 103
Serial SUB-D9 Connectors 103

Appendix G. Specifications 105
Sizes and Weights 105
Environment 105
Temperature 105
Humidity 105

Appendix H. Raritan Inc. Warrenty Information 106
Limited Warranty 106
Customer Remedies 106
No Other Warranties 106
No Liability For Consequential Damages 106

Appendix I. GNU General Public License (GPL) 107

Appendix J. The OpenLDAP Public License 112

Tables

Table 1 - 1. Initial Network Configuration........ 2
Table 1 - 2. Login Settings........ 2
Table 2 - 1. Hardware Failures 5
Table 2 - 2. Host System Failures and how they are detected 6
Table 4 - 1. Initial Network Configuration........ 9
Table 4 - 2. Serial Line Parameters........ 10
Table 4 - 3. Standard User Settings........ 12
Table 5 - 1. Standard User Settings........ 19
Table 5 - 2. Front End Buttons........ 20
Table 5 - 3. Buttons displaying the Access State........ 31
Table 5 - 4. Buttons displaying the Monitor Only State 31
Table 6 - 1. Event Log Assignments........ 81
Table C - 1. Options Overview 94
Table C - 2. Commands Overview 95
Table C - 3. Return Codes Overview 97
Table E - 1. Key Names........ 101
Table F - 1. RJ45........ 103
Table F - 2. Serial Sub D9 Connector 1 104
Table F - 3. Serial Sub D9 Connector 2 104
Table G - 1. OPMA Specification........ 105
Table G - 2. Temperature........ 105
Table G - 3. Humidity 105

Figures

Figure 1 - 1. OPMA M3-G4 Module........ 1
Figure 1 - 2. Top Part of the Remote Console for “Windows Operating Systems”........ 3
Figure 1 - 3. Top Part of the Remote Console for “Other Operating Systems”........ 3
Figure 2 - 1. OPMA M3-G4 Module........ 4
Figure 3 - 1. OPMA add-on Module........ 7
Figure 4 - 1. Remote Console Control Bar: Sync Button........ 14
Figure 5 - 1. The Internet Explorer displaying the Encryption Key Length........ 18
Figure 5 - 2. Login Screen........ 18
Figure 5 - 3. Main Page........ 19
Figure 5 - 4. Remote Console........ 20
Figure 5 - 5. Remote Console Control Bar........ 21
Figure 5 - 6. Remote Console Applet Drive Redirection Menu........ 22
Figure 5 - 7. Redirecting a Local Drive........ 22
Figure 5 - 8. Redirecting an ISO Image........ 23
Figure 5 - 9. Successfully Drive Redirection Connection........ 23
Figure 5 - 10. Remote Console Options Menu........ 24
Figure 5 - 11. Remote Console Options Menu: Scaling........ 25
Figure 5 - 12. Remote Console Options Menu: Mouse Handling........ 25
Figure 5 - 13. Remote Console Options Menu: Local Cursor........ 26
Figure 5 - 14. Remote Console Options Menu: Chat Window........ 26
Figure 5 - 15. Remote Console Options Menu: Soft Keyboard........ 27
Figure 5 - 16. Remote Console Options Menu: Soft Keyboard Mapping........ 28
Figure 5 - 17. Remote Console Options Menu: Local Keyboard........ 28
Figure 5 - 18. Remote Console Options Menu: Hotkey Confirmation Dialog........ 28
Figure 5 - 19. Remote Console Options Menu: Encoding Compression........ 29
Figure 5 - 20. Remote Console Options Menu: Predefined Encoding Compression........ 29
Figure 5 - 21. Remote Console Options Menu: Lossy Compression........ 30
Figure 5 - 22. Remote Console Options Menu: Color Depth........ 30
Figure 5 - 23. Status Line........ 30
Figure 5 - 24. Status Line Transfer Rate........ 31
Figure 6 - 1. KVM Console........ 33
Figure 6 - 2. Virtual Floppy Area........ 34
Figure 6 - 3. Select Image File........ 34
Figure 6 - 4. CD-ROM Selection........ 35
Figure 6 - 5. The Image File on the Share........ 36
Figure 6 - 6. Explorer Context Menu........ 37
Figure 6 - 7. Share Configuration Dialog........ 38
Figure 6 - 8. Drive Redirection........ 39
Figure 6 - 9. Main View........ 40
Figure 6 - 10. Selecting the Desired Drive........ 41

Figure 6 - 11. Selecting Write Support 42
Figure 6 - 12. Device Authentication 42
Figure 6 - 13. Tray Info.......... 43
Figure 6 - 14. USB Mass Storage Option.......... 44
Figure 6 - 15. RawWrite for Windows Selection Dialog 45
Figure 6 - 16. Nero Selecting Dialog.......... 46
Figure 6 - 17. Chassis Control 47
Figure 6 - 18. Monitoring Remote Sensors Screen 48
Figure 6 - 19. System Event Log Screen.......... 49
Figure 6 - 20. System Alert Settings.......... 50
Figure 6 - 21. System Alert Policy Settings 50
Figure 6 - 22. System Alert LAN Destinition Settings.......... 51
Figure 6 - 23. Set Password 52
Figure 6 - 24. Set User 53
Figure 6 - 25. Set Permissions for the Group “user” 55
Figure 6 - 26. User Console Settings (Part 1) 56
Figure 6 - 27. User Console Settings (Part 2) 57
Figure 6 - 28. Keyboard and Mouse Settings.......... 59
Figure 6 - 29. Network Settings.......... 61
Figure 6 - 30. Dynamic DNS 64
Figure 6 - 31. Dynamic DNS Scenario 64
Figure 6 - 32. Device Security 66
Figure 6 - 33. Example of Use for IP Access Control.......... 69
Figure 6 - 34. Example of Use for the Group based System Access Control 69
Figure 6 - 35. Device Security (Part 2).......... 70
Figure 6 - 36. Certificate Settings 71
Figure 6 - 37. SSL Certificate Upload 72
Figure 6 - 38. USB Device Settings.......... 74
Figure 6 - 39. Date and Time 75
Figure 6 - 40. LDAP and other Authentication Settings.......... 76
Figure 6 - 41. Event Log.......... 79
Figure 6 - 42. SNMP Settings 82
Figure 6 - 43. Device Information.......... 85
Figure 6 - 44. Connected Users 85
Figure 6 - 45. Event Log List 86
Figure 6 - 46. Update Firmware.......... 87
Figure 6 - 47. Unit Reset.......... 88
Figure E - 1. English (US) Keyboard Layout, used for the Key Codes 101

Preface

Copyright

Peppercon AG

Scheringerstr. 1

08056 Zwickau

Germany

Document Version and Date

Version: 1.9

Date: Thursday, December 13, 2007

Trademarks

Raritan acknowledges the following trademarks:

- Intel is a registered trademark of Intel Corporation.
- Windows 98, Microsoft Windows,Windows NT, Windows 2000 and Windows XP are trademarks of Microsoft Corporation.
- IBM, AT, VGA, PS/2, and OS/2 are registered trademarks and XT and CGA are trademarks of International Business Machines Corporation.
- Raritan is a registered trademark of Raritan Incorporated.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Raritan disclaims any proprietary interest in trademarks and trade names other than its own.

The firmware of this product uses in part software under GPL licence. See Appendix D for the license text.

This product includes software developed by the University of California, Berkeley and its contributors.

This software is based in part on the work of the Independent JPEG Group.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Authors: Raritan Team

About the OPMA Module

The OPMA module (OPMA M3-G4) provides remote server management capabilities: you can use the OPMA add-on card to manage and monitor components in your servers. The OPMA M3-G4 offers a comprehensive hardware solution for server management.

Limited Warranty

The buyer agrees that if this product proves to be defective, Raritan is only obligated to repair or replace this product at Raritan's discretion according to the terms and conditions of Raritan's general trading conditions.

Raritan shall not be held liable for any loss, expenses or damage, directly, incidentally or consequentially resulting from the use of this product. Please see the Warranty Information shipped with this product for full warranty details.

Limitations of Liability

Raritan shall in no event be held liable for any loss, expenses or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential (whether arising from the design or use of this product or the support materials provided with the product). No action or proceeding against Raritan may be commenced more than two years after the delivery of the product to the buyer.

The licensee agrees to defend and indemnify Raritan from any and all claims, suits, and liabilities (including attorney's fees) arising out of or resulting from any actual or alleged act or omission on the part of Licensee, its authorized third parties, employees, or agents, in connection with the distribution of Licensed Software to end-users, including, without limitation, claims, suits, and liability for bodily or other injuries to end-users resulting from use of Licensee's product not caused solely by faults in Licensed Software as provided by Raritan to Licensee.

Technical Support

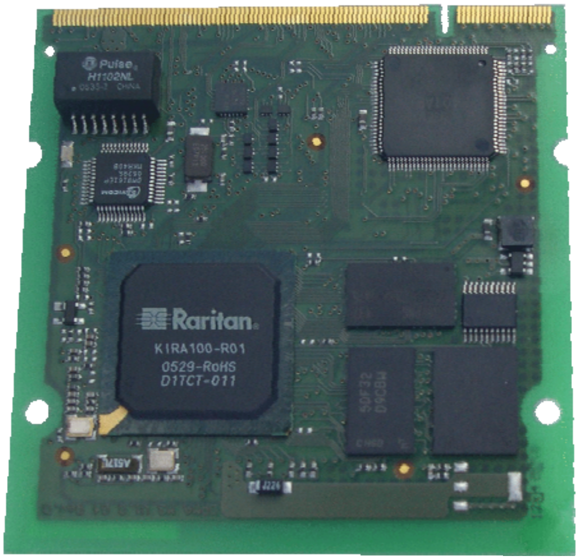
If you need help installing, configuring, or running the OPMA, call your Raritan Technical Support representative.

We invite you to access Raritan's Web site (www.raritan.com) where you shall find all modifications made after the editorial deadline. You may also contact us via e-mail to support@raritan.com.

Chapter 1: The Quick Start Guide

About the OPMA M3-G4 Module

Figure 1 - 1. OPMA M3-G4 Module



The OPMA add-on card provides remote server management capabilities. You can use the OPMA add-on card to manage and monitor components in your servers through the WAN/LAN. The OPMA add-on card offers a comprehensive hardware solution for server management.

One of the key features of the OPMA Module is an integrated BMC (Board Management Controller). This allows you to not only collect the data from the motherboard sensors but the OPMA can take an active role in controlling the motherboard fans and actors.

Connecting the OPMA Module to the Host System

Warning: Please note: the firmware of the OPMA board delivered to you is customised for use with the specified motherboard. If you use your OPMA module in a motherboard with a different sensor and actor configuration it will most probably not operate correctly.

Connecting the OPMA module to the Host System is easy: turn off the host, find the OPMA slot and carefully insert the OPMA module into the slot.

Note: *In order to download the OPMA Specification you may go to* ***http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/32200.pdf***

Warning: You should disconnect the host from the power supply completely, including disconnecting the power supply cable.

Initial Network Configuration

Initially, the OPMA network interface is configured with the parameters shown in **Table 1 - 1**.

Table 1 - 1. Initial Network Configuration

Parameter	**Value**
IP auto configuration	DHCP
IP address	-
Netmask	255.255.255.0
Gateway	none

Warning: If the DHCP connection fails on boot up, the OPMA will not have an IP address and will not function on the network.

If this initial configuration does not meet your local requirements, adjust the values to your needs. To retrieve the IP address of the OPMA add-on card , you could look into the records on the DHCP server.

Needless to say, there are special tools provided by us to ease the configuration and setup of the OPMA board. One of these tools is called “KiraTool”. The “KiraTool” is a small command line based tool which is used for configuring and testing the OPMA module. It can be used in environments where the web frontend cannot be used. On the delivered CD ROM is provided a KiraTool version for Windows, LINUX and DOS.

Web Interface

The OPMA add-on card may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the OPMA add-on card into your web browser.

The OPMA module will require you to change the administrators password to one of your choice during the first login.

The initial login settings for the web interface are as follows:

Table 1 - 2. Login Settings

User	Pasword
super	pass

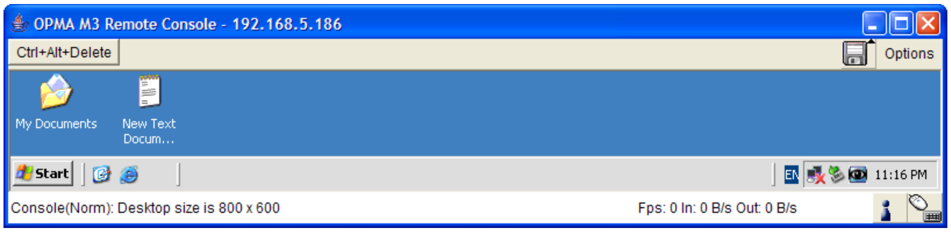
The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system in which the OPMA is installed. The web browser which is used for accessing the OPMA has to supply a Java Runtime Environment version 1.4 or higher.

Note: *You can get things working with lower numbered versions of the JAVA Environment, but we cannot guarantee that all features will be available.*

The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means that both the keyboard and mouse can be used in the usual way. Open the console by choosing the appropriate link in the navigation frame of the HTML frontend. **Figure 1 - 2** shows the top of the Remote Console.

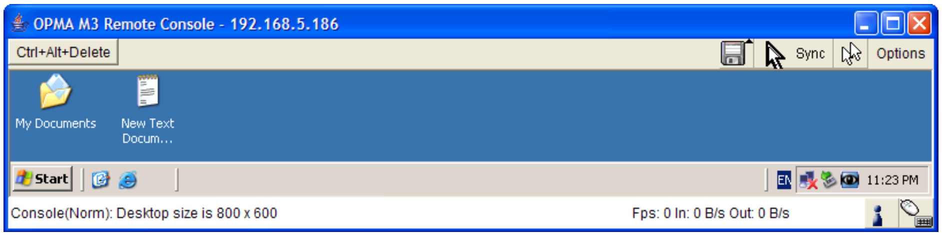
Figure 1 - 2. Top Part of the Remote Console for "Windows Operating Systems"



Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

Figure 1 - 3. Top Part of the Remote Console for "Other Operating Systems"



Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

Generally modern operating systems mouse devices are connected to the USB port. In this case you do not need to worry or configure mouse synchronisation and similar parameters. This generally applies to all "modern"Windows Operating Systems like Windows 2000 and 2003, XP etc. MacIntosh OS/X is the same. They use "Absolute Mouse Mode".

The following options are ONLY visible and available if you choose the option "Other Operating Systems" for the mouse.

In this case there are some options to choose from the menu, the most important one being the following:

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings there.

Chapter 2. Introduction

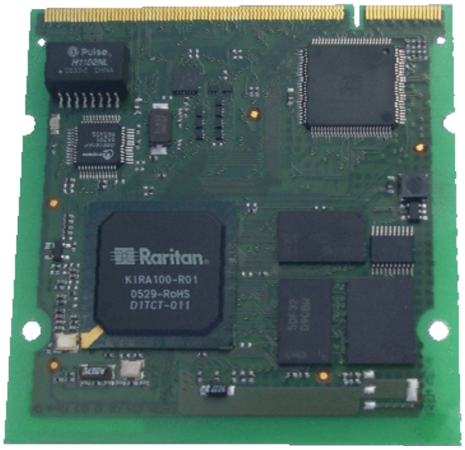
General Information

The OPMA add-on card is a manufacturer-independent remote administration system. It works as an integrated solution on your server system.

Based on an embedded operating system, the OPMA add-on card provides both exceptional stability and permanent availability independent of the present state of the servers operating system.

As a system administrator, you can use the OPMA Module's BMC to gain full control and location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

Figure 2 - 1. OPMA M3-G4 Module



Features

The OPMA add-on card defines a new class of remote access devices. It combines digital remote access via IP networks with IPMI-based comprehensive and integrated system management. The OPMA add-on card offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs on its embedded processors only but not on mission critical servers, so that there is no interference with server operation or impact on network performance. Furthermore, the OPMA add-on card offers integrated remote power management using IPMI. Key features of the OPMA add-on card are:

- OPMA Compliance
- IPMI V2.0
- KVM (keyboard, video, mouse) access over IP
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performancemouse tracking and synchronization
- Local Mouse suppression (only when using SUNs Java Virtual Machine)

OPMA add-on Card System Components

The OPMA add-on card is an add-on card with the following dimensions: 70mm (L) x 67.5mm (W).

The OPMA add-on card is shipped with:

- The actual OPMA module
- CD-ROM with documentation: Installation Guide and User Manual
- The Quick Start Guide

When the Server is up and running

The OPMA gives you full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server.

You can also perform periodic maintenance of the server. Using the Console Redirection Service you can do the following:

- Reboot the system (a graceful shutdown)
- Monitor the boot process
- Boot the system from a separate partition to load the diagnostic environment
- Run special diagnostic programs

When the Server is dead

Obviously, fixing hardware defects is not possible using a remote management device. Nevertheless, the OPMA gives the administrator valuable information about the type of a hardware failure.

Serious hardware failures can be categorized into five different categories with different probabilities. [1]:

Table 2 - 1. Hardware Failures

Category	Probability
Hard disk failure	50%
Power cable detached, power supply failure	28%
CPU, Controller, motherboard failure	10%
CPU fan failure	8%
RAM failure	4%

Using the OPMA, administrators can determine which kind of serious hardware failure has occurred (see **Table 2 - 2**).

Table 2 - 2. Host System Failures and how they are detected

Type of Failure	**Detected by**
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power off state after power on command has been given.
CPU, Controller, motherboard failure	Power supply is on, but there is no video output.
CPU fan failure	By IPMI or server specific management software
RAM failure	Boot-Sequence on boot console

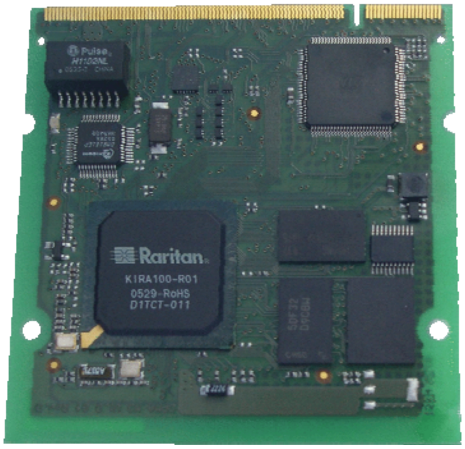
Notes: 1. According to a survey made by the Intel Corp.

Chapter 3. OPMA Installation Guide

About the OPMA add-on card

The OPMA add-on card redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted with the TCP/IP protocol family. The OPMA add-on card is especially useful in a multi-administrator environment.

Figure 3 - 1. OPMA add-on Module



Connectors

Connecting the OPMA add-on card to the Host System

Connecting the OPMA add-on card to the Host System is easy:

a) Turn off the Host and pull the power supply cable of the server,

b) find the OPMA slot and carefully insert the OPMA add-on card into the slot,

c) connect the power plug of the Host into the electrical outlet, but not power on the host,

d) then wait for a first initial boot up of the OPMA module,

e) now the host system has to be started manually for the first time by pressing the **Power** button on the host,

f) while the server is booting his BIOS the OPMA module will be informed about the Board ID, which is needed for the loading process of the appropriate topology of the server board,

g) this step is important for the correct usage of all System Health features and sensors.

Warning: Please note: the firmware of the OPMA board delivered to you is customised for use with the specified motherboard. If you use your OPMA module in a motherboard with a different sensor and actor configuration it will most probably not operate correctly.

Warning: You should turn off the power of the Host completely during the installation of the OPMA module, that includes detaching the power supply cable.

Connecting the Ethernet

The OPMA add-on card needs a dedicated RJ45 Ethernet connector - this has to be provided by the native system. The connector may be used either as a 100 Mbps 100Base-TX connection or as a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will automatically adjust to it.

10 Mbps Connection

For 10BASE-T Ethernet networks the Fast Ethernet adapter uses category 3, 4, or 5 UTP cable. To establish a 10 Mbps connection, the cable has to be connected to a 10BASE-T hub.

1. Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
2. Align the RJ45 plug with the notch on the adapter’s connector and insert it into the adapter’s connector. You should hear an audible click, as the Ethernet plug latches.

100 Mbps Connection

For 100BASE-TX Ethernet networks the OPMA module supports category 5 UTP cabling. To establish a 100 Mbps connection, the cable has to be connected to a 100BASE-TX hub.

1. Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
2. Align the RJ45 plug with the notch on the adapter’s connector and insert it into the adapter’s connector. You should hear an audible click, as the Ethernet plug latches.

Warning: The UTP wire pairs and configuration for 100BASE-TX cable are identical to those for 10BASE-T cable when using category 5 UTP cable.

Chapter 4. OPMA Modul Configuration

Initial Configuration

The OPMA module's communication interfaces are all based on TCP/IP. It comes pre-configured with the IP configuration listed in **Table 4 - 1**. Additionally you can do some simple configuration using the serial interface.

Table 4 - 1. Initial Network Configuration

Parameter	Value
IP auto configuration	DHCP
IP address	-
Netmask	255.255.255.0
Gateway	none
IP access control	none

Warning: If the DHCP connection fails on boot up, the OPMA module will not have obtained an IP address. This means it will not be accessible over the network.

If this initial configuration does not meet your requirements, the following describes the initial IP configuration that is necessary to access the OPMA module for the first time.

Initial Configuration via DHCP Server

By default, the OPMA module will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the OPMA module. You can find the MAC address on the outside of the shipping box and labeled on the bottom side.

If this initial configuration does not meet your local requirements, use the KiraTool to adjust the values to your needs. The KiraTool can be found on the CD ROM delivered with this package. An overview of all supported Command Line commands and options are displayed in **Appendix C. KiraTool Commands.**

Initial Configuration via Serial Console

To configure the OPMA module via serial interface a null modem cable is required (available separately) to connect the user computer and the host system, on which the OPMA add-on card is installed. The communication software can be telnet (Windows) or kermit (Linux).

Normally the OPMA board will simply make a connection between the UART on the motherboard of your device with the Serial Port at the back. However for a few seconds after startup you can interrupt this switch by typing **ESC**ape.

Indeed for all the lovers of detail there is one more serial mode. This allows the OPMA module to monitor the serial traffic and listen to SOL sequences. This way you can open a command session to the OPMA module inside normal serial communication. However this is rarely used in practice.

The serial line has to be configured using the parameters given in **Table 4 - 2**.

When configuring with a serial terminal, you need to start up the communication software and then power-cycle the OPMA add-on card (perhaps by power-cycling the server it is attached to) and **immediately** press the **ESC** key. You will see a => prompt.

At this point you have two useful commands at your fingertips:

- **defaults -** this recalls the factory settings fopr the OPMA module.
- **config -** this allows you to enter a more detailed configuration menu. Please wait for a few seconds for the configuration questions to appear.

Table 4 - 2. Serial Line Parameters

Parameter	Value
Bits/ssecond	115200
Data bits	8
Parity	no
Stop bits	1
Flow Control	none

As you proceed, the following questions will appear on the screen. To accept the default values which are shown in square brackets below, press **Enter**. Note that you will see two sets of questions depending if you decide to enable DHCP or a static IP address. The final message of "Configuring device...Done" means that the configuration was accepted and written and saved successfully.

```
Welcome!
Choose a login for the following features:
-Initial IP configuration: "config".
-Unblock currently blocked users: "unblock".
192.168.1.185 login: config
IP autoconfiguration (none/dhcp/bootp) [dhcp]:
Enable IP Access Control (yes/no) [no]:
LAN interface speed (auto/10/100) [auto]:
LAN interface duplex mode (auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to
Cancel y

Configuring device ...
Done.
```

The following is the above interaction, but this time specifying a static IP adress.

```
Welcome!
Choose a login for the following features:
-Initial IP configuration: "config".
-Unblock currently blocked users: "unblock".
192.168.1.185 login: config
IP autoconfiguration (none/dhcp/bootp) [dhcp]: none
IP [192.168.1.185]: 192.168.1.63
NetMask [255.255.255.0]:
Gateway (0.0.0.0 for none) [192.168.1.1]:
Enable IP Access Control (yes/no) [no]:
LAN interface speed (auto/10/100) [auto]:
LAN interface duplex mode (auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to
Cancel y

Configuring device ...
Done.
```

IP autoconfiguration

With this option you can specify whether the OPMA module should get its network settings from a DHCP or BOOTP server. For DHCP, enter "dhcp", and for BOOTP enter "bootp". If you do not specify any of these, the IP autoconfiguration is disabled and subsequently you will be asked for the following network settings.

IP address

The IP address the OPMA module uses. This option is only available if IP autoconfiguration is disabled.

Net mask

The net mask of the connected IP subnet. This option is only available if IP autoconfiguration is disabled.

Gateway address

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP autoconfiguration is disabled.

Enable IP Access Control

Here you should be careful and normally accept the default "no".When you configure the OPMA module using the serial interface you are usually in some sort of trouble accessing the module over the Ethernet. If you enable the IP access control by entering "yes", you may find yourself locked out again, letting the very same problem arise again that you are trying to fix.

LAN Interface Speed

You may accept the default "auto". In this case the OPMA Ethernet hardware will auto-sense the interface speed by listening to the heartbeat on the wire. However in some cases this does not work properly, you should then set the speed manually to either 10 or 100MB per second.When the Ethernet wire the OPMA module is attached to is out of spec (like being too long) then auto-sensing can easily cause a "flapping interface". This makes it very difficult to access the OPMA module and you should then set a fixed speed.

LAN interface duplex mode

You may specify "auto" for auto-sensing adjustment or you may force full-duplex or half-duplex mode by entering the desired value.

Finally, you will be asked if the values are correct and may adjust them if necessary. After your confirmation the OPMA module performs a reset using the new values.

Web Interface

The OPMA module may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of the OPMA module into your web browser. The initial login settings are:

Table 4 - 3. Standard User Settings

Parameter	Value
Login	super
Password	pass

Changing these settings to user specific values is strongly recommended and can be done on the "User Management" page (see the Section called **Users And Groups** in Chapter 6).

Mouse and Keyboard Configuration

Remote Mouse Modes

The proper configuration of a remote mouse is somewhat difficult to understand unless you know some underlying concepts. Basically mice transmit their movement using two methods: either absolute or relative mode.

Absolute mode means that the mouse transmits absolute co-ordinates to the OPMA module. This is information like: "I am moving to screen co-ordinates X,Y". This mode is very easy to track and most modernWindows versions (XP, 2000, 2003) as well as Mac OS X use this. This mode is also easiest for the OPMA module to track.

The second mode is "relative mode". In this case the mouse transmits information like "I am moving 97 pixels vertically and 88 pixels horizontally from my previous position". This is much more difficult to track. Firstly the OPMA module has to know the starting point of the movement (hence you need to press a special Synchronize Button, which allows the OPMA module to enquire the starting point of the mouse). Secondly a lot of other factors come into play like the mouse acceleration which can be different on the remote system and the system you are using to talk to the OPMA module. Hence the OPMA module has to do a lot more conversion work to track the mouse than using absolute mode.

Relative mode is used by most Linux Systems and older operating system like Windows 95/98. Therefore you need to select "Other Operating Systems" if your PC/mouse uses this mode.

Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The OPMA module addresses this situation with an intelligent synchronization algorithm. There are three mouse modes available on the OPMA module:

Auto Mouse Speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed Mouse Speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to “n” pixel moves on the remote system. This parameter “n” is adjustable with the scaling. It should be noted that this works only when mouse acceleration is turned off on the remote system.

Single/Double Mouse Mode

This mode is described in the Section called **Single and Double Mouse Mode**.

Auto Mouse Speed and Mouse Synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the mouse does not move correctly, there are two ways for re-synchronizing local and remote mouse:

Fast Sync

The fast synchronization is used to correct a temporary but fixed skew. Choose this option from the Remote Console Options menu (entry: Mouse Handling). If defined you may also press the mouse synchronization hotkey sequence (see the Section called **Remote Console Control Bar** in Chapter 5 for details).

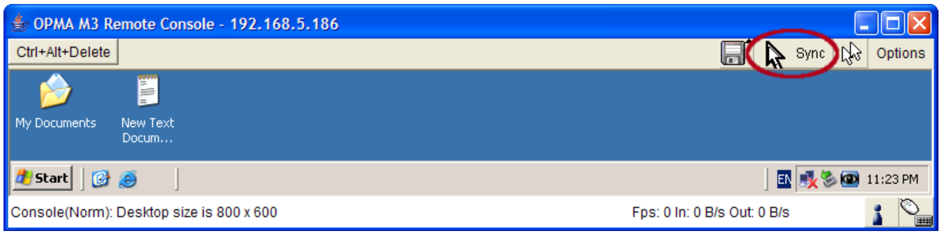
Intelligent Sync

If the Fast Sync does not work or the mouse settings have been changed on the host system, use the Intelligent Synchronization, instead. This method adjusts the parameters for the actual movement of the mouse pointer so that the mouse pointer is displayed at the correct position on the screen.

This method takes more time than the Fast Sync and can be accessed with the appropriate item in the Remote Console Option menu (entry: Mouse Handling).

Furthermore, the shape of the mouse pointer has a significant influence on the pointer detection.We recommend to use a simple, but common pointer shape. In most cases, the detection and synchronization of animated pointer shapes is likely to fail. In general, pointer shapes that change during the pointer detection process are rather impossible to figure out in the transferred video picture.With the usage of a standard mouse pointer shape the detection is rather simple and the syncronization is at its best.

Figure 4 - 1. Remote Console Control Bar: Sync Button



Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

The **Sync Mouse** button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a Fast Sync, except in situations where the KVM port or the video mode changed recently. See also the Section called **Remote Console Control Bar** in Chapter 5.

Host System Mouse Settings

The host's operating system knows various settings for the mouse driver.

Warning: The following limitations do not apply in case of USB and Mouse Type "Windows >= 2000, MAC OS X".

While the OPMA module works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations which may prevent this synchronization from working properly:

Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows 2003 Server/XP Mouse Settings

Windows XP knows a setting named "improve mouse acceleration" which has to be deactivated.

Active Desktop

If the Active Desktop feature of MicrosoftWindows is enabled, do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

See also the Section called **Recommended Mouse Settings** for mouse mode recommendations.

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If resynchronizing fails, disable the mouse acceleration and repeat the procedure.

Single and Double Mouse Mode

The above information applies to the Double Mouse Mode where remote and local mouse pointers are visible and need to be synchronized. The OPMA module also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the Remote Console (see the Section called **Remote Console Control Bar** in Chapter 5) and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode it is necessary to define a mouse hotkey in the Remote Console Settings Panel Press this key to free the captured local mouse pointer.

Recommended Mouse Settings

For the different operating systems we can give the following advice:

MS Windows 2000, 2003, XP (all versions)

For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option "enhance pointer precision" in the Control Panel.

***Note:** The remote mouse is always synchronized with the local mouse if selecting the option "Windows >= 2000, MAC OS X".*

SUN Solaris

Adjust the mouse settings either via "xset m 1" or use the CDE Control Panel to set the mouse to "1:1, no acceleration". As an alternative you may also use the Single Mouse Mode.

MAC OS X

We recommend using the Single Mouse Mode.

Linux

First, choose the option "Other Operating Systems" from the the Mouse Type selection box.

Second, choose the option Auto Mouse Speed. This applies for both USB and PS/2 mice.

Video Modes

The OPMA module recognizes a limited number of common video modes.When running X11 on the host system please do not use any custom modelines with special video modes. If you do, the OPMA module may not be able to detect them. We recommend using any of the standard VESA video modes instead.

Resetting the OPMA module to its Factory Settings

Using the Serial Interface

Power-cycle the OPMA module (this may require power-cycling the server) and immediately press the **ESC** key. On your screen a command prompt "=>" will be visible. Enter the command "defaults", press the **Enter** key and wait for a few seconds for the OPMA module to reboot. Now, you may use the default settings as described in the Section called **Initial Configuration**.

Using KiraTool

The OPMA module configuration can be reset to factory defaults by using the KiraTool. KiraTool can be used locally on the host containing the OPMA module or remotely.

For Example:

For a local access:

```
kiratool -s -u admin -p password defaults
```

For a remote access:

```
kiratool -l 192.168.1.52 -u admin -p password
defaults
```

Chapter 5. OPMA Module Usage

Prerequisites

The OPMA module features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the built-in Ethernet adapter.

The following interfaces are supported:

HTTP/HTTPS

Full access is provided by the embedded web server. The OPMA module environment can be entirely managed using a standard web browser. You can access the OPMA module using the insecure HTTP protocol or using the encrypted HTTPS protocol.Whenever possible use HTTPS.

Telnet

A standard Telnet client can be used to access most of the OPMA module's functionality, including a text-mode console redirection.

SSH

A Secure Shell (SSH) client can also be used to access the OPMA module, including a text-mode console redirection as mentioned above.

The primary interface of the OPMA module is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.4 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Important: We recommend you to install a Sun JVM 1.4 or higher version.

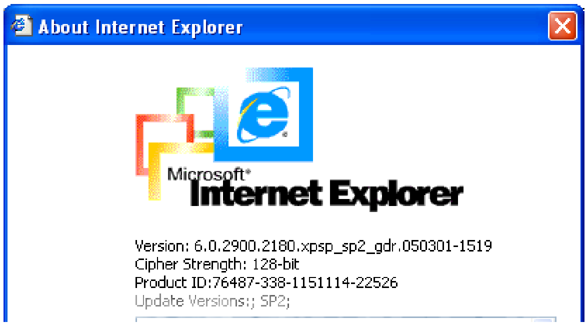
For an insecure connection to the OPMA module we can recommend the following web browsers:

- Microsoft Internet Explorer version 5.0 or higher on Windows 98, Windows ME, Windows 2000 and Windows XP
- Netscape Navigator 7.0, Mozilla 1.6 and Mozilla Firefox onWindows 98, Windows ME, Windows 2000,Windows XP, Linux and other UNIX-like Operating Systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm.

Using the Internet Explorer, open the menu entry "?" and "Info" to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. **Figure 5 - 1** shows the dialog box presented by the Internet Explorer 6.0.

Figure 5 - 1. The Internet Explorer displaying the Encryption Key Length



Version: 6.0.2900.2180.xpsp_sp2_gdr.050301-1519
Cipher Strength: 128-bit
Product ID:76487-338-1151114-22526
Update Versions:; SP2;

Newer web browsers support strong encryption by default.

Login and Logout to the OPMA Module

Login into the OPMA Module

Open your web browser. Type in the address of your OPMA module which you configured during the installation process. The address used might be a plain IP address or a host and domain name, in case you have given your OPMA module a symbolic name in the DNS. For instance, type the following in the address line of your browser when establishing an unsecured connection:

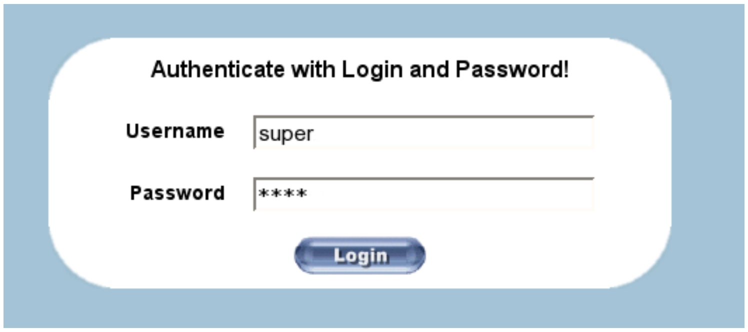
```
http://192.168.1.22/
```

In order to use a secure connection type in:

```
https://192.168.1.22/
```

This will take you to the OPMA module login page as shown in **Figure 5 - 2**.

Figure 5 - 2. Login Screen



Authenticate with Login and Password!

Username: super

Password: ****

Warning: Your web browser has to accept cookies or else login is not possible.

The OPMA module has a built-in super user that has all the permissions to administrate your OPMA module. See the following table for the default settings. Please note that the user "super" is not allowed to login via the serial interface of the OPMA module.

Table 5 - 1. Standard User Settings

Parameter	Value
Login	super
Password	pass

Warning: The OPMA module will force you to change the super user password at first login.

Navigation

After the successful login to the OPMA module, the main page of the OPMA module appears (see **Figure 5 - 3**). This page consists of three parts, each of them contains specific information. The buttons on the upper side allow you to navigate within the front end (see **Table 5 - 2** for details). The lower left frame contains a navigation bar and allows you to switch between the different sections of the OPMA module.

Within the right frame, task-specific information is displayed that depends on the section you have chosen before.

Figure 5 - 3. Main Page

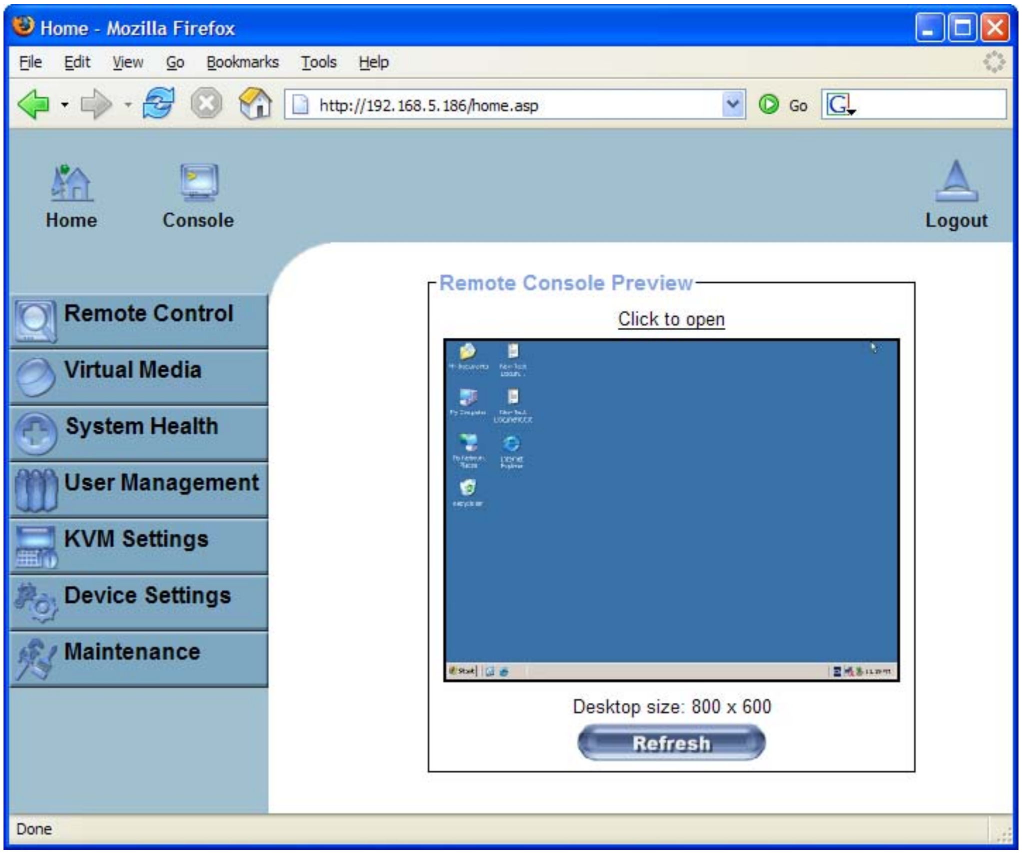


Table 5 - 2. Front End Buttons

Home	Return to the main page of the OPMA module.
Console	Open the OPMA module Remote Console.
Logout	Exit from the OPMA module front end.

Logging out of the OPMA Module

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for half an hour.

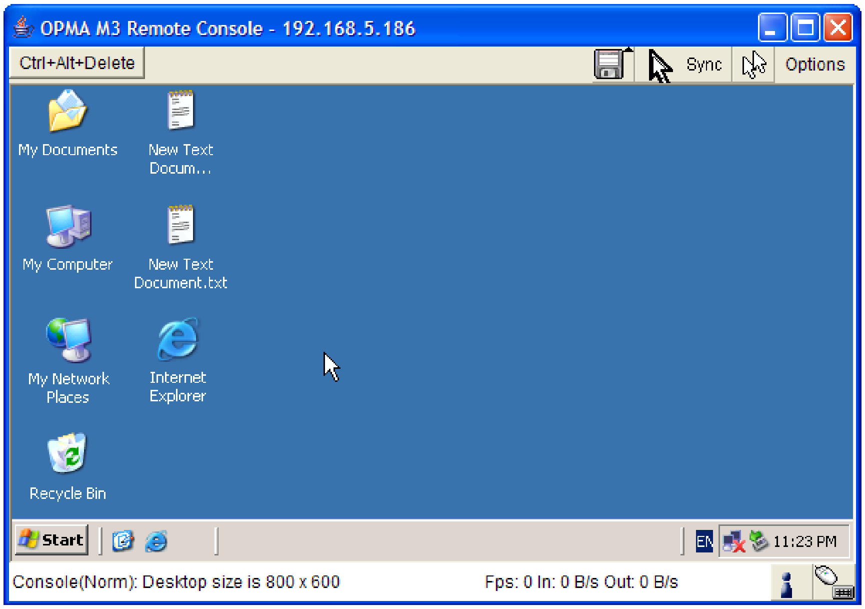
Warning: If there is no activity for half an hour, the OPMA module will log you out automatically. A click on one of the links will bring you back to the login screen.

The Remote Console

General Description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that the OPMA module controls.

Figure 5 - 4. Remote Console



Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

The Remote Console window is a Java Applet that tries to establish its own TCP connection to the OPMA module. The protocol that is run over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port #443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

In case the OPMA module is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today’s web proxies are not capable of relaying the RFB protocol.

In case of problems, please consult your network administrator in order to provide an appropriate network environment.

Main Window

Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. However, please be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth and latency of the line which you use to connect to the OPMA module.

With respect to the keyboard, the precise remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system and your host system uses a US English keyboard layout, for instance, special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

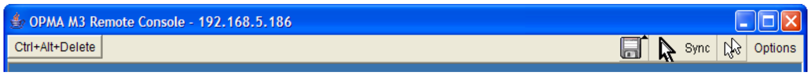
The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Warning: As different to the remote host system, the Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings. A description for each control follows.

Figure 5 - 5. Remote Console Control Bar



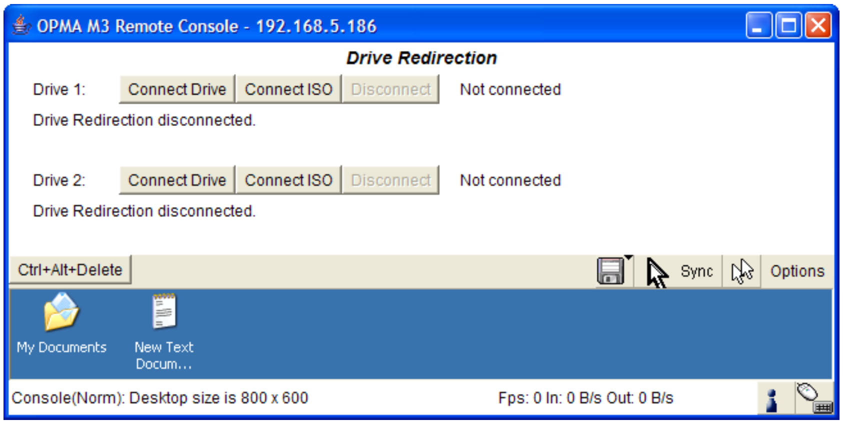
Warning: Please note that some of these options are only visible and usable when you have selected the operating system type "Other Operating Systems".

Drive Redirection

Opens the virtual media Drive Redirection menu for the Remote Console.

The Dual-channel Virtual Media allows a remote user to transfer installation files and other media to a target machine over KVM ports. 2 USB Mass Storage Redirection channels (redirection of Floppy/CD/DVD images, client drives or ISO images) can access media at the same time, useful for special applications like installing OS with driver disk.

Figure 5 - 6. Remote Console Applet Drive Redirection Menu



Not connected

Drive Redirection disconnected.

Not connected

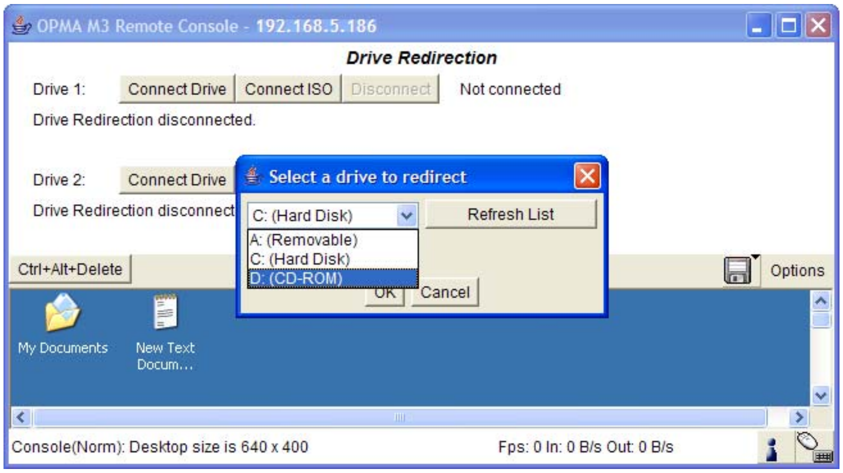
Drive Redirection disconnected.

Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

By help of this menu, you can either redirect a local drive (only available under Windows):

Figure 5 - 7. Redirecting a Local Drive



Not connected

Drive Redirection disconnected.

Drive Redirection disconnect

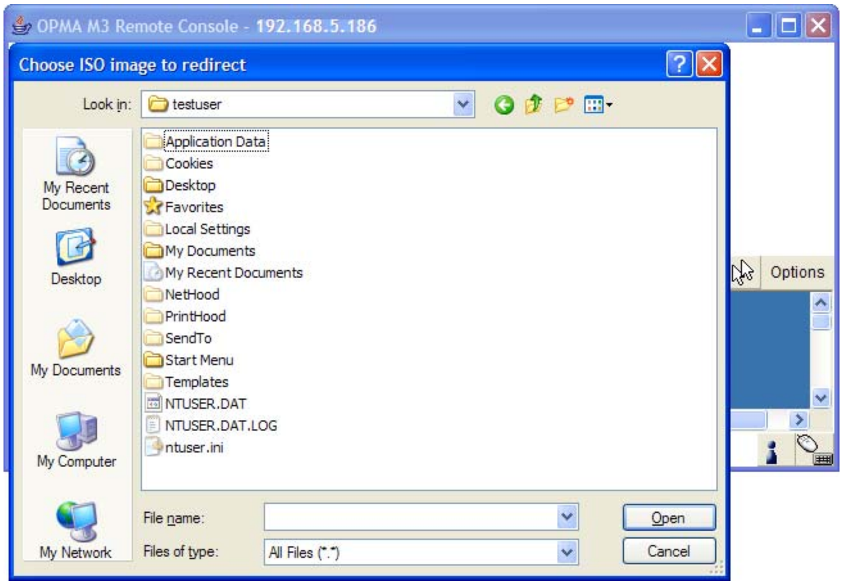
C: (Hard Disk)

Console(Norm): Desktop size is 640 x 400

Fps: 0 In: 0 B/s Out: 0 B/s

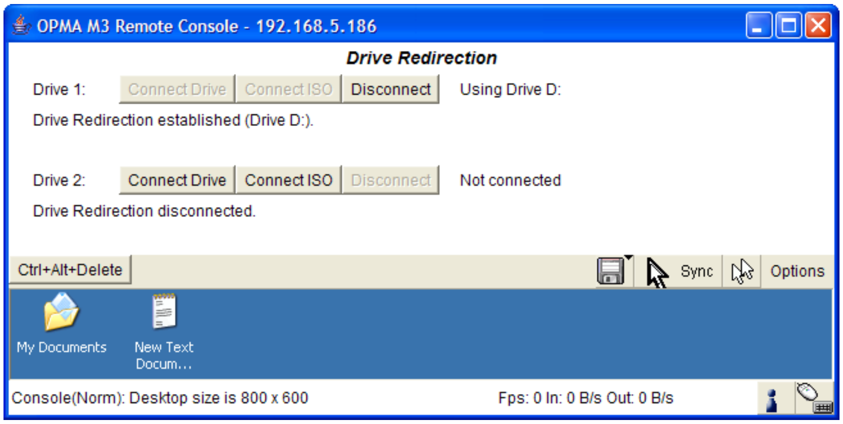
or redirect an ISO CD/DVD image:

Figure 5 - 8. Redirecting an ISO Image



Finally the established Drive Redirection connection will be displayed.

Figure 5 - 9. Successfully Drive Redirection Connection



Using Drive D:

Drive Redirection established (Drive D:).

Not connected

Drive Redirection disconnected.

Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

Sync Mouse Sync

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings there.

Ctrl+Alt+Delete Ctrl+*Alt+*Delete

Special button key to send the "Control Alt Delete" key combination to the remote system (see also the Section called **KVM Settings** in Chapter 6 for defining new button keys).

Single/Double Mouse Mode

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchonized). Single Mouse Mode is only available if using SUN JVM 1.4 or higher.

To leave the single mouse mode and get your local mouse pointer back, please press **Alt-F12**.

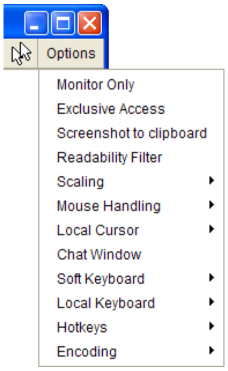
Options

To open the Options menu click on the **Options** button. See the Section called **Remote Console Options** for a detailed description of the available options for the OPMA module.

Remote Console Options

To open the Options menu click on the **Options** button.

Figure 5 - 10. Remote Console Options Menu



A description of the options follows.

Monitor Only

Toggles the Monitor Only filter on or off. If the filter is switched on no remote console interaction is possible. The remote screen can be viewed, only.

Exclusive Access

If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

Note: *This option is only accessible for members of the "administrator" group and the user "super".*

A change in the access mode is also visible in the status line. See the Section called

Remote Console Status Line for more information.

Screenshot to Clipboard

This button allows you to capture a screenshot: the OPMA module will automatically place it onto the "clipboard". This allows you to easily import the screenshot into your documents or other programs.

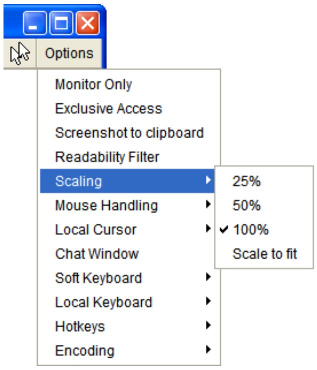
Readability Filter

Toggles the Readability Filter on or off. If the filter is switched on in scaling mode, it will preserve most of the screen details even if the image is substantially scaled down. This option is only available with a JVM 1.4 or higher.

Scaling

Allows you to scale down the Remote Console. You can still use both mouse and keyboard, however the scaling algorithm will not preserve all display details.

Figure 5 - 11. Remote Console Options Menu: Scaling

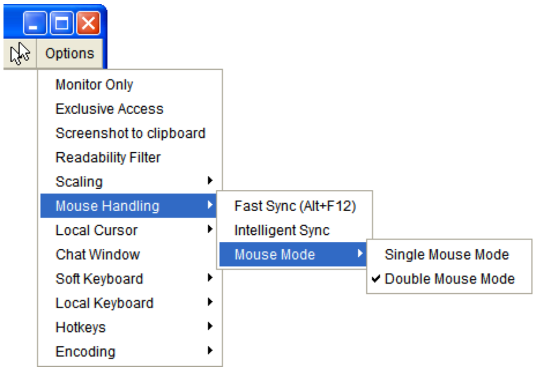


Mouse Handling

__Note:__ Only available when you have selected the option "Other Operating System".

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer when using Soft Mouse Mode as explained in the Section called **Mouse and Keyboard Configuration** in Chapter 4.

Figure 5 - 12. Remote Console Options Menu: Mouse Handling



Fast Sync

The fast synchronization is used to correct a temporary but fixed skew.

Intelligent Sync

Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

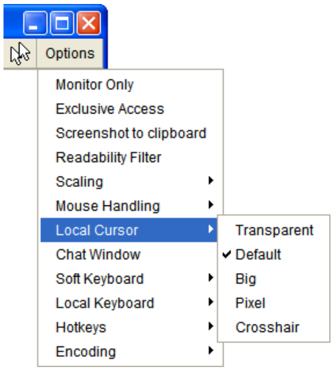
Mouse Mode

This mode is described in the Section called **Single and Double Mouse Mode**.

Local Cursor

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine, a version of 1.2 or higher offers the full list.

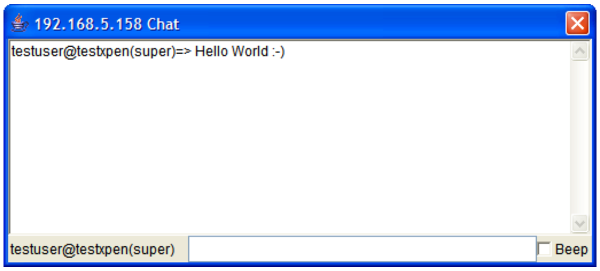
Figure 5 - 13. Remote Console Options Menu: Local Cursor



Chat Window

This opens a chat window allowing you to interactively "chat" with other users logged into the OPMA module.

Figure 5 - 14. Remote Console Options Menu: Chat Window



testuser@testxpen(super)=> Hello World :-)

Soft Keyboard

The Soft Keyboard simulates an entire keyboard that is connected to the remote system. It is necessary in case your remote system runs with a completely different language and country mapping to your administration machine. By selecting the apropriate button(s) you can send key codes and also key sequences to the remote system and act as if you would work with a keyboard that is directly connected to the remote system.

In order to open the Soft Keyboard select the entry **Soft Keyboard** from the Options menu. You can send single key strokes like `F` as well as combinations of keys such as `Ctrl+C or AltGr+Shift+F4`.

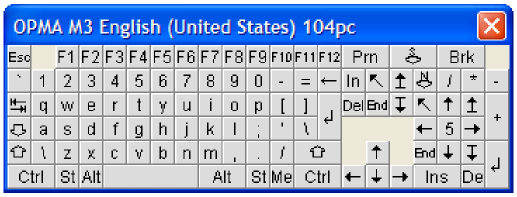
For a single key stroke you can click on the button with the wanted character. Single keys such as regular characters and numbers are sent immediately. Special keys like `Ctrl`, `Shift` as well as the function keys `F1` to `F12` have to be selected twice. The first press sends the signal "key is pressed", the second press indicated the signal "key is released" to the remote system. After the first press the button will change its color to signalize that the according key is pressed, currently. After the second press the button will appear as usual and signalize that the key was sent.

To send the key combination `Ctrl+C` select the button `Ctrl` first. The button will change its color. Press the button `C`. The following key (`C` in our example) will be combined with the previously selected key. Both the buttons `Ctrl` and `C` are released and the key combination will be sent to the remote system. The button `Ctrl` will appear as normal (color change).

In order to send the key combination `Ctrl+F5` three steps have to be done. Select the button `Ctrl` once and the button `F5` twice. The last press will release both buttons and send the key combination to the remote system.

In order to send the key combination `AltGr+Shift+F4` four steps are required. First, select the button `AltGr` once. Second, select the button `Shift`. Finally, choose the button `F4` twice. The last press will release all the buttons and send the key combination to the remote system.

Figure 5 - 15. Remote Console Options Menu: Soft Keyboard


OPMA M3 English (United States) 104pc
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prn Brk
` 1 2 3 4 5 6 7 8 9 0 - = ← In / * -
q w e r t y u i o p [ ] Del End +
a s d f g h j k l ; ' \ ← 5 →
\ z x c v b n m , . / ↑ End
Ctrl St Alt Alt St Me Ctrl ← ↓ → Ins De

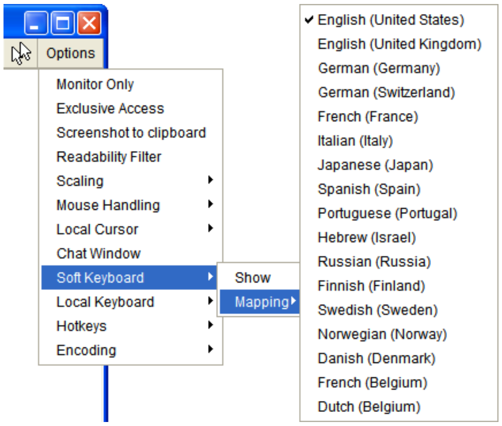
Show

Displays the Soft Keyboard.

Mapping

Used for choosing the according language and country mapping of the Soft Keyboard.

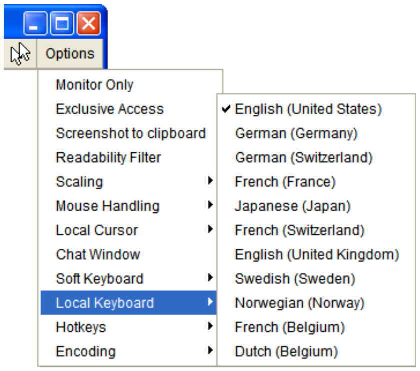
Figure 5 - 16. Remote Console Options Menu: Soft Keyboard Mapping



Local Keyboard

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses a US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language manually.

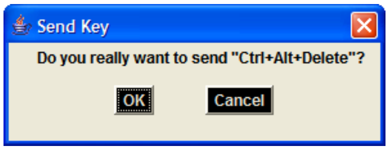
Figure 5 - 17. Remote Console Options Menu: Local Keyboard



Hotkeys

Opens a list of hotkeys defined before. In order to send a registered command to the host system choose the according entry. A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Choose **OK** to perform the command on the remote host. For a detailed description see the Section called **Remote Console Button Keys** in Chapter 6.

Figure 5 - 18. Remote Console Options Menu: Hotkey Confirmation Dialog



Do you really want to send "Ctrl+Alt+Delete"?

Encoding

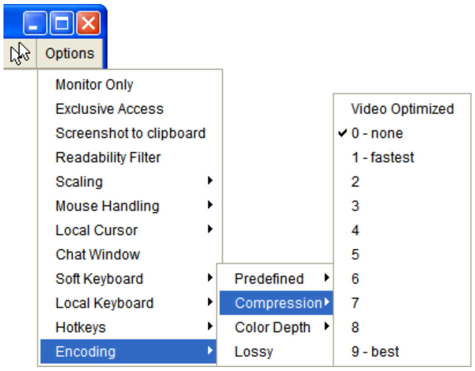
These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless "Transmission Encoding" is determined automatically (see the Section called **Transmission Encoding** in Chapter 6).

- **Compression Level**: you may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression. The most suitable compression level should always be seen as a compromise between the network bandwith that is available, on your video picture to be transferred, and on the number of changes between two single video pictures.We recommend to use a higher compression level if the network bandwidth is low. The higher the compression level the more time is necessary to both pack or unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

  If level 0 is chosen the video compression is disabled, completely.

  The option "Video Optimized" has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

Figure 5 - 19. Remote Console Options Menu: Encoding Compression



The next two options allow you to set the compression level to a predefined level OR to set a level for "lossy" compression. This compresses well, but leads to a degradation in image quality.

Figure 5 - 20. Remote Console Options Menu: Predefined Encoding Compression

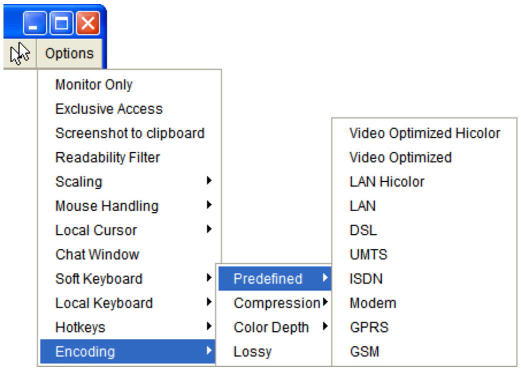
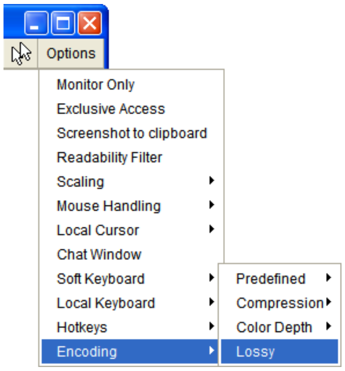
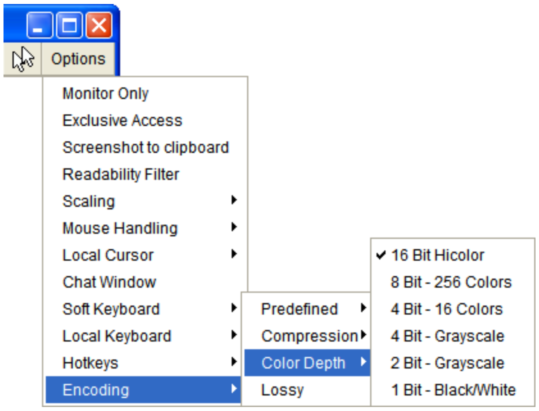


Figure 5 - 21. Remote Console Options Menu: Lossy Compression



- **Color Depth**: set the desired color depth. You may select between 8 or 16 bit for Video Optimized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and to be transferred.

Figure 5 - 22. Remote Console Options Menu: Color Depth

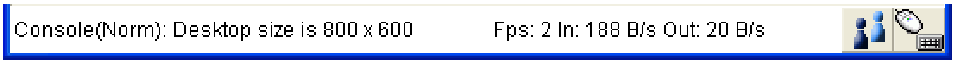


Note: *If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized". As a general result, the data rate is reduced (less bits per color). Furthermore, the OPMA module will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.*

Remote Console Status Line

The status line shows both console and the connection state. **Figure 5 - 23** was taken from a Remote Console with a resolution of 800 x 600 pixels. The value in brackets describes the connection to the Remote Console. "Norm" means a standard connection without encryption, "SSL" indicates a secure connection using Secure Socket Layer (SSL).

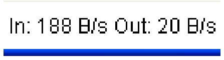
Figure 5 - 23. Status Line



Console(Norm): Desktop size is 800 x 600 Fps: 2 In: 188 B/s Out: 20 B/s

The status line displays the number of frame buffer updates ("Fps") as well as the incoming ("In:") and the outgoing ("Out:") network traffic in KB per second. A low value of the network traffic is recommended and can be achieved as described in the Section called **Optimizing the Video Picture**. If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

Figure 5 - 24. Status Line Transfer Rate



In: 188 B/s Out: 20 B/s

The next button displays the Remote Console Access settings.

Table 5 - 3. Buttons displaying the Access State

👤	One single user is connected to the Remote Console of the OPMA module.
👥	One or more users are connected to the Remote Console of the OPMA module.
✗👥	Exclusive access is set for you. Any other user may not access the remote host via Remote Console unless you disable this option.
👥✗	A remote user has exclusive access. You may not access the remote host via Remote Console unless the other user disables this option.

The outer right button displays the state of the Monitor Only settings.

Table 5 - 4. Buttons displaying the Monitor Only State

🖱⌨	The option Monitor Only is disabled.
🚫⌨	The option Monitor Only is enabled.

For more information about Monitor Only and Exclusive Access settings see the according paragraphs in the Section called **Remote Console Control Bar**.

Optimizing the Video Picture

The OPMA module detects the video mode with 8 bits (256 colors) automatically. To improve the picture quality you may select 16 bit (True Color) from the Options Menu of the Remote Console, sub menu "Encoding", entry "Color Depth" (see the Section called **Encoding** for details).

Currently, the video picture with the best quality can be achieved with the settings "16 bit (High Color)" in the Remote Console or "LAN (High Colour)" in the web frontend. This option can also be preset in the Section called **User Console** in Chapter 6.

The sub menu "Compression" from the Options menu has no influence on the picture quality but on the data rate of the picture that is transferred to the Remote Console.

Using the OPMA module with low bandwidth

The network connection of the OPMA module has an important influence on the time between two single video pictures. On a connection with low bandwidth it takes longer to transfer the video data from the OPMA module to the Remote Console on the local host. If the remote screen has changed a new picture is sent.

In terms of transfer time there is no difference between text screens and screens in graphics mode. The video picture is taken as graphics data no matter what the screen looks like and which video mode is chosen.

In terms of transferred data there can be an improvement. The compression plays an important role here. You can choose a compression level from the sub menu "Compression" in the Options menu of the Remote Console.

Please note that the video will be compressed on the OPMA module, transferred to the Remote Console and unpacked in a Java environment. Depending on the OPMA module and on the local machine this procedure may take some time and may result in an slowly updated picture in the Remote Console.

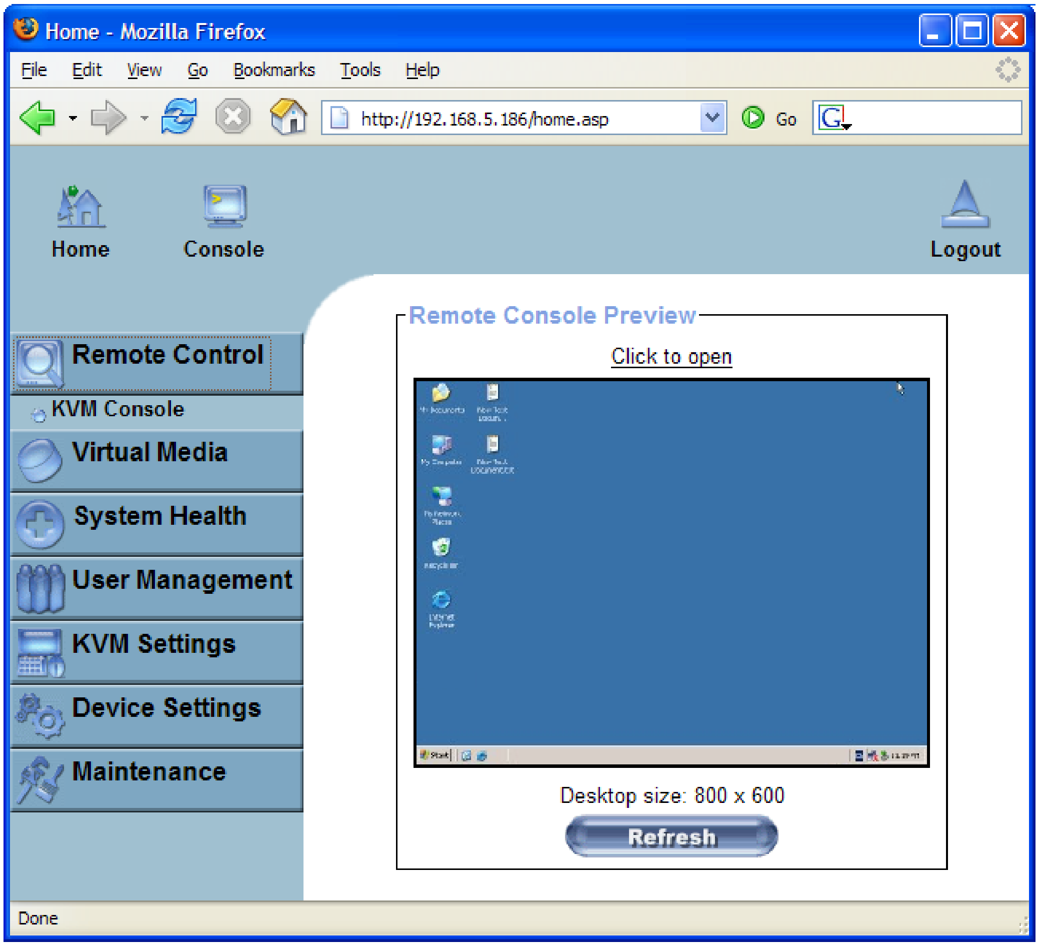
To improve the speed you may also set the picture quality in the Remote Console to either "8 bit" or even to grayscale. Due to less video data to be processed this is likely to be more effective than the highest compression level.

Chapter 6. Menu Options

Remote Control

KVM Console

Figure 6 - 1. KVM Console



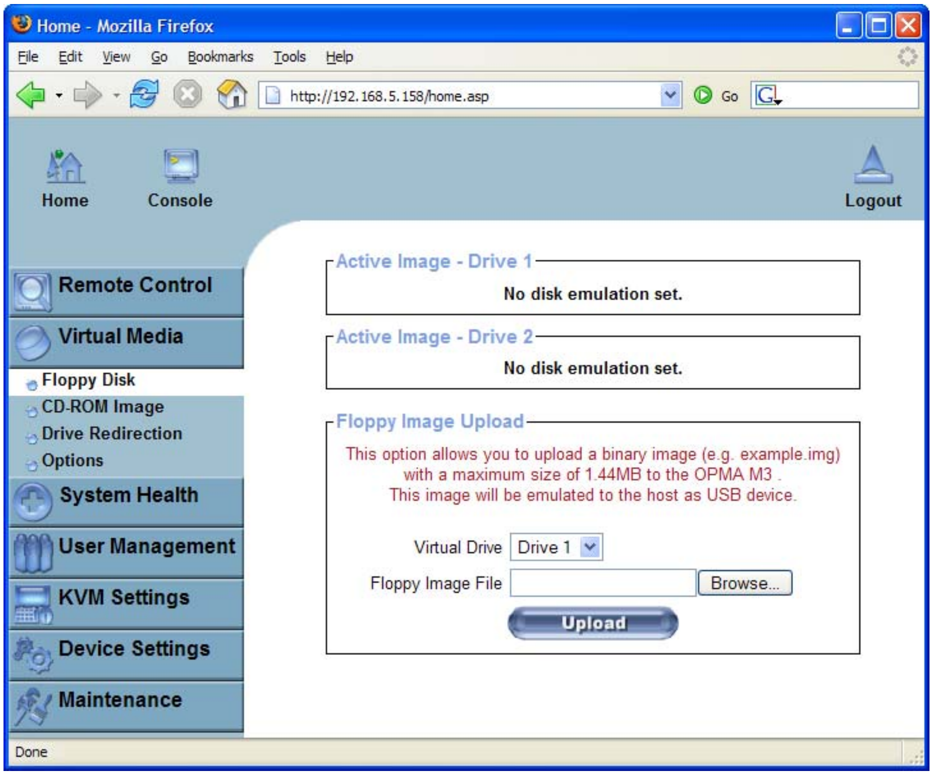
Remote Console Preview

To open the KVM console either click on the menu entry on the left or on the console picture on the right. To refresh the picture click on the button that is named **Refresh**.

Virtual Media

Floppy Disk

Figure 6 - 2. Virtual Floppy Area



Active Image - Drive 1

No disk emulation set.

Active Image - Drive 2

No disk emulation set.

Floppy Image Upload

This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the OPMA M3 . This image will be emulated to the host as USB device.

Virtual Drive: Drive 1

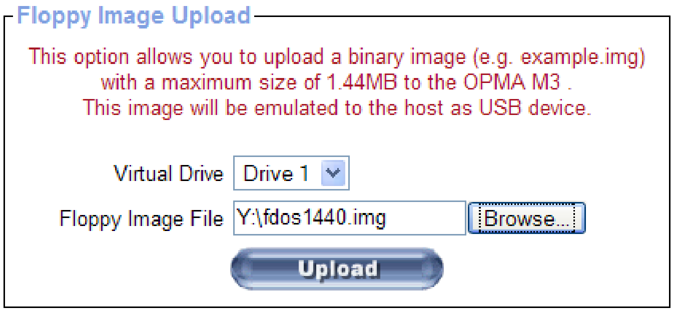
Floppy Image File:

Upload a Floppy Image

With two small steps working on the basis of a certain (floppy) image can be achieved.

- First the path of the images has to be specified. You can specify up to two images. You can do that either by hand or by using the file selection dialog of your web browser. To open the file selection dialog click on the **Browse** button and select the desired image file.

Figure 6 - 3. Select Image File



Floppy Image Upload

This option allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the OPMA M3 . This image will be emulated to the host as USB device.

Virtual Drive: Drive 1

Floppy Image File: Y:\fdos1440.img

The maximum image size is limited to 1.44MB. To use a larger image mount this image via Windows Share (or SAMBA) (see the Section called Use Image on Windows Share (via SAMBA) for details).

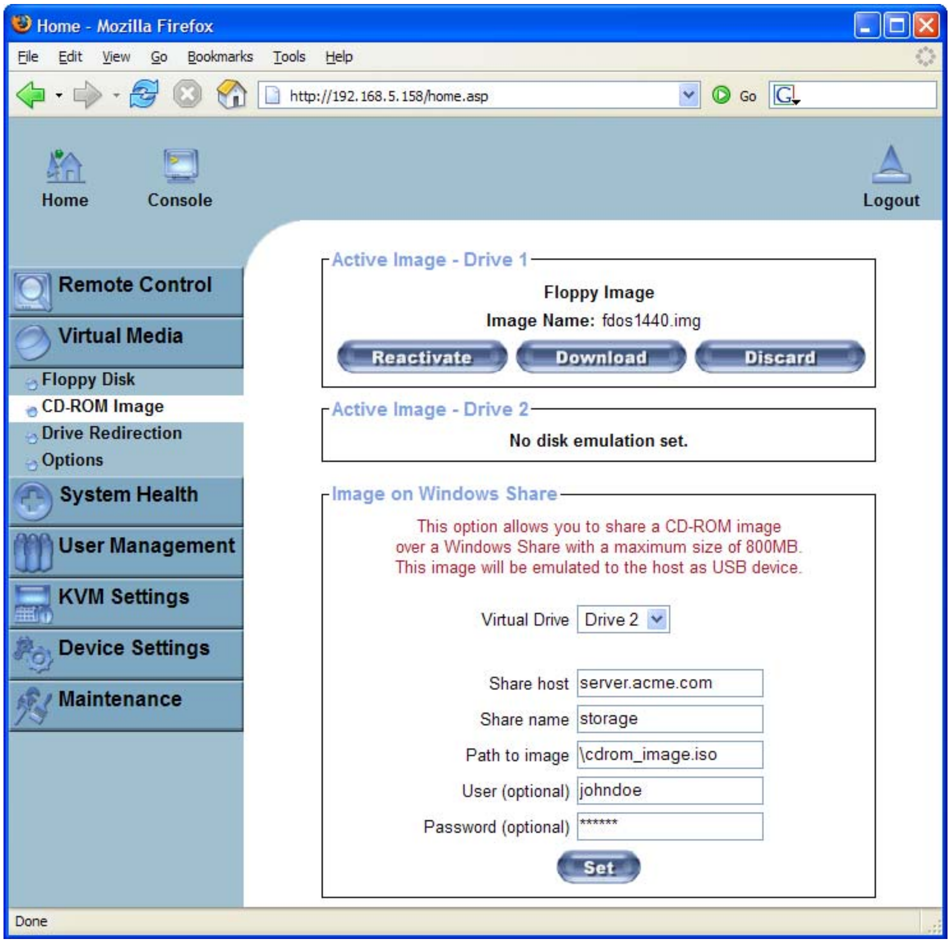
- Secondly, click on the button **Upload** to initiate the transfer of the chosen image file into the OPMA module's on-board memory. This image file is kept in the on-board memory of the OPMA module until the end of the current session, until you logged out or initiated a reboot of the OPMA module.

CD ROM

Use Image on Windows Share (via SAMBA)

To include an image from a Windows share select "CD-ROM" from the submenu.

Figure 6 - 4. CD-ROM Selection



Active Image - Drive 1

Floppy Image

Image Name: fdos1440.img

Active Image - Drive 2

No disk emulation set.

Image on Windows Share

This option allows you to share a CD-ROM image over a Windows Share with a maximum size of 800MB. This image will be emulated to the host as USB device.

Virtual Drive	Drive 2
Share host	server.acme.com
Share name	storage
Path to image	\cdrom_image.iso
User (optional)	johndoe
Password (optional)	******

The following information has to be given to mount the selected image properly:

Share host

The server name or its IP address. On Windows 95, 98 and Windows ME do not specify the IP address but the server name ("NetBIOS Name").

Share name

The name of the share to be used.

Path to image

The path of the image file on the share.

User (optional)

If necessary, specify the user name for the share named before. If unspecified and a guest account is activated, this guest account information will be used as your login.

Password (optional)

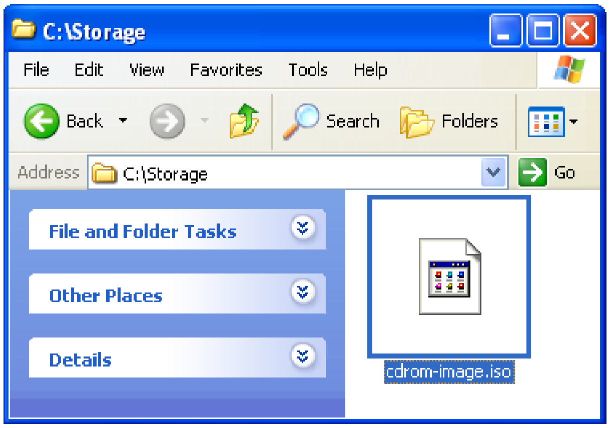
If necessary, specify the password for the given user name.

For an example you may have a look at the previous image: the OPMA module will look for a server named `mysql.acme.com`. Then, the entered share name is selected (in our example we use the share storage) and the image file `\cdrom_image.iso` is opened. If this file can only be accessed with both an user name and password enter the according values in the input fields for user name and password. In our case the file is owned by the user "johndoe" and protected by an user-specific pass-phrase (displayed as a number of stars).

To register the specified file image and its location click on the **Set** button.

The specified image file is supposed to be accessible from the OPMA module. The information above has to be given from the point of view of the OPMA module. It is important to specify correct IP addresses or device names. Otherwise, the OPMA module may not be able to access the referenced image file properly, leave the given file unmounted and will display an according error message, instead. So, we recommend to state correct values and repeat this step if necessary.

Figure 6 - 5. The Image File on the Share



Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as "root" on UNIX systems) or ask your system administrator for help to complete this task.

Windows 2000/XP

Open the Explorer, navigate to the directory (or share) and press the right mouse button to open the context menu. Select **Sharing** to open the configuration dialog (see **Figure 6 - 6**).

Figure 6 - 6. Explorer Context Menu

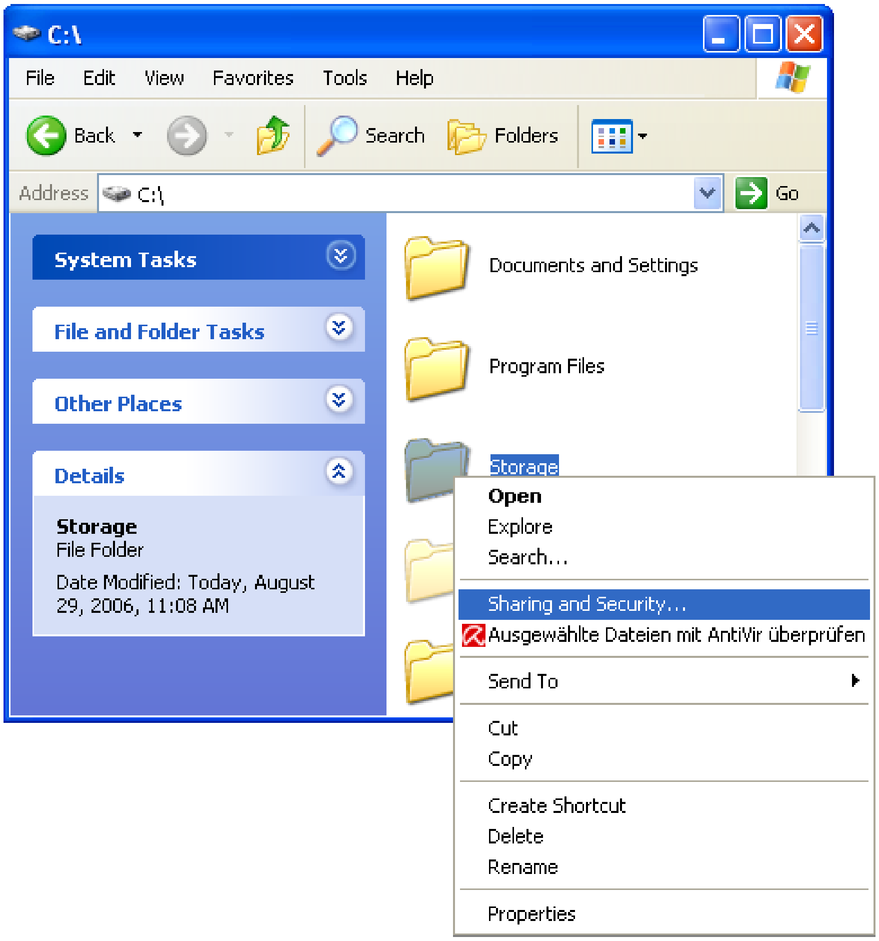
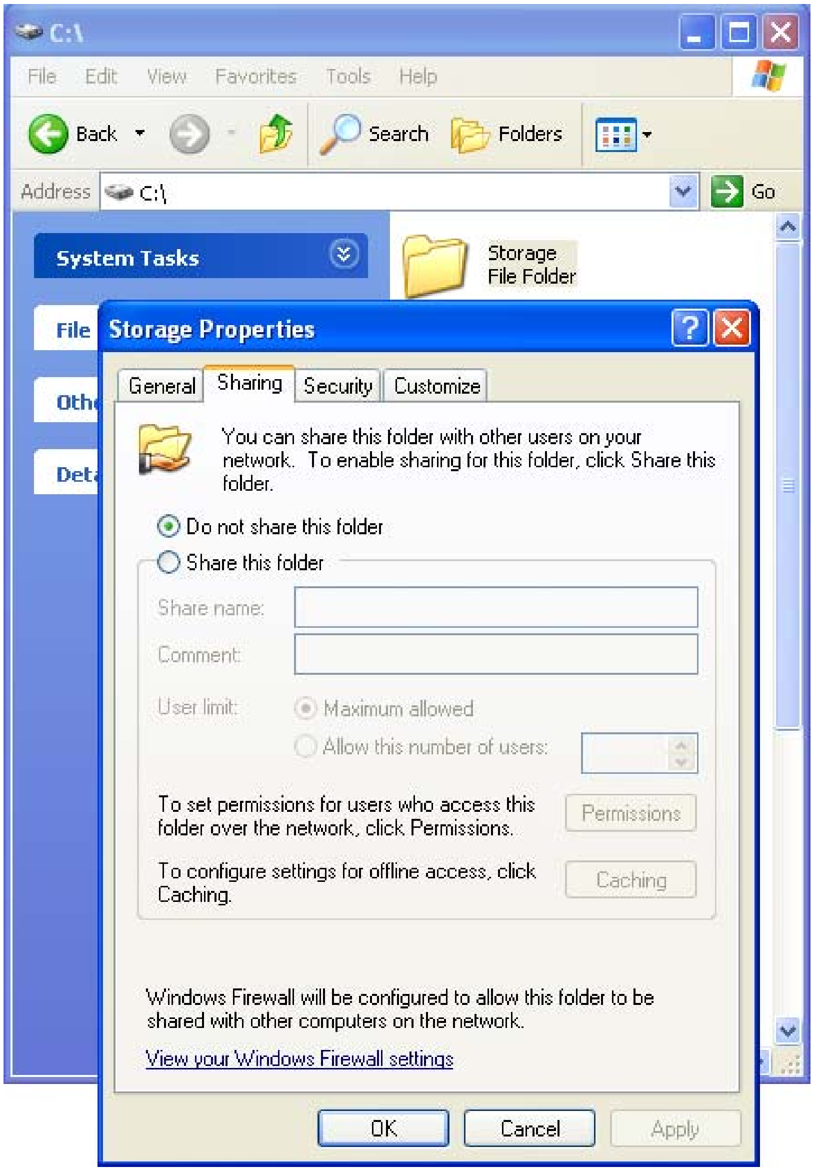


Figure 6 - 7. Share Configuration Dialog



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

◉ Do not share this folder

○ Share this folder

Share name:

Comment:

User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

Windows Firewall will be configured to allow this folder to be shared with other computers on the network.

View your Windows Firewall settings

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select **Share this folder**.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field **Comment**).
- If necessary, adjust the permissions (**Permissions** button).
- Click **OK** to set the options for this share.

UNIX and UNIX-like OS (UNIX, Solaris, Linux)

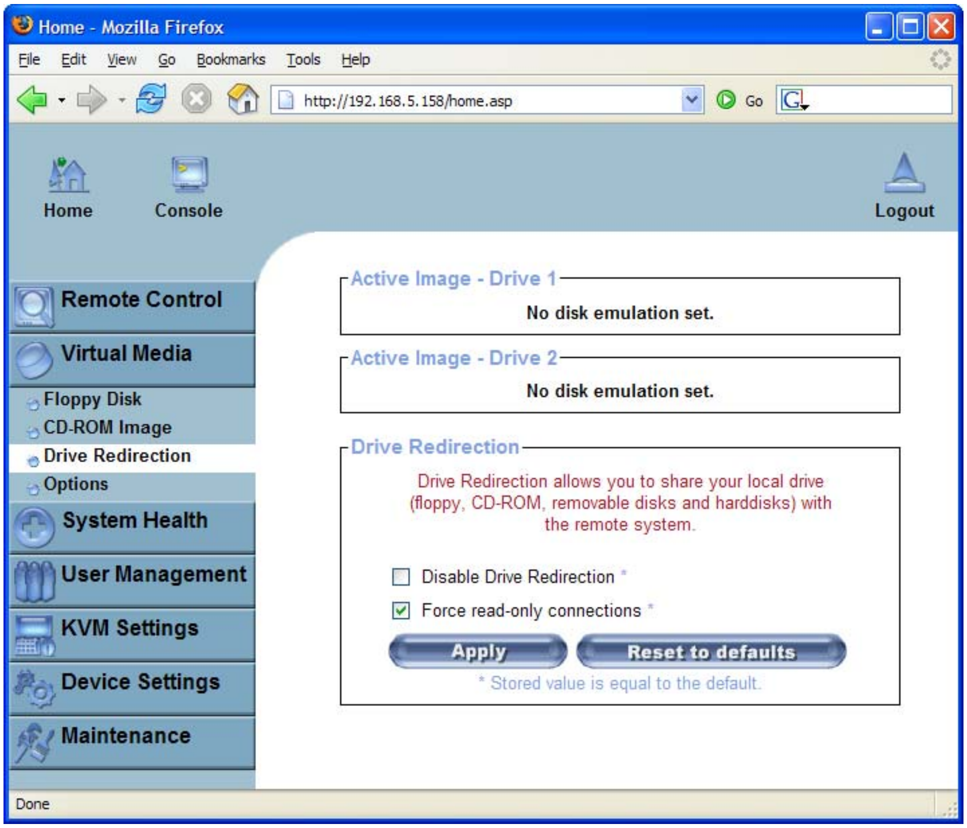
If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file `/etc/samba/smb.conf` or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

Also looking at the **man**-entry of **smb.conf** is very helpful.

Drive Redirection

The Drive Redirection is another possibility to use a virtual disc drive on the remote computer.With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that for the remote machine it is possible to write data to your local disc.

Figure 6 - 8. Drive Redirection



Active Image - Drive 1

No disk emulation set.

Active Image - Drive 2

No disk emulation set.

Drive Redirection

Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.

☐ Disable Drive Redirection *

☑ Force read-only connections *

Apply | Reset to defaults

* Stored value is equal to the default.

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host’s operating system. We recommend to use the Drive Redirection with care, especially the write support.

Drive Redirection Options

As shown in **Figure 6 - 8** the following options may be enabled:

Disable Drive Redirection

If enabled the Drive Redirection is switched off.

Force read-only connections

If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

Click **Apply** to submit your changes.

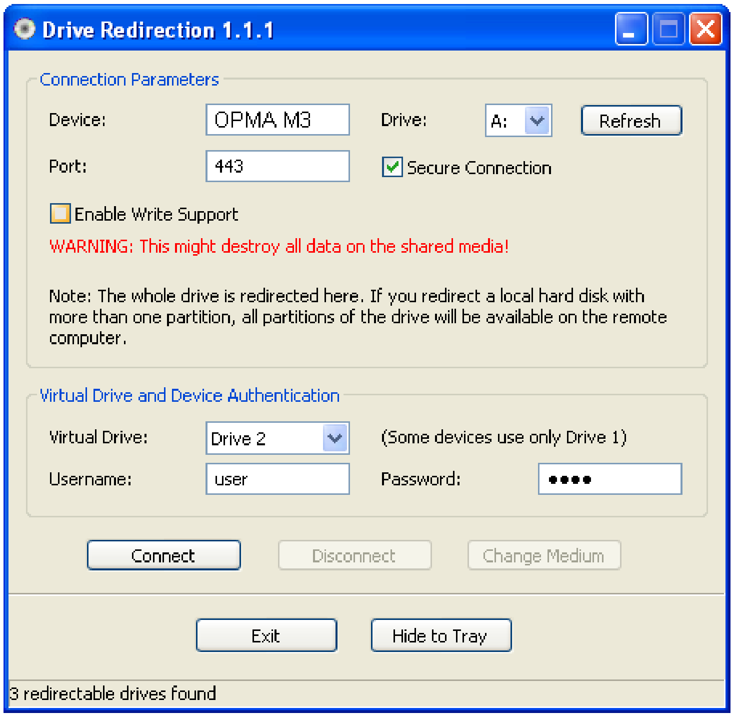
Software Requirements

To use this Drive Redirection feature, you can install the Drive Redirection software that is currently only available for Microsoft Windows. This software can be found on the product CD ROM.

On the other hand the Remote Console can be used for establishing a Drive Redirection connection to a CD ROM, Iso Image or other drive on client side. The Java applet offers the usage of a Drive Redirection menu like shown in Section **Remote Console Control Bar**.

Configuration

Figure 6 - 9. Main View



Device: OPMA M3

Drive: A:

Port: 443

☑ Secure Connection

□ Enable Write Support

WARNING: This might destroy all data on the shared media!

Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Virtual Drive: Drive 2

(Some devices use only Drive 1)

Username: user

Password: ●●●●

3 redirectable drives found

Specify the parameters of the network connection (see **Figure 6 - 9**).

Device

This is the address (either the DNS name or the IP address) of the OPMA module you would like to connect to.

Port

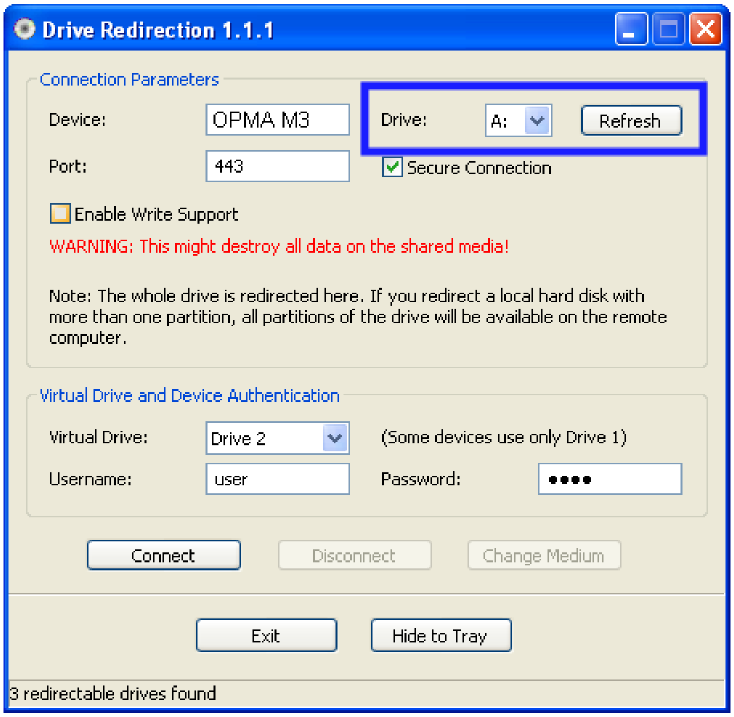
This is the network port. By default, OPMA module uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your OPMA module's network settings.

Secure Connection

Enable this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

Drive Selection

Figure 6 - 10. Selecting the Desired Drive



Drive Redirection 1.1.1

Connection Parameters

Device: OPMA M3

Port: 443

Drive: A:

☑ Secure Connection

□ Enable Write Support

WARNING: This might destroy all data on the shared media!

Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Virtual Drive and Device Authentication

Virtual Drive: Drive 2 (Some devices use only Drive 1)

Username: user

Password: ••••

3 redirectable drives found

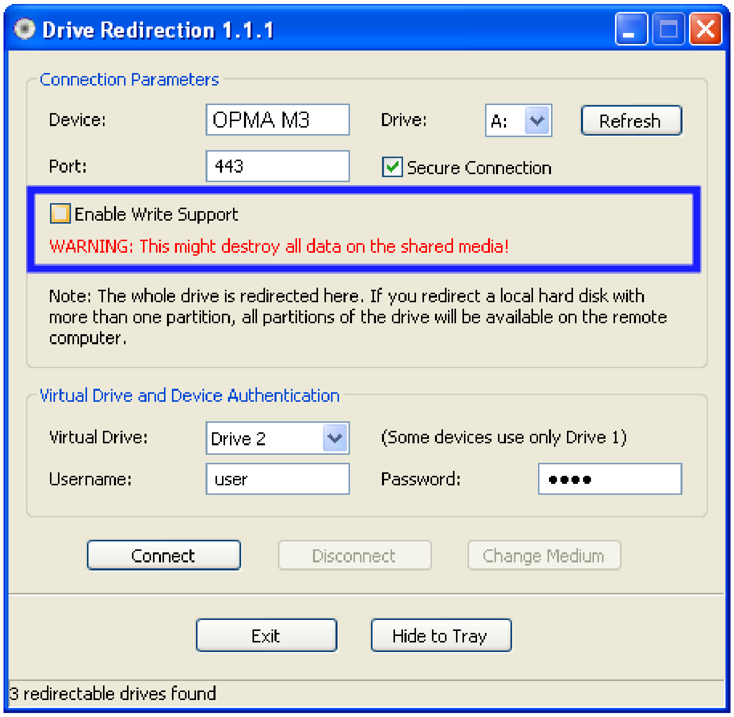
Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected.

The **Refresh** button may be used to regenerate the list of drive letters, especially for an USB stick.

Write Support

This feature may be enabled here.Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

Figure 6 - 11. Selecting Write Support



Drive Redirection 1.1.1

Connection Parameters

Device: OPMA M3

Drive: A:

Port: 443

☑ Secure Connection

☐ Enable Write Support

WARNING: This might destroy all data on the shared media!

Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Virtual Drive and Device Authentication

Virtual Drive: Drive 2

(Some devices use only Drive 1)

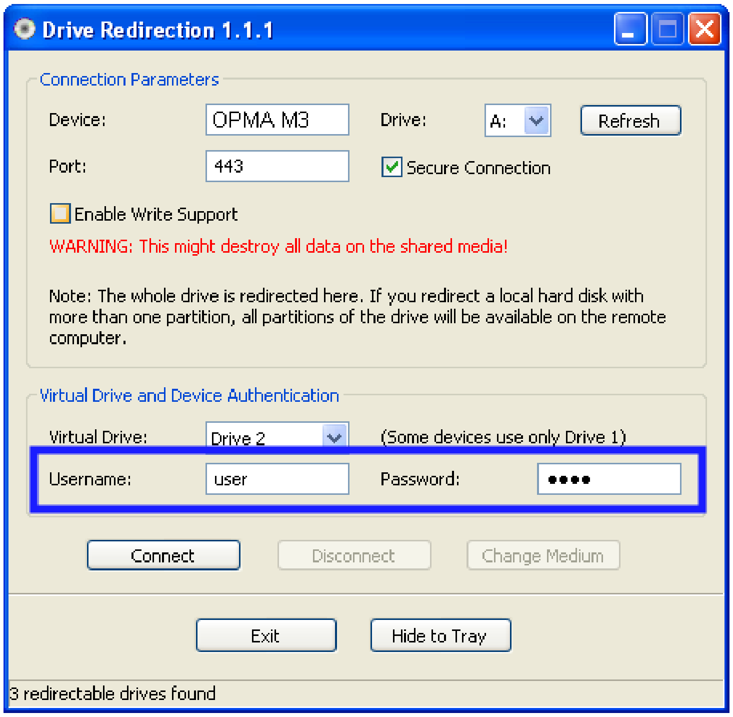
Username: user

Password: ●●●●

3 redirectable drives found

Device Authentication

Figure 6 - 12. Device Authentication



Drive Redirection 1.1.1

Connection Parameters

Device: OPMA M3

Drive: A:

Port: 443

☑ Secure Connection

☐ Enable Write Support

WARNING: This might destroy all data on the shared media!

Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.

Virtual Drive and Device Authentication

Virtual Drive: Drive 2

(Some devices use only Drive 1)

Username: user

Password: ●●●●

3 redirectable drives found

To use the Drive Redirection, you have to authenticate on the OPMA module using a valid username and password. You need permission to change the virtual disc configuration.

Navigation Buttons

Connect/Disconnect

To establish the drive redirection press the **Connect** button once. If all the settings are correct, the status bar displays that the connection has been established, the **Connect** button is disabled and the **Disconnect** button is enabled.

On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

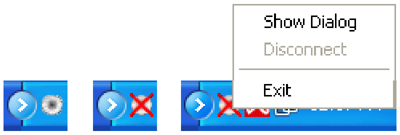
With the **Disconnect** button, a connection via Drive Redirection connection is stopped.

Exit/Hide

If the **Exit** button is pressed, the Drive Redirection software is closed. If a Drive Redirection connection is active, the connection will be closed before the application terminates.

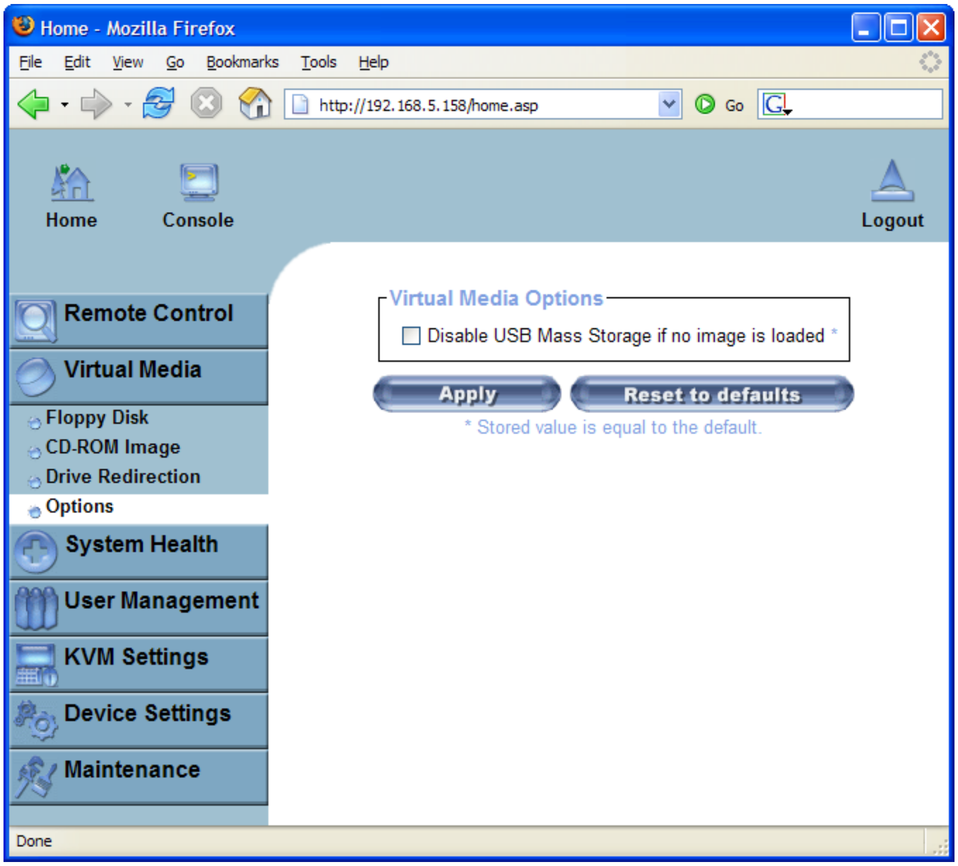
Using the **Hide to Tray** button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu (see **Figure 6 - 13**).

Figure 6 - 13. Tray Info



Options

Figure 6 - 14. USB Mass Storage Option



Virtual Media Options

□ Disable USB Mass Storage if no image is loaded *

* Stored value is equal to the default.

Set this option to disable the mass storage emulation (and hide the virtual drive) as long as no image file is currently loaded. If unset and no file image will be found, it may happen that the host system will hang on boot due to changes in the boot order or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS may not be fully excluded. This behaviour depends on the BIOS version used in that machine.

To set this option press the **Apply** button.

Creating an Image

Floppy Images

UNIX and UNIX-like OS

To create an image file make use of "dd". This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux).

To create a floppy image file copy the floppy raw device to a file using the following command:

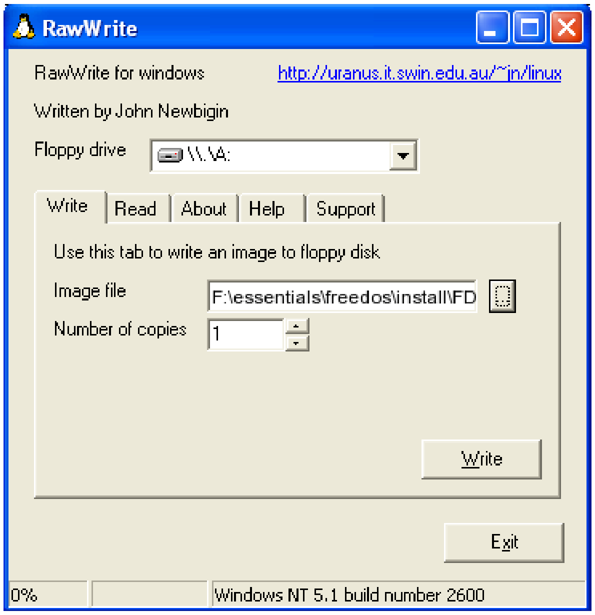
```
dd [if=/dev/fd0]  [of=/tmp/floppy.image]
```

dd reads the entire disc from the device `/dev/fd0` and saves the output in the specified output file `/tmp/floppy.image`. Adjust both parameters exactly to your needs (input device etc.)

MS Windows

You can use the tool "RawWrite for Windows". It is included on the CD ROM shipped with the OPMA module.

Figure 6 - 15. RawWrite for Windows Selection Dialog



RawWrite for windows http://uranus.it.swin.edu.au/~jn/linux

Written by John Newbigin

Floppy drive \\.\A:

Use this tab to write an image to floppy disk

Image file F:\essentials\freedos\install\FD

Number of copies 1

0% Windows NT 5.1 build number 2600

Select the tab **Read** from the menu. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the **Copy** button to initiate the image creation process.

For related tools you may have a look at the homepage of the fdos project (`http://www.fdos.org/ripcord/rawrite/`).

CD ROM/ISO 9660 Images

UNIX and UNIX-like OS

To create an image file make use of "dd". This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux).

To create a CDROM image file you have to copy the contents of the CDROM to a file. Use the following command:

```
dd [if=/dev/cdrom] [of=/tmp/cdrom.image]
```

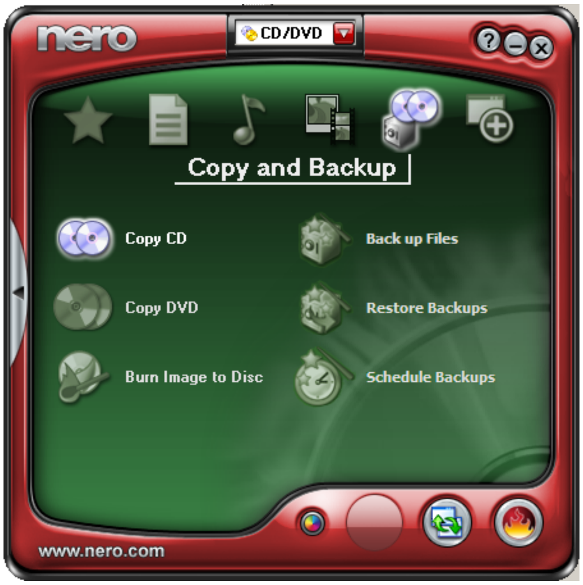
dd reads the entire disc from the device `/dev/cdrom` and saves the output in the specified output file `/tmp/cdrom.image`. Adjust both parameters to suit your needs (input device etc.).

MS Windows

To create the image file use your favourite CD imaging tool to oopy the whole contents of the disc into one single ISO image file on your harddisk.

For example, with **Nero** you choose **Copy and Backup**. Then, navigate to the **Copy Disc** section. Select the CD ROM or DVD drive you would like to create an ISO image from. Specify the filename of the ISO image and save the CD ROM content in that file.

Figure 6 - 16. Nero Selecting Dialog

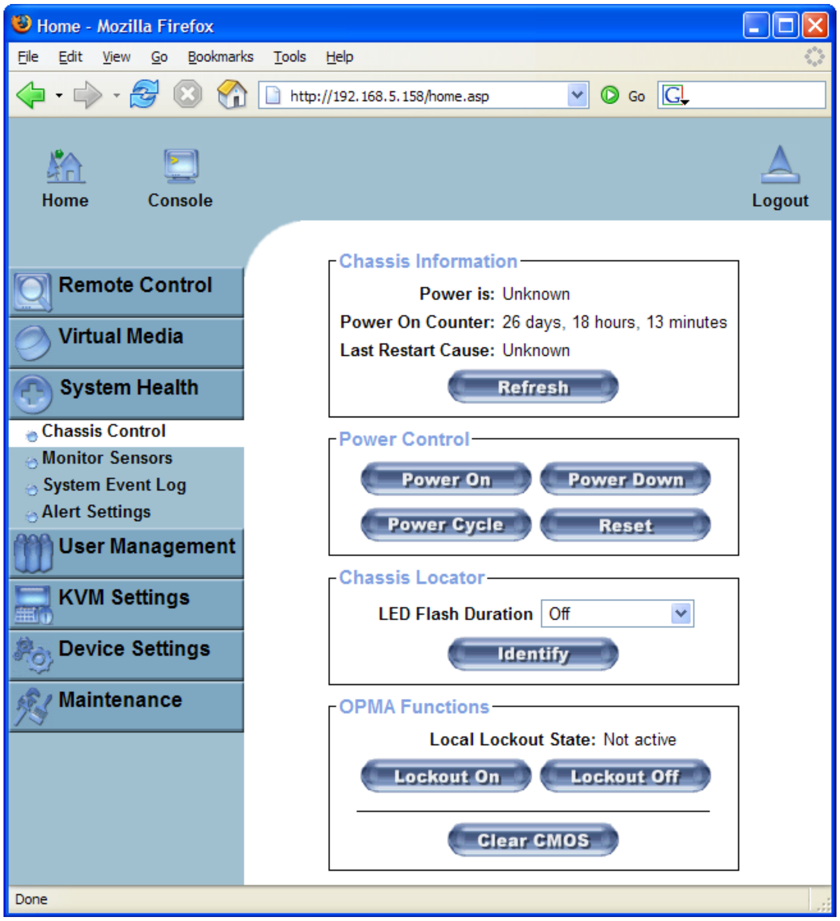


System Health

The IPMI support on the OPMA module allows you to power cycle the remote host system or to perform a hard reset. Additonally you can see the remote event log and interrogate the state of some system sensors like for example temperature.

Chassis Control

Figure 6 - 17. Chassis Control



http://192.168.5.158/home.asp

Power is: Unknown

Power On Counter: 26 days, 18 hours, 13 minutes

Last Restart Cause: Unknown

LED Flash Duration: Off

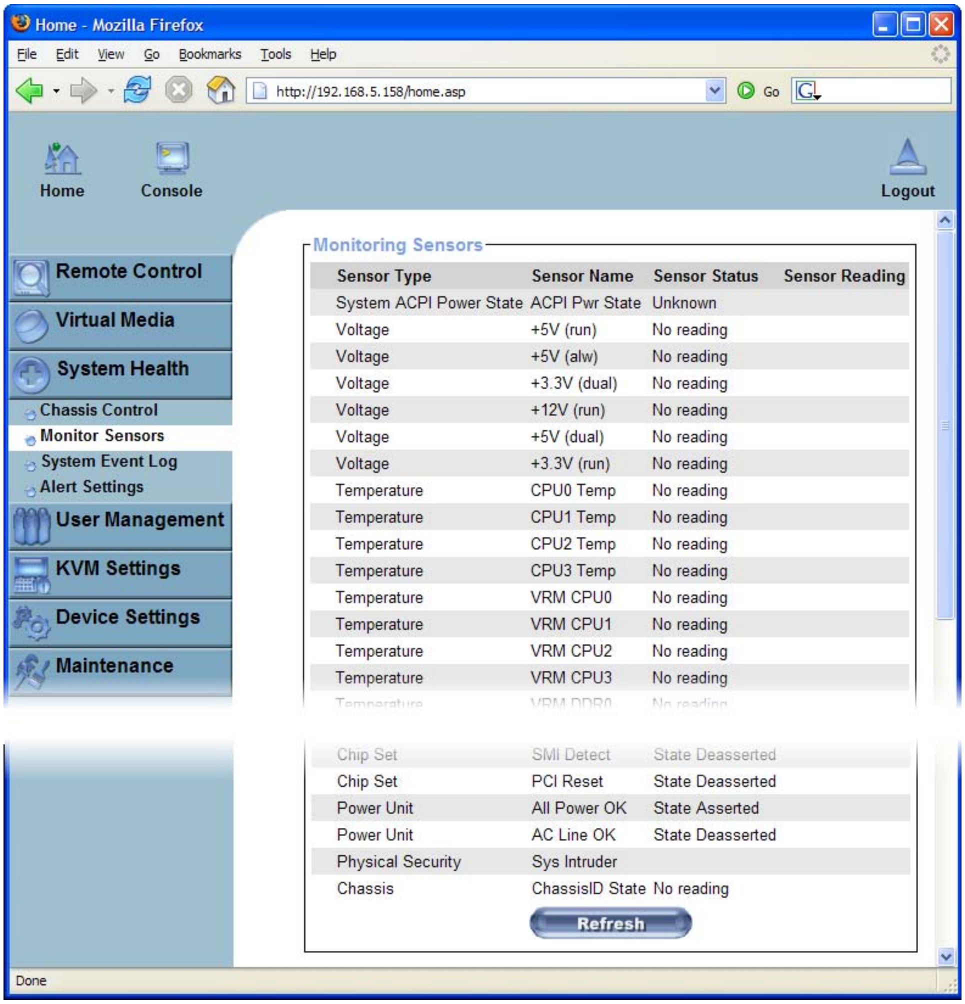
Local Lockout State: Not active

Using Chassis Control you can:

- Obtain information about the selected chassis
- Switch the remote power on and off (power cycle)
- Locate the remote host chassis
- Enable or disable the power and NMI reset buttons on the front panel

Monitor Sensors

Figure 6 - 18. Monitoring Remote Sensors Screen



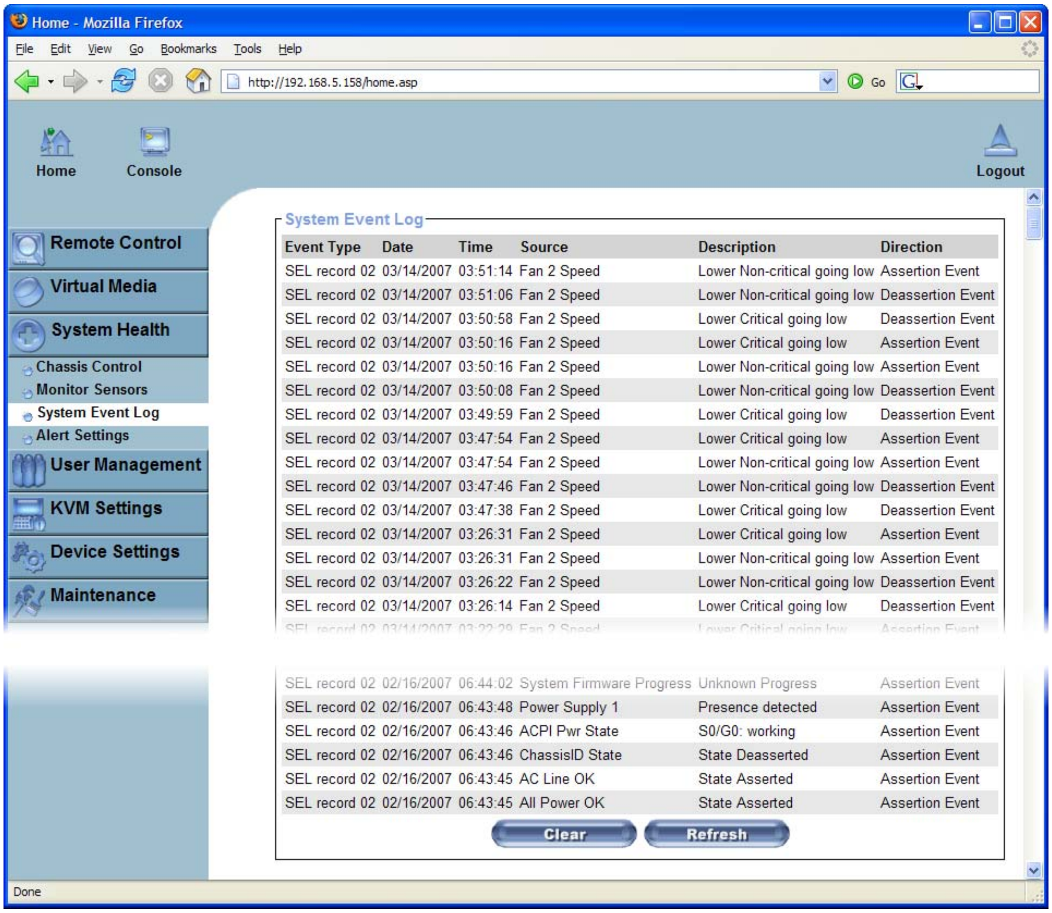
Monitoring Sensors

Sensor Type	Sensor Name	Sensor Status	Sensor Reading
System ACPI Power State	ACPI Pwr State	Unknown	
Voltage	+5V (run)	No reading	
Voltage	+5V (alw)	No reading	
Voltage	+3.3V (dual)	No reading	
Voltage	+12V (run)	No reading	
Voltage	+5V (dual)	No reading	
Voltage	+3.3V (run)	No reading	
Temperature	CPU0 Temp	No reading	
Temperature	CPU1 Temp	No reading	
Temperature	CPU2 Temp	No reading	
Temperature	CPU3 Temp	No reading	
Temperature	VRM CPU0	No reading	
Temperature	VRM CPU1	No reading	
Temperature	VRM CPU2	No reading	
Temperature	VRM CPU3	No reading	
Temperature	VRM DDR0	No reading	
Chip Set	SMI Detect	State Deasserted	
Chip Set	PCI Reset	State Deasserted	
Power Unit	All Power OK	State Asserted	
Power Unit	AC Line OK	State Deasserted	
Physical Security	Sys Intruder		
Chassis	ChassisID State	No reading	

On this screen you can see some of the remote hosts sensors and their values or state.

System Event Log

Figure 6 - 19. System Event Log Screen



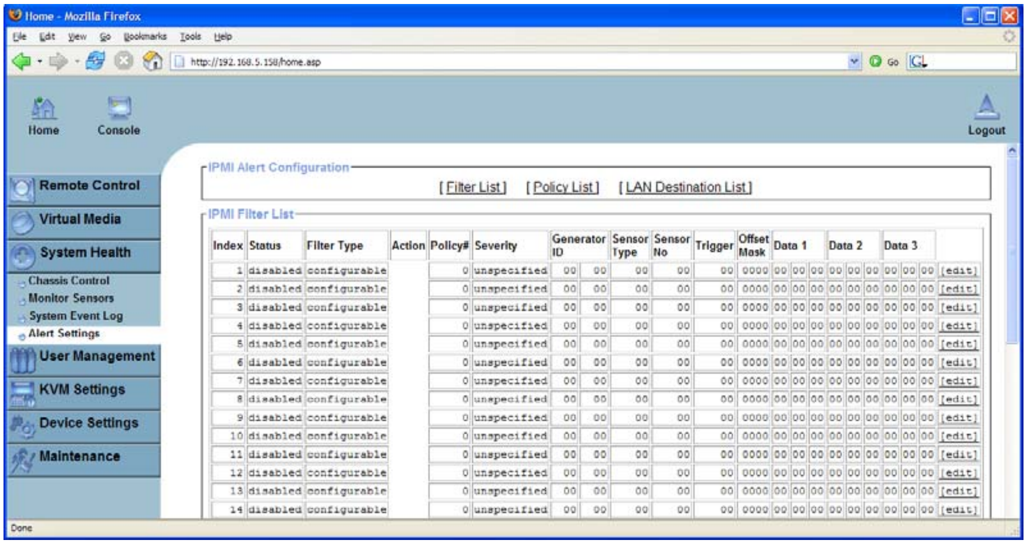
System Event Log

Event Type	Date	Time	Source	Description	Direction
SEL record 02	03/14/2007	03:51:14	Fan 2 Speed	Lower Non-critical going low	Assertion Event
SEL record 02	03/14/2007	03:51:06	Fan 2 Speed	Lower Non-critical going low	Deassertion Event
SEL record 02	03/14/2007	03:50:58	Fan 2 Speed	Lower Critical going low	Deassertion Event
SEL record 02	03/14/2007	03:50:16	Fan 2 Speed	Lower Critical going low	Assertion Event
SEL record 02	03/14/2007	03:50:16	Fan 2 Speed	Lower Non-critical going low	Assertion Event
SEL record 02	03/14/2007	03:50:08	Fan 2 Speed	Lower Non-critical going low	Deassertion Event
SEL record 02	03/14/2007	03:49:59	Fan 2 Speed	Lower Critical going low	Deassertion Event
SEL record 02	03/14/2007	03:47:54	Fan 2 Speed	Lower Critical going low	Assertion Event
SEL record 02	03/14/2007	03:47:54	Fan 2 Speed	Lower Non-critical going low	Assertion Event
SEL record 02	03/14/2007	03:47:46	Fan 2 Speed	Lower Non-critical going low	Deassertion Event
SEL record 02	03/14/2007	03:47:38	Fan 2 Speed	Lower Critical going low	Deassertion Event
SEL record 02	03/14/2007	03:26:31	Fan 2 Speed	Lower Critical going low	Assertion Event
SEL record 02	03/14/2007	03:26:31	Fan 2 Speed	Lower Non-critical going low	Assertion Event
SEL record 02	03/14/2007	03:26:22	Fan 2 Speed	Lower Non-critical going low	Deassertion Event
SEL record 02	03/14/2007	03:26:14	Fan 2 Speed	Lower Critical going low	Deassertion Event
SEL record 02	03/14/2007	03:22:29	Fan 2 Speed	Lower Critical going low	Assertion Event
SEL record 02	02/16/2007	06:44:02	System Firmware Progress	Unknown Progress	Assertion Event
SEL record 02	02/16/2007	06:43:48	Power Supply 1	Presence detected	Assertion Event
SEL record 02	02/16/2007	06:43:46	ACPI Pwr State	S0/G0: working	Assertion Event
SEL record 02	02/16/2007	06:43:46	ChassisID State	State Deasserted	Assertion Event
SEL record 02	02/16/2007	06:43:45	AC Line OK	State Asserted	Assertion Event
SEL record 02	02/16/2007	06:43:45	All Power OK	State Asserted	Assertion Event

You can browse the System Event Logs here. Note: these logs are for IPMI events. These are different from the OPMA module’s own system logs.

System Alert Management

Figure 6 - 20. System Alert Settings



IPMI Alert Configuration

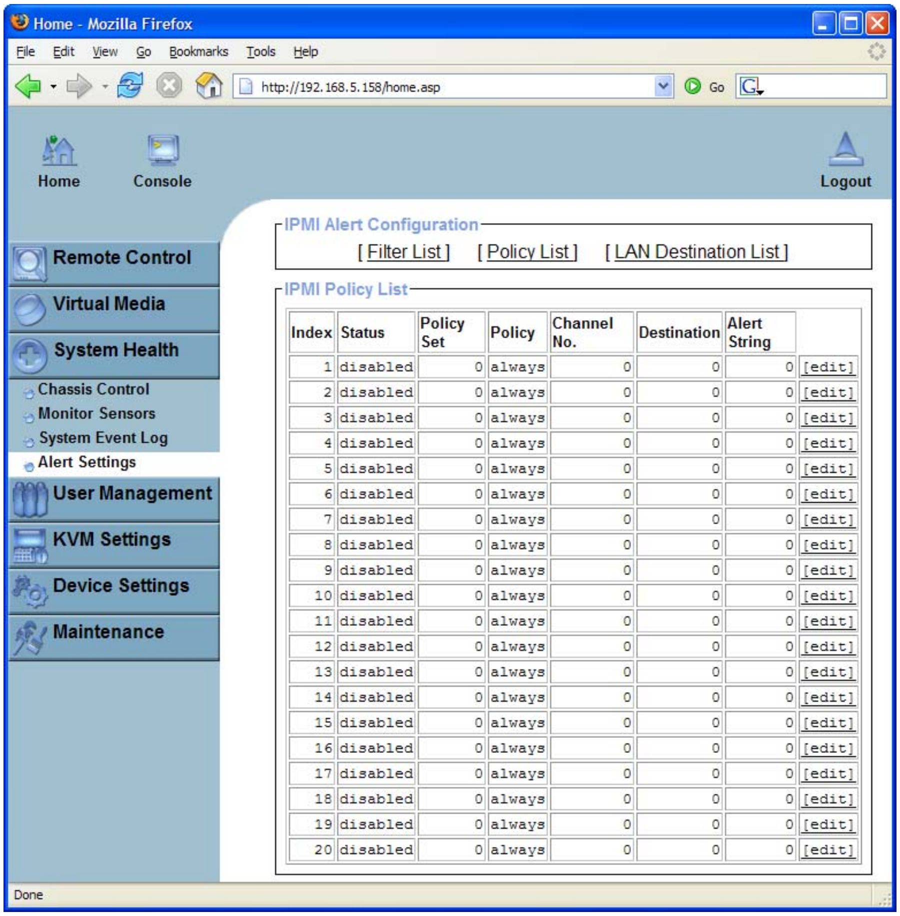
[Filter List] [Policy List] [LAN Destination List]

IPMI Filter List

Index	Status	Filter Type	Action	Policy#	Severity	Generator ID		Sensor Type	Sensor No	Trigger	Offset Mask	Data 1			Data 2			Data 3			
1	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
2	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
3	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
4	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
5	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
6	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
7	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
8	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
9	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
10	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
11	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
12	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
13	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]
14	disabled	configurable		0	unspecified	00	00	00	00	00	0000	00	00	00	00	00	00	00	00	00	[edit]

This screen shows all of the system alerts. You can also set up filters, policies and LAN destinations, where the module will send the alerts. Please see the IPMI Specifications for more details.

Figure 6 - 21. System Alert Policy Settings



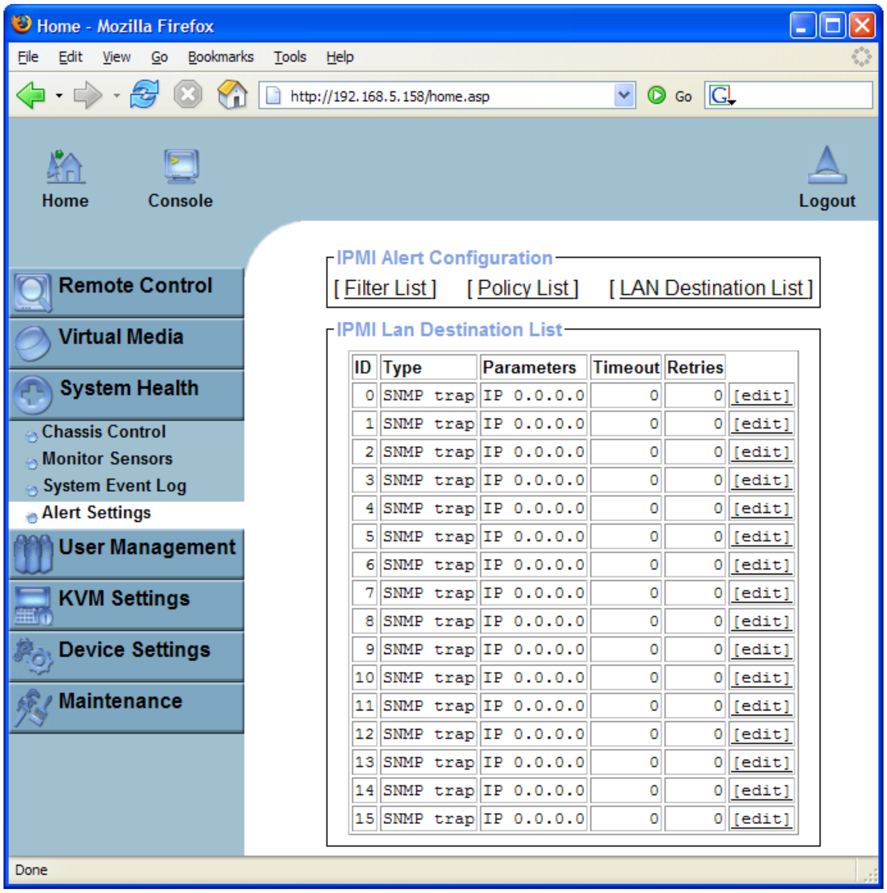
IPMI Alert Configuration

[Filter List] [Policy List] [LAN Destination List]

IPMI Policy List

Index	Status	Policy Set	Policy	Channel No.	Destination	Alert String	
1	disabled	0	always	0	0	0	[edit]
2	disabled	0	always	0	0	0	[edit]
3	disabled	0	always	0	0	0	[edit]
4	disabled	0	always	0	0	0	[edit]
5	disabled	0	always	0	0	0	[edit]
6	disabled	0	always	0	0	0	[edit]
7	disabled	0	always	0	0	0	[edit]
8	disabled	0	always	0	0	0	[edit]
9	disabled	0	always	0	0	0	[edit]
10	disabled	0	always	0	0	0	[edit]
11	disabled	0	always	0	0	0	[edit]
12	disabled	0	always	0	0	0	[edit]
13	disabled	0	always	0	0	0	[edit]
14	disabled	0	always	0	0	0	[edit]
15	disabled	0	always	0	0	0	[edit]
16	disabled	0	always	0	0	0	[edit]
17	disabled	0	always	0	0	0	[edit]
18	disabled	0	always	0	0	0	[edit]
19	disabled	0	always	0	0	0	[edit]
20	disabled	0	always	0	0	0	[edit]

Figure 6 - 22. System Alert LAN Destinition Settings



IPMI Alert Configuration

[Filter List] [Policy List] [LAN Destination List]

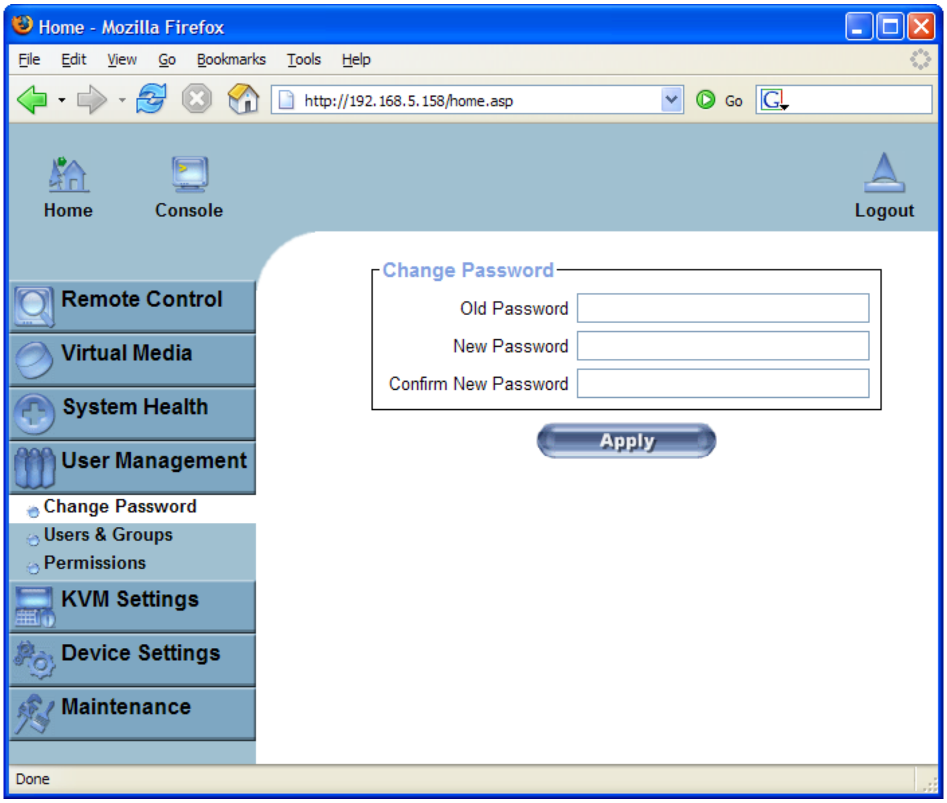
IPMI Lan Destination List

ID	Type	Parameters	Timeout	Retries	
0	SNMP trap	IP 0.0.0.0	0	0	[edit]
1	SNMP trap	IP 0.0.0.0	0	0	[edit]
2	SNMP trap	IP 0.0.0.0	0	0	[edit]
3	SNMP trap	IP 0.0.0.0	0	0	[edit]
4	SNMP trap	IP 0.0.0.0	0	0	[edit]
5	SNMP trap	IP 0.0.0.0	0	0	[edit]
6	SNMP trap	IP 0.0.0.0	0	0	[edit]
7	SNMP trap	IP 0.0.0.0	0	0	[edit]
8	SNMP trap	IP 0.0.0.0	0	0	[edit]
9	SNMP trap	IP 0.0.0.0	0	0	[edit]
10	SNMP trap	IP 0.0.0.0	0	0	[edit]
11	SNMP trap	IP 0.0.0.0	0	0	[edit]
12	SNMP trap	IP 0.0.0.0	0	0	[edit]
13	SNMP trap	IP 0.0.0.0	0	0	[edit]
14	SNMP trap	IP 0.0.0.0	0	0	[edit]
15	SNMP trap	IP 0.0.0.0	0	0	[edit]

User Management

Change Password

Figure 6 - 23. Set Password

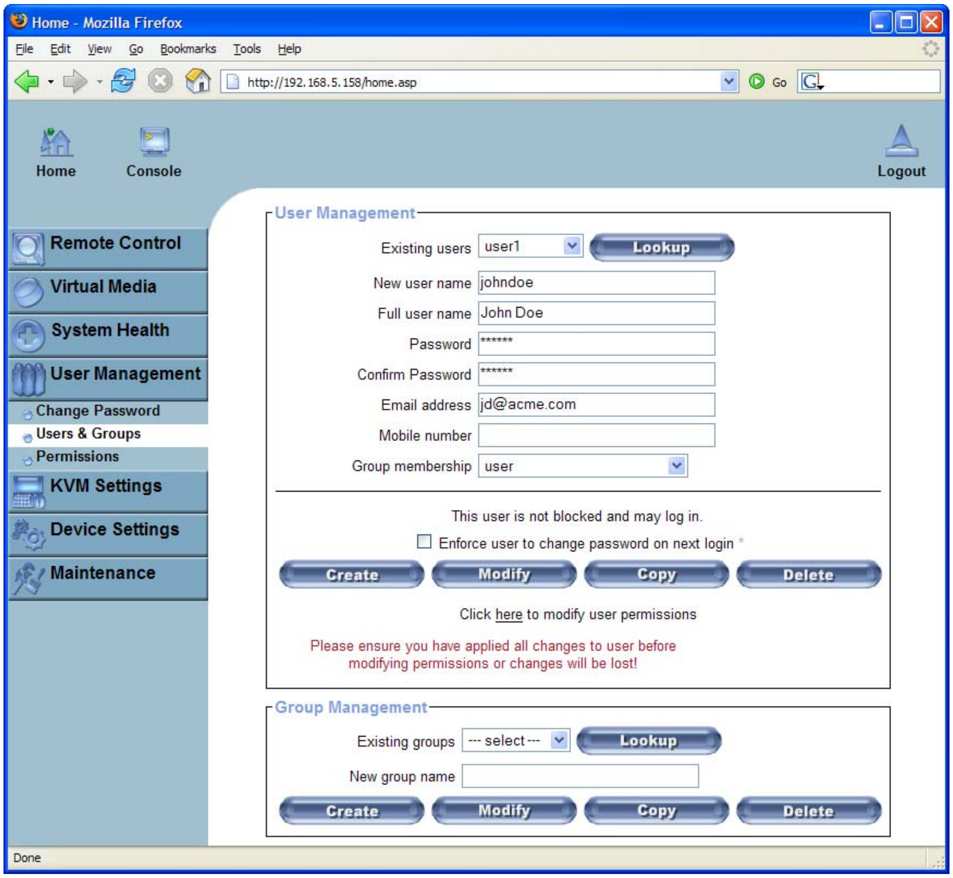


To change your password enter the new password in the upper entry field. Retype the password in the field below.

Click **Apply** to submit your changes.

Users And Groups

Figure 6 - 24. Set User



User Management

Existing users	user1
New user name	johndoe
Full user name	John Doe
Password	******
Confirm Password	******
Email address	jd@acme.com
Mobile number	
Group membership	user

This user is not blocked and may log in.

☐ Enforce user to change password on next login *

Click here to modify user permissions

Please ensure you have applied all changes to user before modifying permissions or changes will be lost!

Group Management

Existing groups	--- select ---
New group name	

User Management

The configurable settings of the OPMA module are split into user settings (basically authentication and user information) and group settings (authorization).

There is one predefined user "admin" and two predefined group "admin" and "<unknown>", which cannot be renamed or deleted.

Each user may be member of one group and inherits permissions set for this group. If a user is not member of a group, permissions can be set exclusively for that user. The user “admin” is always member of admin group which has full system access. The <unknown> group initially does not have any permissions, but is modifiable.

Users can authenticate against a remote authentication service (such as LDAP or RADIUS). If this remote authentication service returns an invalid or no group assignment, the user is considered to be member of the <unknown> group.

Upon delivery, the account for the user “admin” has the password “raritan”. Make sure to change the password immediately after you have installed and first accessed your OPMA module.

List of Available Options

A full list of available options follows. This list can only be seen by the superuser.

Existing users

Select an existing user for modification. Once a user has been selected, click the L**ookup** button to see the user information.

New user name

The new user name for the selected account.

Password

The password for the login name. It must be at least four characters long.

Confirm Password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

Role

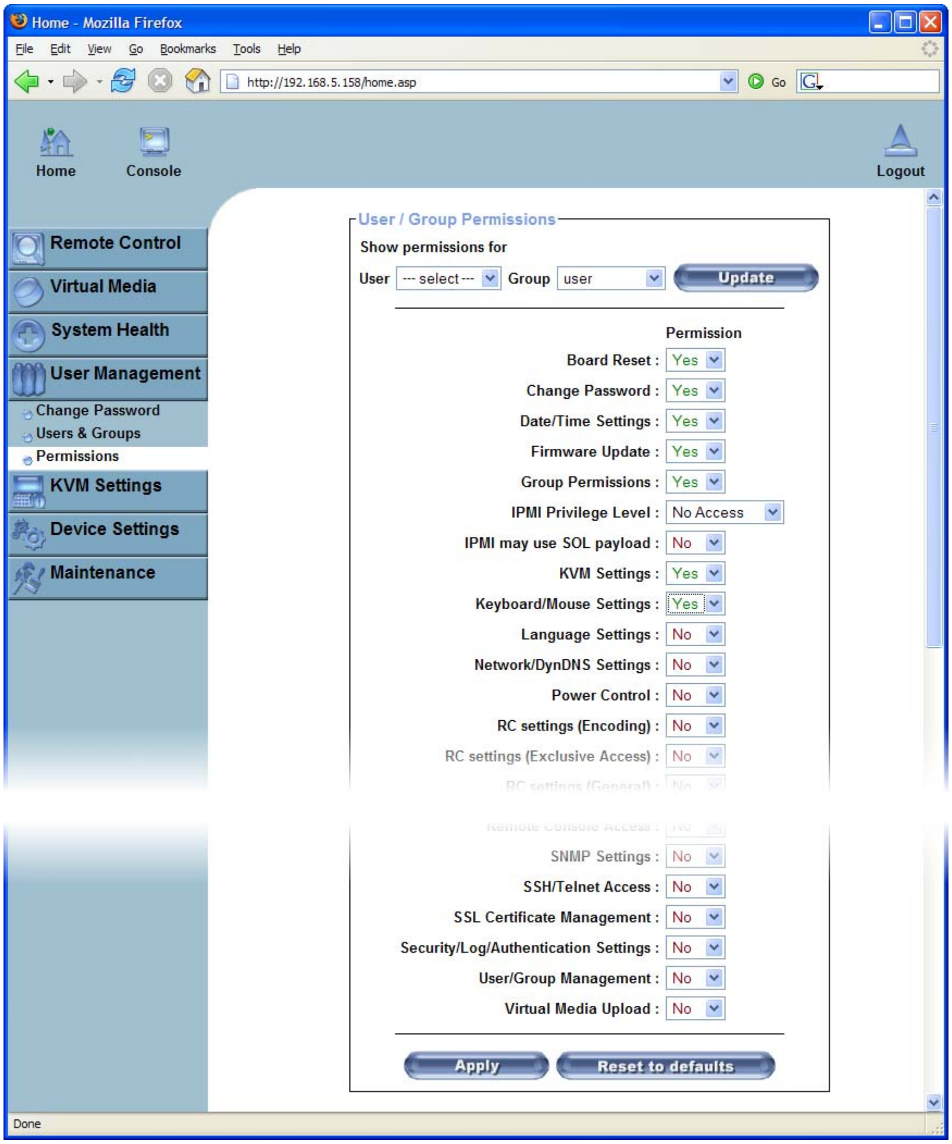
Each user can be a member of a group (named a "role") - either an administrator, or a regular user. Choose the desired role from the selection box.

To create a user press the **Create** button. The **Modify** button changes the displayed user settings. To delete an user press the **Delete** button.

Note: *The OPMA module is equipped with an host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not to exceed the number of 25 users connected to the OPMA module at the same time. The memory space that is available onto the OPMA module mainly depends on the configuration and the usage of the OPMA module (log file entries etc.). That’s why we recommend not to store more than 150 user profiles.*

Permissions

Figure 6 - 25. Set Permissions for the Group “user”



User / Group Permissions

Show permissions for

User --- select --- Group user

	Permission
Board Reset :	Yes
Change Password :	Yes
Date/Time Settings :	Yes
Firmware Update :	Yes
Group Permissions :	Yes
IPMI Privilege Level :	No Access
IPMI may use SOL payload :	No
KVM Settings :	Yes
Keyboard/Mouse Settings :	Yes
Language Settings :	No
Network/DynDNS Settings :	No
Power Control :	No
RC settings (Encoding) :	No
RC settings (Exclusive Access) :	No
RC settings (General) :	No
Remote Console Access :	No
SNMP Settings :	No
SSH/Telnet Access :	No
SSL Certificate Management :	No
Security/Log/Authentication Settings :	No
User/Group Management :	No
Virtual Media Upload :	No

This page allows you to set the permissions for each user or group. You select the item (user and/or group) from the drop-down menu. All changes you make then affect the permission set of the selected entity. The user can only access and use the selected function if the permissions field is set to "yes".

Again most entries are fairly self-explanatory. The fields labelled RC Settings pertain to the settings of the Remote Console.

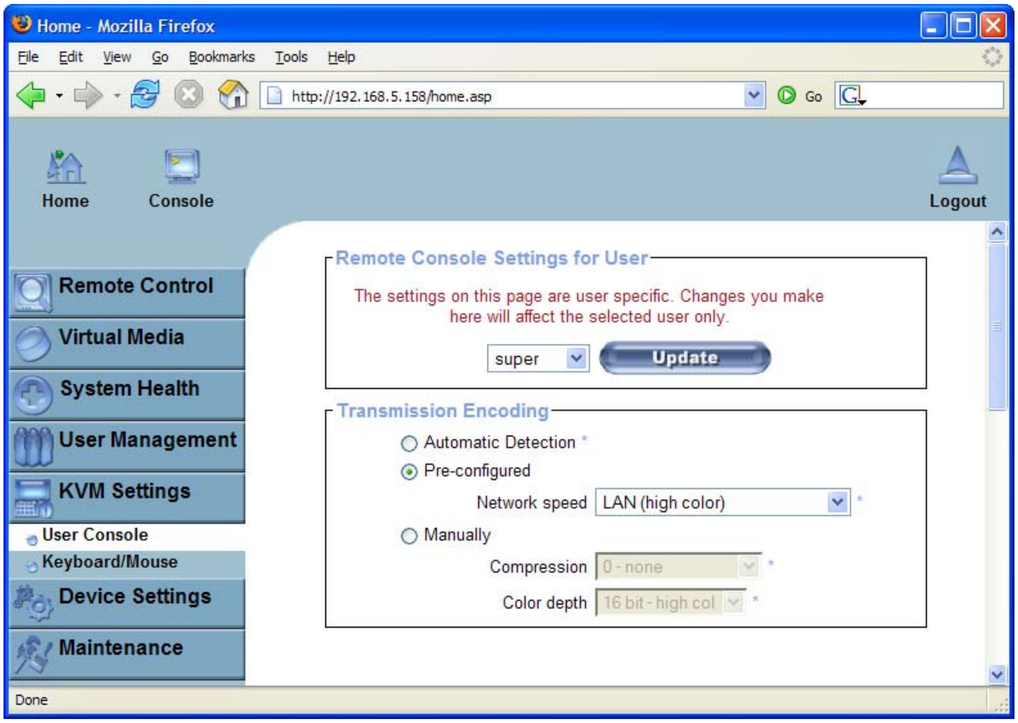
A kind of special case is the field "IPMI may use SOL payload". this sets if the user/group is allowed to use administrative sessions over the serial line.

KVM Settings

User Console

The following settings are user specific. That means the super user can customize these settings for every user. Changing the settings for one user does not affect the settings of other users.

Figure 6 - 26. User Console Settings (Part 1)



Remote Console Settings for User

The settings on this page are user specific. Changes you make here will affect the selected user only.

super

Transmission Encoding

○ Automatic Detection *
● Pre-configured
Network speed: LAN (high color) *
○ Manually
Compression: 0 - none *
Color depth: 16 bit - high col *

Remote Console Settings for Users

This selection box displays the user ID for which the values are shown and for which the changes will take effect. Select the desired user from the selection box and press the **Update** button. This will result in displaying the according user settings below.

Note: *You are allowed to change the settings of other users only if you have the necessary access rights for this task. For a regular user without the correct permissions it is not possible to change the settings for any other user.*

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

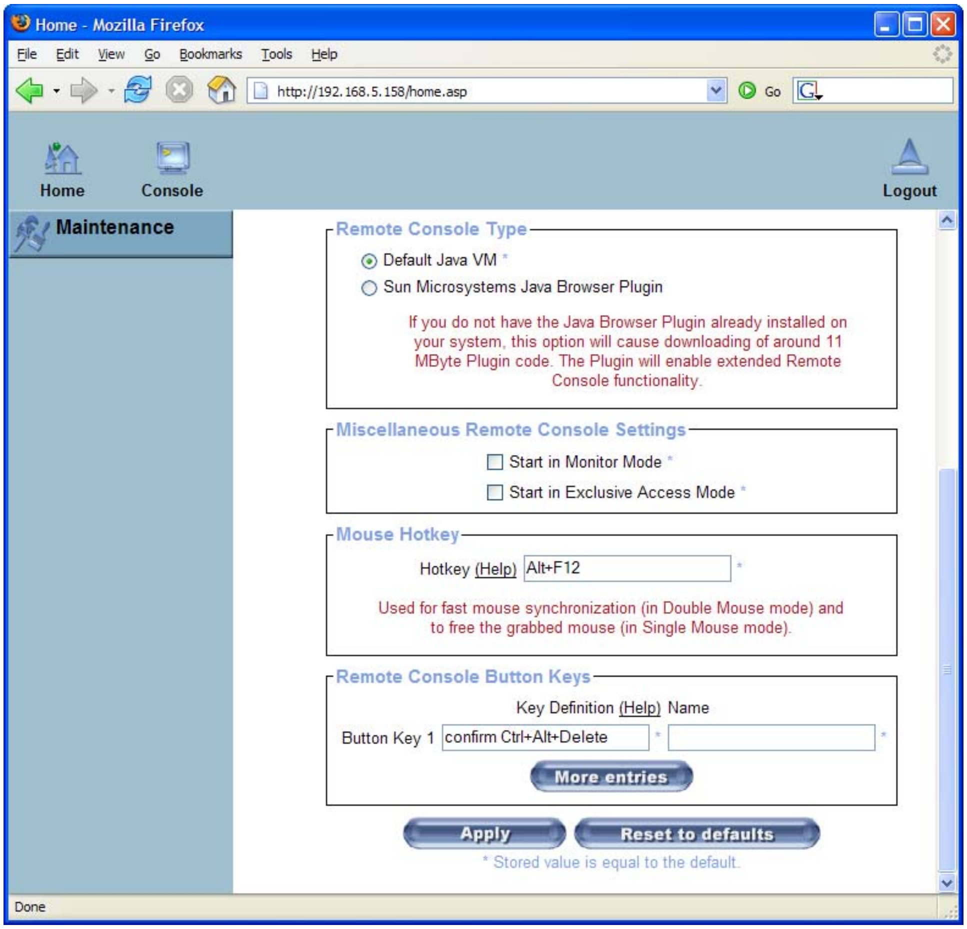
The pre-configured settings deliver the best result because of optimized adjustment of compression and color depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the color depth individually. Depending on the selected compression rate the data stream between the OPMA module and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used while several users are accessing the OPMA module simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Figure 6 - 27. User Console Settings (Part 2)



Remote Console Type

● Default Java VM *

○ Sun Microsystems Java Browser Plugin

If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.

Miscellaneous Remote Console Settings

□ Start in Monitor Mode *

□ Start in Exclusive Access Mode *

Mouse Hotkey

Hotkey (Help) Alt+F12 *

Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).

Remote Console Button Keys

	Key Definition (Help)	Name
Button Key 1	confirm Ctrl+Alt+Delete *	*

* Stored value is equal to the default.

Remote Console Type

Specifies which Remote Console Viewer to use.

Default Java Virtual Machine (JVM)

Uses the default JVM of your web browser. This may be the Microsoft JVM for the Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not yet installed on your system, it may be downloaded and installed automatically. However, in order to make the installation possible, you still have to answer the according dialogs with "yes". The download volume is around 11 Mbytes. The advantage of downloading Sun’s JVM is the usage of a stable and identical JVM across different platforms. The Remote Console software is optimized for this JVM version and offers a wider range of functionality when run in SUN’s JVM. (Hint: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine. The software is available on the CD ROM that is delivered along with the OPMA module.

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is disabled. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. Nobody else can open the Remote Console at the same time again until you disable this feature or log off.

Mouse Hotkey

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console or is used to leave the single mouse mode. This is only available if you have selected the Mouse Mode "Other Operating System".

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or just the fact that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are "`Control+Alt+Delete`" on Windows and DOS, that is always caught, or the key sequence "`Control+Backspace`" on Linux that can be used for terminating the X-Server.

In order to define a new Button Key or to adjust an existing one have a look at the rules that describe the setting for a key. In general, the syntax for a key is as follows:

```
    [confirm] <keycode>[+|-|>[*]<keycode>]*
```

A term in brackets is optional. The star at the end means that you add further keys as often as required for your case. The term "confirm" adds an confirmation dialogue that is displayed before the key strokes will be sent to the remote host.

The "keycode" is the key to be sent. Multiple key codes can be concatenated with either a plus, a minus, or an ">" sign. The plus sign builds key combinations - all the keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So, the minus sign builds single, separate keypresses and keyreleases. The ">" sign releases the last key, only. The star inserts a pause with a duration of 100 milliseconds.

As an example, the key combination of Ctrl, Alt and F2 is represented by the sequence

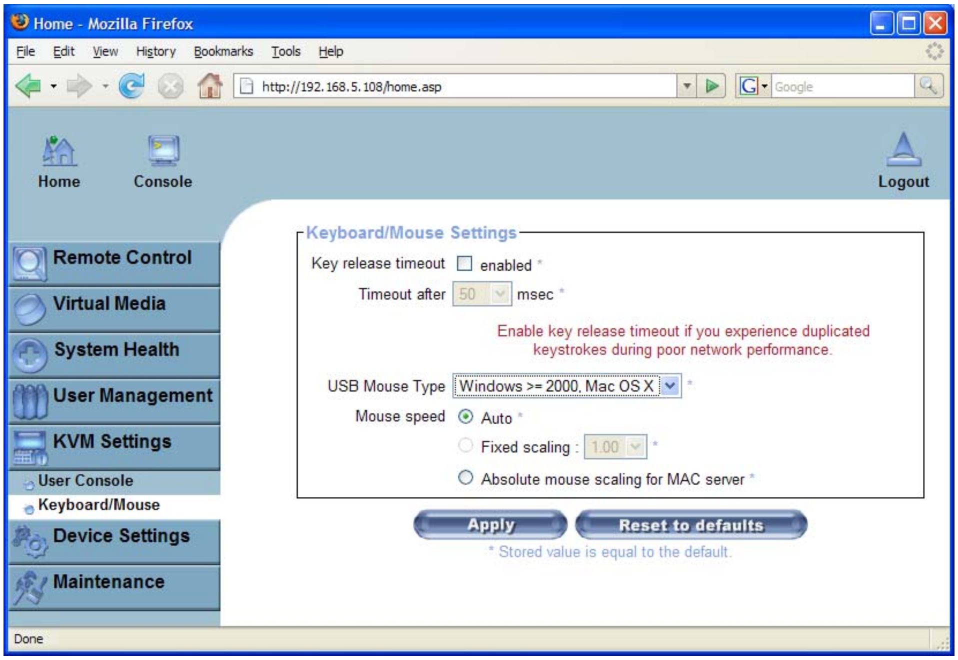
```
Ctrl+Alt+F2
```

For a full list of key codes and aliases please refer to the **Appendix E. Key Codes**.

Note: *If you need more button keys than shown use the button "More entries". This will open a list of additional entry fields.*

Keyboard/Mouse

Figure 6 - 28. Keyboard and Mouse Settings



Keyboard/Mouse Settings

Key release timeout ☐ enabled *

Timeout after 50 msec *

Enable key release timeout if you experience duplicated keystrokes during poor network performance.

USB Mouse Type Windows >= 2000, Mac OS X *

Mouse speed ● Auto *

○ Fixed scaling : 1.00 *

○ Absolute mouse scaling for MAC server *

* Stored value is equal to the default.

Key Release Timeout

This is an important option if you are accessing the OPMA module over a slow or congested network. In such a situation you transmit a network packet containing the key PRESS to the OPMA module.When you release the key, then the OPMA module will receive a corresponding RELEASE packet.When the network is slow then it take too long for the RELEASE packet to arrive. This might mislead the OPMA module to replicate the key press, this is like you holding down the desired key. The Key Release Timeout in Milli-Seconds tells the OPMA module to consider the key released, even if no RELEASE packet has arrived. This avoids keys being unwantedly repeated.

USB Mouse Type

Enables the USB mouse type. Choose an appropriate option from the selection box. Choose between "Windows >= 2000, MAC OS X" for MS Windows 2000, 2003 Server, XP, or "Other Operating Systems" for MS Windows NT, Linux, or OS X.

In "Windows >= 2000, MAC OS X" mode the remote mouse is always synchronized with the local mouse. For a detailed description about the mouse type and recommended options for the different operating systems see the Section called **Recommended Mouse Settings** in Chapter 4.

Mouse Speed

Auto mouse speed

> Use this option if the mouse settings on the host use an additional acceleration setting. The OPMA module tries to detect the acceleration and speed of the mouse during the mouse sync process.

Fixed mouse speed

> Use a direct translation of mouse movements between the local and the remote pointer.
>
> You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

Absolute mouse scaling for MAC systems

> Use this option if the host system use an MAC OS X.

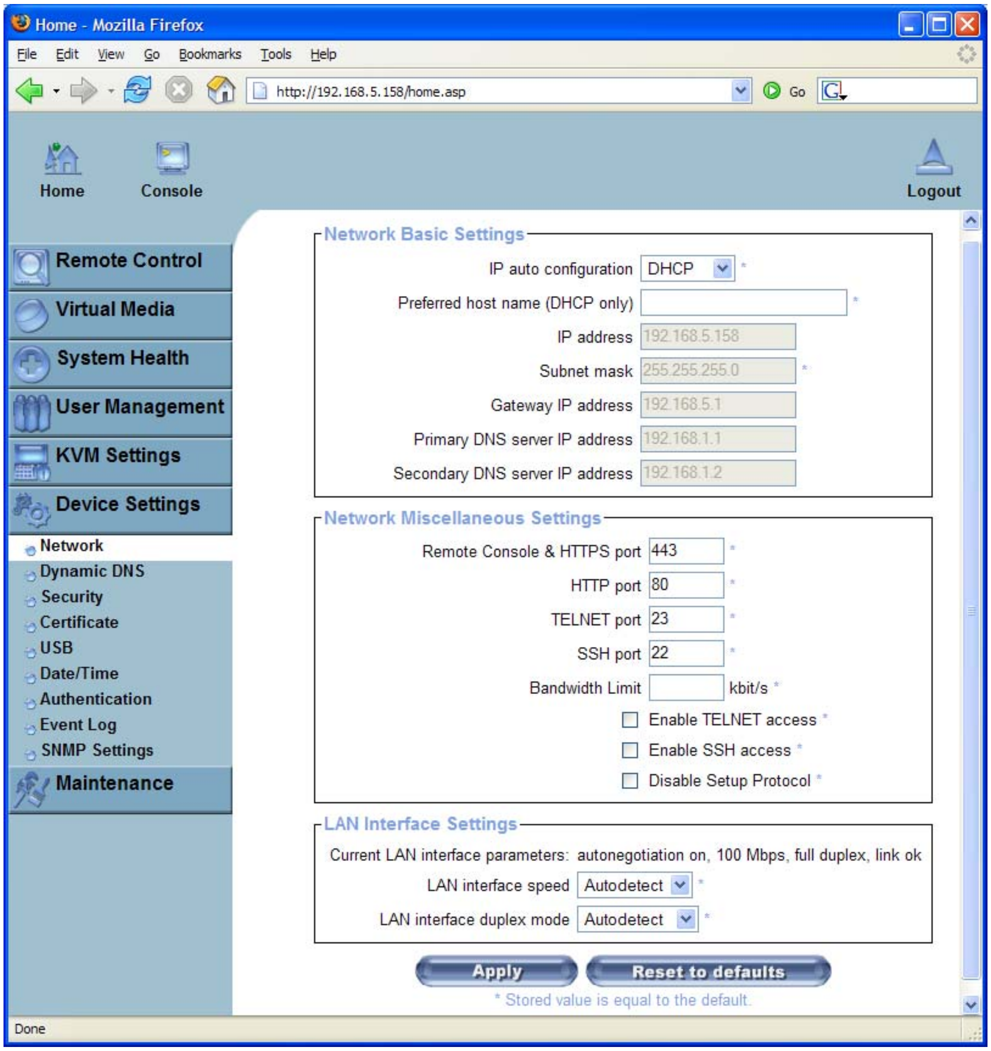
To set the options click on the **Apply** button.

Device Settings

Network

The Network Settings panel as shown in **Figure 6 - 29** allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

Figure 6 - 29. Network Settings



Network Basic Settings

IP auto configuration: DHCP *

Preferred host name (DHCP only): *

IP address: 192.168.5.158

Subnet mask: 255.255.255.0 *

Gateway IP address: 192.168.5.1

Primary DNS server IP address: 192.168.1.1

Secondary DNS server IP address: 192.168.1.2

Network Miscellaneous Settings

Remote Console & HTTPS port: 443 *

HTTP port: 80 *

TELNET port: 23 *

SSH port: 22 *

Bandwidth Limit: kbit/s *

□ Enable TELNET access *

□ Enable SSH access *

□ Disable Setup Protocol *

LAN Interface Settings

Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok

LAN interface speed: Autodetect *

LAN interface duplex mode: Autodetect *

* Stored value is equal to the default.

Warning: The initial IP configuration is usually done directly at the host system using the special procedure described in Table 4 - 1 in Chapter 4.

Warning: Changing the network settings of the OPMA module might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the OPMA module.

Basic Network Settings

IP auto configuration

With this option you can define if the OPMA module should fetch its network settings from a DHCP or BOOTP server. For DHCP select "dhcp" and for BOOTP select "bootp" accordingly. If you choose "none" then IP auto configuration is disabled.

Preferred host name

Preferred host name to request from DHCP server.Whether the DHCP server takes the OPMA module’s suggestion into account or not depends on the server configuration.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the OPMA module should be accessible from networks other than the local one, this IP address must be set to the local network router’s IP address.

Primary DNS Server IP Address

IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the OPMA module will not be able to perform name resolution.

Secondary DNS Server IP Address

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Miscellaneous Network Settings

Remote Console and HTTPS port

Port number at which the OPMA module’s Remote Console server and HTTPS server are listening. If lef.t empty the default value (port 444) will be used.

HTTP port

Port number at which the OPMA module’s HTTP server is listening. If left empty the default value (port 80) will be used.

Telnet port

Port number at which the OPMA module’s Telnet server is listening. If left empty the default value (port 25) will be used.

SSH port

Port number at which the OPMA module’s SSH (Secure SHell) server is listening. If left empty the default value (port 22) will be used.

Bandwidth Limit

The maximum network traffic generated through the OPMA module Ethernet device. Value in Kbit/s.

Enable Telnet

This enables the Telnet client mode.

Enable SSH

This enables the SSH (Secure SHell) client mode.

Disable Setup Protocol

Enable this option to exclude the OPMA module from the setup protocol.

LAN Interface Settings

This entry field displays the current settings for the Ethernet/LAN interface of the OPMA module. You may choose between auto negotiation and a fixed setting for the Ethernet transceiver settings "interface speed" and "duplex mode" in case auto negotiation does not work correctly.

LAN interface speed

Depending on your network connection you may select an according speed value for this interface. To adjust the interface automatically choose "autodetect" (default value). If this selection results in misbehaviour of the interface, choose one of other speed options to work with. The interface will transmit and receive data with that fixed speed.

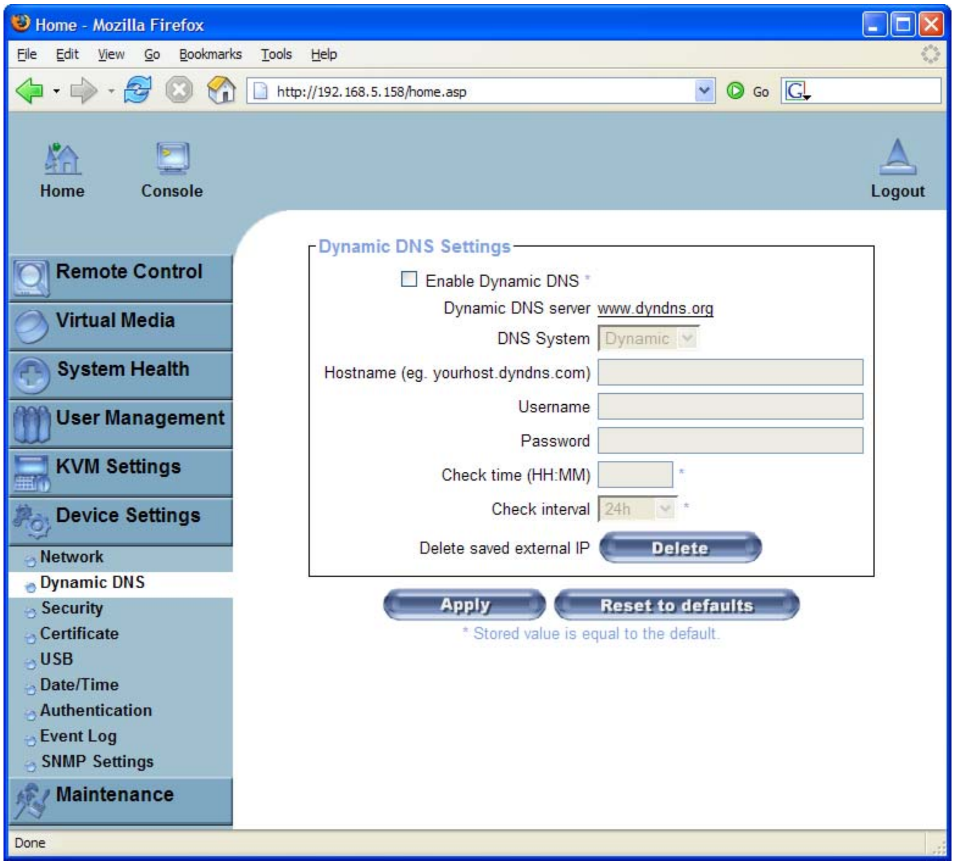
LAN interface duplex mode

If necessary you may also select a specific duplex mode. The default value is set to "autodetect" which leads to an automatic setting of the duplex mode depending on your network (recommended). As an alternative you may explicitly set the interface to either "half duplex" or "full duplex" mode.

These settings may also be configured via serial console. See the Section called **Initial Configuration via Serial Console** in Chapter 4 for details.

Dynamic DNS

Figure 6 - 30. Dynamic DNS



Dynamic DNS Settings

☐ Enable Dynamic DNS *

Dynamic DNS server www.dyndns.org

DNS System Dynamic

Hostname (eg. yourhost.dyndns.com)

Username

Password

Check time (HH:MM) *

Check interval 24h *

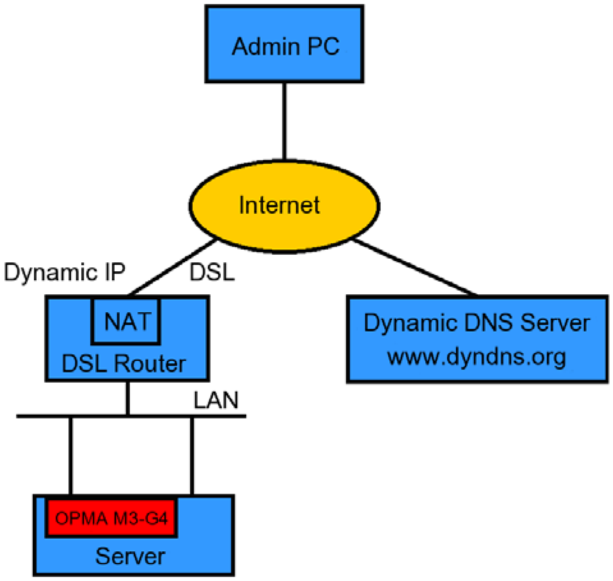
Delete saved external IP Delete

Apply Reset to defaults

* Stored value is equal to the default.

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario (see **Figure 6 - 30**):

Figure 6 - 31. Dynamic DNS Scenario



The OPMA module is reachable via the IP address of the DSL router which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the OPMA module connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card.

The administrator has to register the OPMA module that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return to the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered OPMA module.

You have to perform the following steps in order to enable Dynamic DNS:

1. Make sure that the LAN interface of the OPMA module is properly configured.
2. Enter the Dynamic DNS Settings configuration dialog as shown in **Figure 6 - 30**.
3. Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server

This is the server name where OPMA module registers itself in regular intervals. Currently this is a fixed setting since only dyndns.org is supported for now.

Hostname

This is the hostname of the OPMA module that is provided by the Dynamic DNS Server. (use the whole name including the domain, e.g. testserver.dyndns.org, not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The OPMA module card registers itself in the Dynamic DNS server at this time.

Check interval

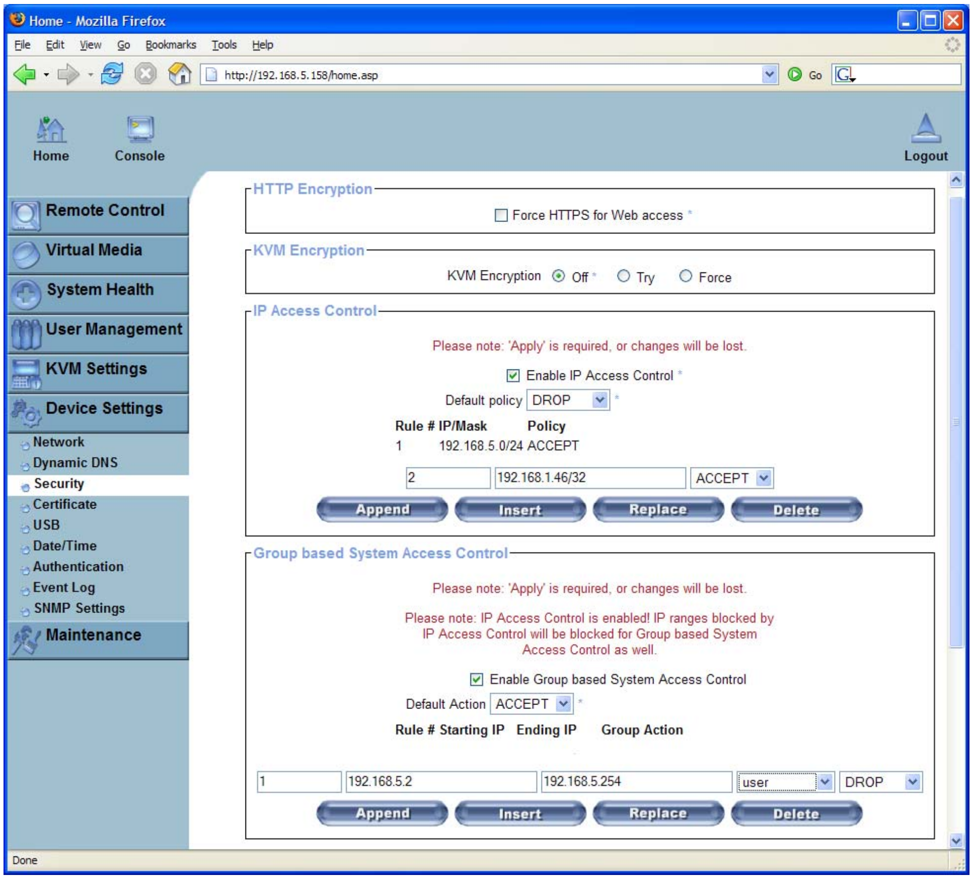
This is the interval for reporting again to the Dynamic DNS server by the OPMA module.

Warning: The OPMA module has its own independent real time clock. Make sure the time setting of the OPMA module is correct (see the Section called Date And Time).

The option **Delete saved external IP** is useful if you would like to update your IP address saved externally. To delete the saved address press the **Delete** button.

Security

Figure 6 - 32. Device Security



HTTP Encryption

□ Force HTTPS for Web access *

KVM Encryption

KVM Encryption ● Off * ○ Try ○ Force

IP Access Control

Please note: 'Apply' is required, or changes will be lost.

☑ Enable IP Access Control *

Default policy DROP *

Rule #	IP/Mask	Policy
1	192.168.5.0/24	ACCEPT
2	192.168.1.46/32	ACCEPT

Group based System Access Control

Please note: 'Apply' is required, or changes will be lost.

Please note: IP Access Control is enabled! IP ranges blocked by IP Access Control will be blocked for Group based System Access Control as well.

☑ Enable Group based System Access Control

Default Action ACCEPT *

Rule #	Starting IP	Ending IP	Group	Action
1	192.168.5.2	192.168.5.254	user	DROP

HTTP Encryption

If this option is enabled, access to the web front-end is only possible using a HTTPS connection. The OPMA module will not listen on the HTTP port for incoming connections.

In case you want to create your own SSL certificate that is used to identify the OPMA module refer to the Section called **Certificate**.

KVM Encryption

This option controls the encryption of the KVM protocol. This protocol is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host.

If set to **Off** no encryption will be used. If set to **Try** the applet tries to make an encrypted connection. In case that the connection cannot be established an unencrypted connection will be used instead. If set to **Force** the applet tries to make an encrypted connection. An error will be reported in case the connection establishment fails.

IP Access Control

This section contains settings for the OPMA module's built-in firewall. The firewall can be enabled or disabled. When enabled the firewall allows you to explicitly block or allow connections from certain client IP addresses.

If the default policy is set to **DROP**, a list of IP addresses or address ranges can be configured to be exceptionally **ACCEPTed**. When the default policy is set to **ACCEPT**, a list of IP addresses or address ranges can be configured to be exceptionally **DROPped**.

The network or address range has to be configured in CIDR (Classless Inter-Domain Routing) notation, e.g. 192.168.1.0/24. It has to consist of a IP address followed by a slash and the number of relevant bits belonging to the network or address range (counting from the left).

Warning: The IP access control settings apply to the LAN interface only!

Enable IP Access Control

Enables access control based on IP source addresses.

Default policy

This option controls what to do with arriving IP packets that do not match any of the configured rules. They can be accepted or dropped.

Warning: If you set this to "DROP" and you have no "ACCEPT" rules configured, the access to the web front end over LAN is actually impossible! To enable access again you can change the security settings via modem or by temporarily disabling IP access control with the initial configuration procedure (see Table 4 - 1. Initial Network Configuration).

Rule Number

This should contain the number of a rule for which the following commands will apply. In case of appending a new rule, this field will be ignored.

IP/Mask

Specifies the IP address or IP address range for which the rule applies. Examples (the number concatenated to an IP address with a "/" is the number of valid bits that will be used of the given IP address):

`192.168.1.22/32`	Matches the IP Address 192.168.1.22
`192.168.1.0/24`	Matches all IP packets with sources addresses from 192.168.1.0 to 192.168.1.255
`0.0.0.0/0`	Matches any IP packet

Policy

The policy determines what to do with matching packets. They can be either accepted or dropped.

Warning: The order of the rules is important. The rules are checked in ascending order until a rule matches. All the rules below the matching one will be ignored. The default policy applies if no match has been found.

Appending a rule

Enter the IP/Mask and set the policy. Finally, press the **Append** button.

Inserting a rule

Enter the rule number, the IP/Mask and set the policy. Finally, press the **Insert** button.

Replacing a rule

Enter the rule number, the IP/Mask and set the policy. Finally, press the **Replace** button.

Deleting a rule

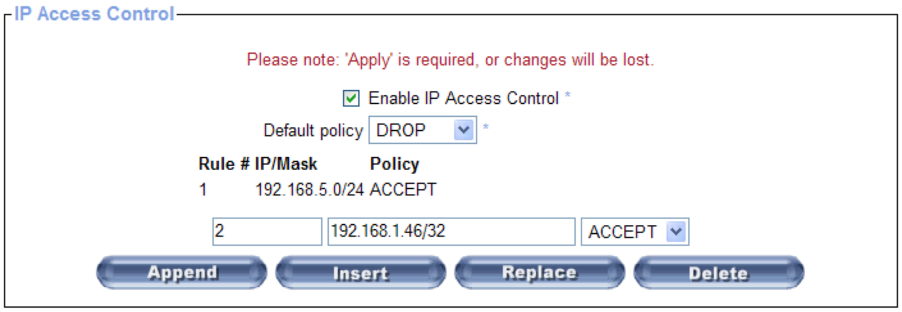
Enter the rule number and press the **Delete** button.

Example of Use:

In the following example (**Figure 6 - 33**) the OPMA module is configured to be inaccessible for all IP addresses, except for the IP addresses which follow the two rules below:

Rule #	IP/Mask	Policy	Effect
1	192.168.5.0/24	ACCEPT	All IP addresses of the Privat Class C (16-bit block) subnet 5 can access the OPMA module.
2	192.168.1.46/32	ACCEPT	Only the host with the IP address "192.168.1.46/32" of the Privat Class C subnet 1 can access the OPMA module.

Figure 6 - 33. Example of Use for IP Access Control



IP Access Control

Please note: 'Apply' is required, or changes will be lost.

☑ Enable IP Access Control *

Default policy DROP *

Rule #	IP/Mask	Policy
1	192.168.5.0/24	ACCEPT
2	192.168.1.46/32	ACCEPT

Group Based System Access Control

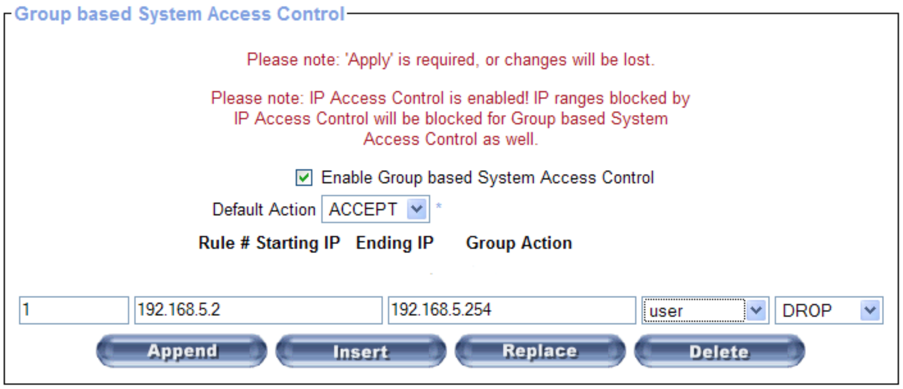
This is similar to the option above, except that you can specify a group of IP addresses and not a network with a network mask.

Example of Use:

In the following example (**Figure 6 - 34**) the OPMA module is configured to be accessible for all IP addresses which passed the IP Access Control rules, except for users with an IP addresse which follow the rule below:

Rule #	Starting IP	Ending IP	Group	Action	Effect
1	192.168.5.2	192.168.5.254	Admin	Drop	All users of the group “Admin” with IP addresses of the Privat Class C (16-bit block) subnet 5 can not access the OPMA module. Only the “Admin” with the IP 192.168.5.1 can login on the OPMA module. Additional to the one admin all other user groups which pass the IP Access Control rules can access the device.

Figure 6 - 34. Example of Use for the Group based System Access Control



Group based System Access Control

Please note: 'Apply' is required, or changes will be lost.

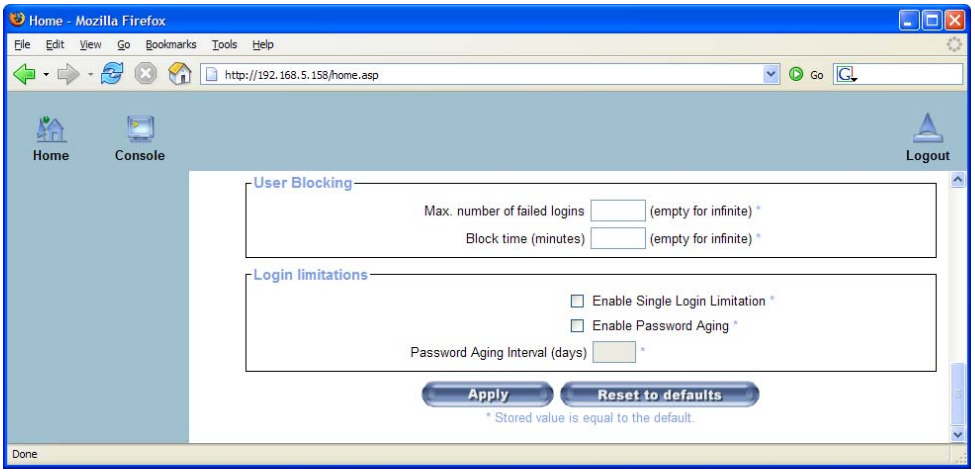
Please note: IP Access Control is enabled! IP ranges blocked by IP Access Control will be blocked for Group based System Access Control as well.

☑ Enable Group based System Access Control

Default Action ACCEPT *

Rule #	Starting IP	Ending IP	Group	Action
1	192.168.5.2	192.168.5.254	user	DROP

Figure 6 - 35. Device Security (Part 2)


Home - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.5.158/home.asp
Go
Home
Console
Logout
Apply
Reset to defaults
Done

User Blocking

Max. number of failed logins [ ] (empty for infinite) *

Block time (minutes) [ ] (empty for infinite) *

Login limitations

□ Enable Single Login Limitation *

□ Enable Password Aging *

Password Aging Interval (days) [ ] *

* Stored value is equal to the default.

User Blocking

When someone attempts to login to the OPMA module device and fails, you can specify how many failed login attempts the OPMA module should tolerate before waiting for the specified number of "Block Time" minutes before it allows further logins. This is useful for blocking automated hacking and cracking attempts.

Maximum number of failed logins

> Enter the maximum number of failed login attempts after which it should not be possible for this user to login anymore. Leave this field empty to disable the user blocking feature.

Block time

> The number of minutes the user is blocked after he exceeded his maximum number of failed login attempts. Leave this field empty to block him for an infinite amount of time until he is manually unblocked again.

Unblocking Users

There are two possibilties to unblock a blocked user.

- A parent user may go to the user management settings (see the Section called **User Management)** and press the **Unblock** button for the user.
- It is also possible to use the serial console for the initial configuration (see **Table 4 - 1. Initial Network Configuration**) and login as the user “unblock”. The OPMA module will ask for the superuser password and present a list of blocked users which may be unblocked.

Login Limitations

Single Loging Limitation

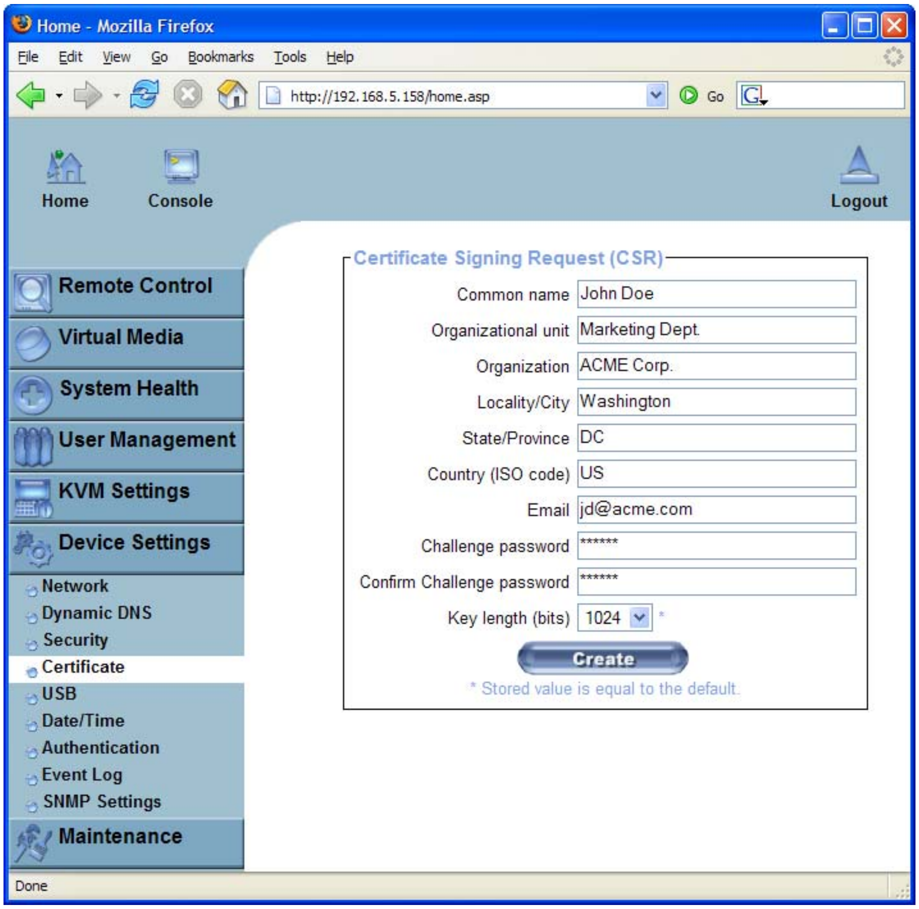
If this option is enabled, the user can access the OPMA module only from one IP adress with one connection. It is not possible to access the OPMA module from different IP addresses or web browsers with the same login at the same time. You have to be logged out or the session has to be timed out to get a new connection on a different IP address on the OPMA module with this login.

Password Aging

If this option is enabled after a defined interval a reminder will request a new password for the user. The set interval displays how many days the password is active.

Certificate

Figure 6 - 36. Certificate Settings



Certificate Signing Request (CSR)

Common name	John Doe
Organizational unit	Marketing Dept.
Organization	ACME Corp.
Locality/City	Washington
State/Province	DC
Country (ISO code)	US
Email	jd@acme.com
Challenge password	******
Confirm Challenge password	******
Key length (bits)	1024 *

Create

* Stored value is equal to the default.

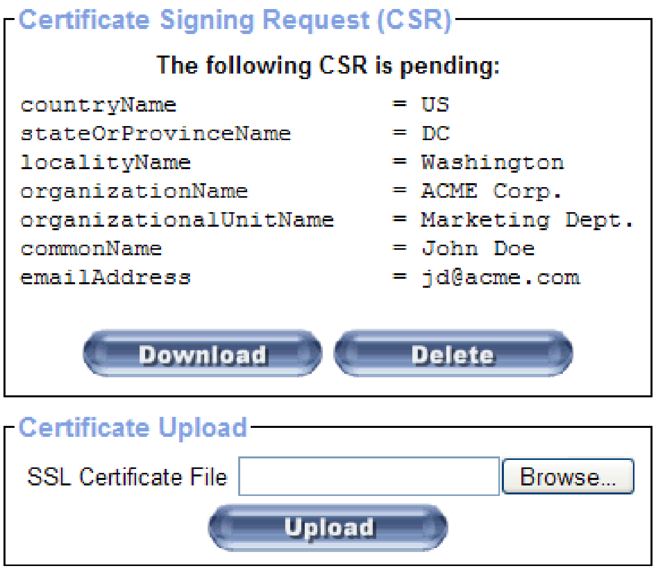
The OPMA module uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the OPMA module has to expose its identity to a client using a cryptographic certificate. Upon delivery this certificate and the underlying secret key is the same for all OPMA module ever produced and certainly will not match the network configuration that will be applied to the OPMA module cards by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

However, it is possible to generate and install a new base64 x.509 certificate that is unique for a particular OPMA module card. In order to do that, the OPMA module is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are and signs and issues a SSL certificate to you.

To create and install a SSL certificate for the OPMA module the following steps are necessary:

1. Create a SSL Certificate Signing Request using the panel shown in **Figure 6 - 36**. You need to fill out a number of fields that are explained below. Once this is done, click on the **Create** button which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download CSR** button (see **Figure 6 - 37**).
2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
3. Upload the certificate to the OPMA module using the **Upload** button as shown in **Figure 6 - 37**.

Figure 6 - 37. SSL Certificate Upload



Certificate Signing Request (CSR)

The following CSR is pending:

```
countryName                  = US
stateOrProvinceName          = DC
localityName                 = Washington
organizationName             = ACME Corp.
organizationalUnitName       = Marketing Dept.
commonName                   = John Doe
emailAddress                 = jd@acme.com
```

After completing these three steps the OPMA module has its own certificate that is used for identifying the card to its clients.

Warning: If you destroy the CSR on the OPMA module there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name

This is the network name of the OPMA module once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the OPMA module with a web browser but without the prefix "http://". In case the name given here and the actual network name differ, the browser will pop up a security warning when the OPMA module is accessed using HTTPS.

Organizational unit

This field is used for specifying to which department within an organization the OPMA module belongs.

Organization

The name of the organization to which the OPMA module belongs.

Locality/City

The city where the organization is located.

State/Province

The state or province where the organization is located.

Country (ISO code)

The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.

Challenge Password

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is four characters.

Confirm Challenge Password

Confirmation of the Challenge Password.

Email

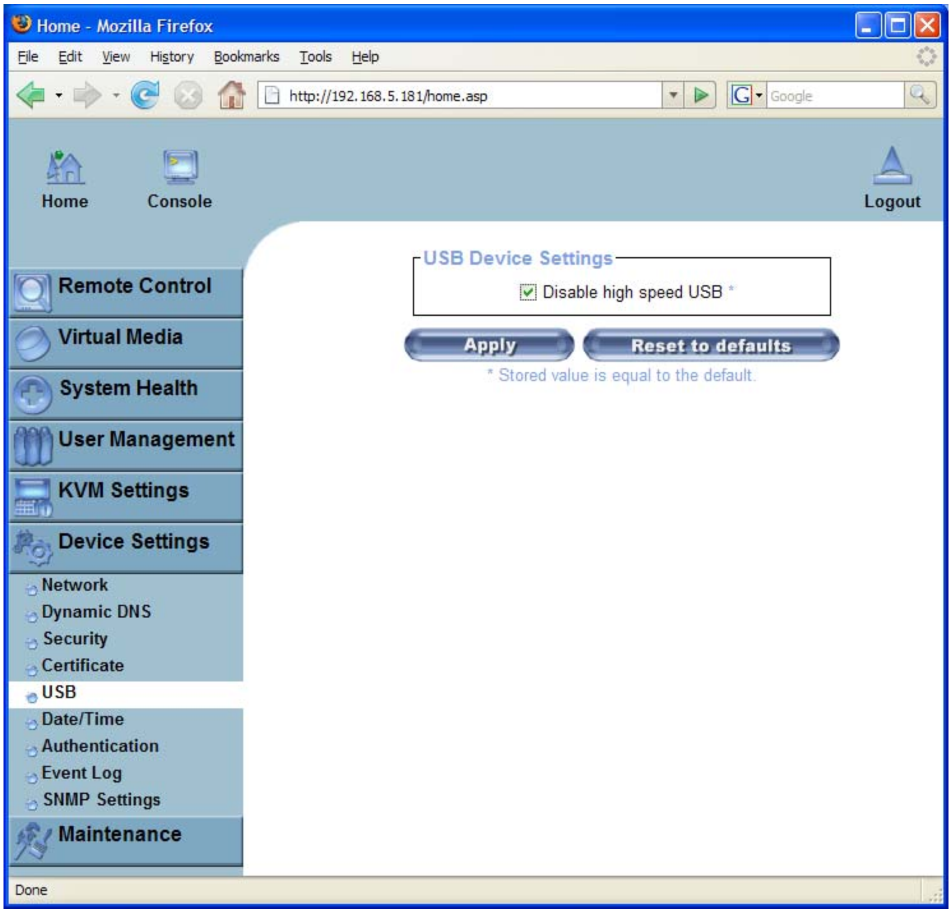
The email address of a contact person that is responsible for the OPMA module and its security.

Key length

This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the OPMA module during connection establishment.

USB

Figure 6 - 38. USB Device Settings



USB Device Settings

☑ Disable high speed USB *

* Stored value is equal to the default.

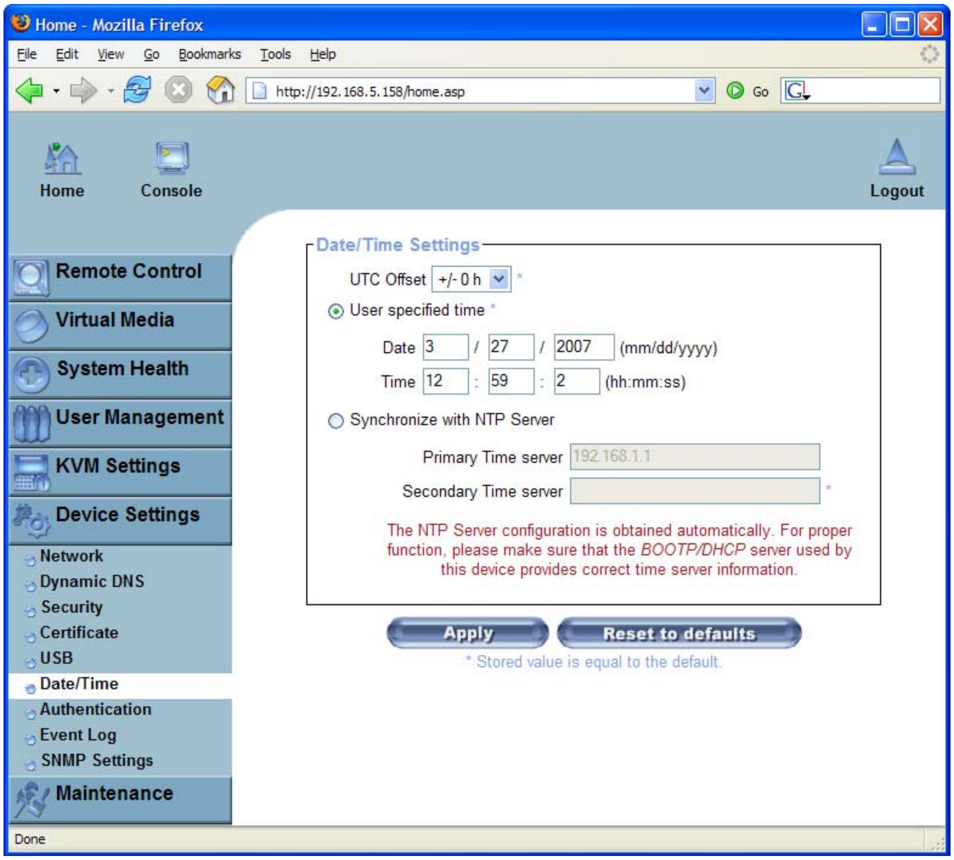
In this section, you can disable the USB high speed mode. This helps solving some compatibility issues with BIOS versions or very old linux versions. However, this reduces the speed of the virtual media emulation.

To set this option press the **Apply** button.

Warning: This feature will not be supported if a KIRA100 R01.x is on the OPMA module.

Date And Time

Figure 6 - 39. Date and Time



Date/Time Settings

UTC Offset +/- 0 h *

● User specified time *

Date 3 / 27 / 2007 (mm/dd/yyyy)

Time 12 : 59 : 2 (hh:mm:ss)

○ Synchronize with NTP Server

Primary Time server 192.168.1.1

Secondary Time server *

The NTP Server configuration is obtained automatically. For proper function, please make sure that the *BOOTP/DHCP* server used by this device provides correct time server information.

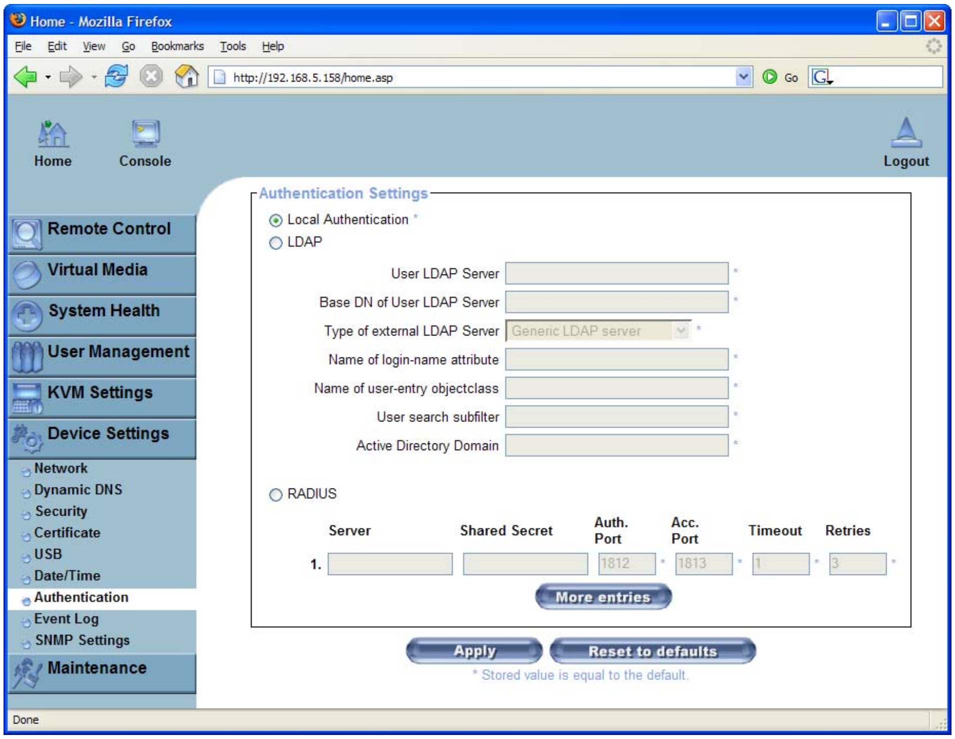
* Stored value is equal to the default.

This link refers to a page where the internal realtime clock of the OPMA module can be set up (see **Figure 6 - 39**). You have the possibility to adjust the clock manually or to use a NTP time server.Without a time server your time setting will not be persistent, so you have to adjust it again after the OPMA module loses power for more than a few minutes. To avoid this you can use a NTP time server which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Warning: There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

Authentication Settings

Figure 6 - 40. LDAP and other Authentication Settings



Authentication Settings

● Local Authentication *

○ LDAP

User LDAP Server *

Base DN of User LDAP Server *

Type of external LDAP Server: Generic LDAP server *

Name of login-name attribute *

Name of user-entry objectclass *

User search subfilter *

Active Directory Domain *

○ RADIUS

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.			1812 *	1813 *	1 *	3 *

More entries

Apply | Reset to defaults

* Stored value is equal to the default.

On this screen you can specify where the OPMA module will look in order to authenticate the users. You can either use "Local Authentication", this means you need to have created the user account on the OPMA module and the user/group information residing on the OPMA module will be used for authentication.

The other options allow you to specify an LDAP or a RADIUS Server to use for the login authentication. These methods are very useful when you want to map users into specific groups which have certain privileges. It is usually far easier and simpler to refer to a lready existing groups, rather than having to re-enter everything into the OPMA module.

Note: *Whatever you configure, you can always login over the network as the superuser "admin". The superuser is always authenticated and authorized locally, so you always have a "back door" to the OPMA module.*

LDAP Access

The OPMA module uses LDAP only for authentication (password verification). User privileges and private settings are still stored locally at the OPMA. That’s why, a user account has to be created on the OPMA module before this user can login via LDAP. Also, all privilege configurations have to be done within the OPMA user management (see the Section called **User Management**).

In order to configure the LDAP access, you can set the following options:

User LDAP Server

Here you enter the name or IP address of the LDAP server containing all the user entries. If you choose a name instead of an IP address you need to configure a DNS server in the network settings. E.g.: 192.168.1.250

Base DN of User LDAP Server

Here you specify the distinguished name (DN) where the directory tree starts in the user LDAP server. E.g.: dc=test,dc=domain,dc=com

Type of external LDAP Server

With this option you set the type of the external LDAP server. This is necessary since some server types require special handling. Additionally, the default values for the LDAP scheme are set appropriately. You can choose between a Generic LDAP Server, a Novell Directory Service and a Microsoft Active Directory. If you have neither a Novell Directory Service nor a Microsoft Active Directory then choose a Generic LDAP Server and edit the LDAP scheme used (see below).

Name of login-name attribute

This is the name of the attribute containing the unique login name of a user. To use the default leave this field empty. The default depends on the selected LDAP server type.

Name of user-entry object class

This is the object class that identifies a user in the LDAP directory. To use the default leave this field empty. The default depends on the selected LDAP server type.

User search subfilter

Here you can refine the search for users that should be known to the OPMA module.

Active Directory Domain

This option represents the active directory domain that is configured in the Microsoft Active Directory server. This option is only valid if you have chosen a Microsoft Active Directory as the LDAP server type. E.g.: test.domain.com

Using the RADIUS Server

RADIUS (Remote Authentication Dial In User Service) is a protocol specified by the Internet Engineering Task Force (IETF) working group. There are two specifications that make up the RADIUS protocol suite: Authentication and Accounting. These specifications aim to centralize authentication, configuration and accounting for dial-in services to an independent server. The RADIUS protocol exists in several implementations such as freeRADIUS, openRADIUS or RADIUS on UNIX systems. The RADIUS protocol itself is well specified and tested. We can give a recommendation for all products listed above, especially for the freeRADIUS implementation.

For detailed information on how to setup the RADIUS server, please refer to **Appendix D. Configuring the RADIUS Server**.

Note: *Currently, we do not support challenge/response. An Access Challenge response is seen and evaluated as an Access Reject.*

To access a remote device using the RADIUS protocol you have to login, first. You are asked to specify your user name and password, then. The RADIUS server reads your input data (Authentication) and the OPMA looks for your profile (Authorization). The profile defines (or limits) your actions and may differ depending on your specific situation. If there is no such profile your access via RADIUS will be refused. In terms of the remote activity mechanism the login via RADIUS works similar to the Remote Console. If there is no activity for half an hour your connection to the OPMA module will be aborted and closed.

Server

Enter either the IP address or the hostname of the RADIUS Server to connect to. For the hostname DNS has to be configured and enabled.

Shared Secret

A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the OPMA module serves as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (message integrity). For the shared secret you can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z,a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation mark (!) or an asterisk (*).

Authentication Port

The port the RADIUS server listens for authentication requests. The default value is #1812.

Accounting Port

The port the RADIUS server listens for accounting requests. The default value is #1813.

Timeout

Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the request. If the request job is not completed within this interval of time it is cancelled. The default value is 1 second.

Retries

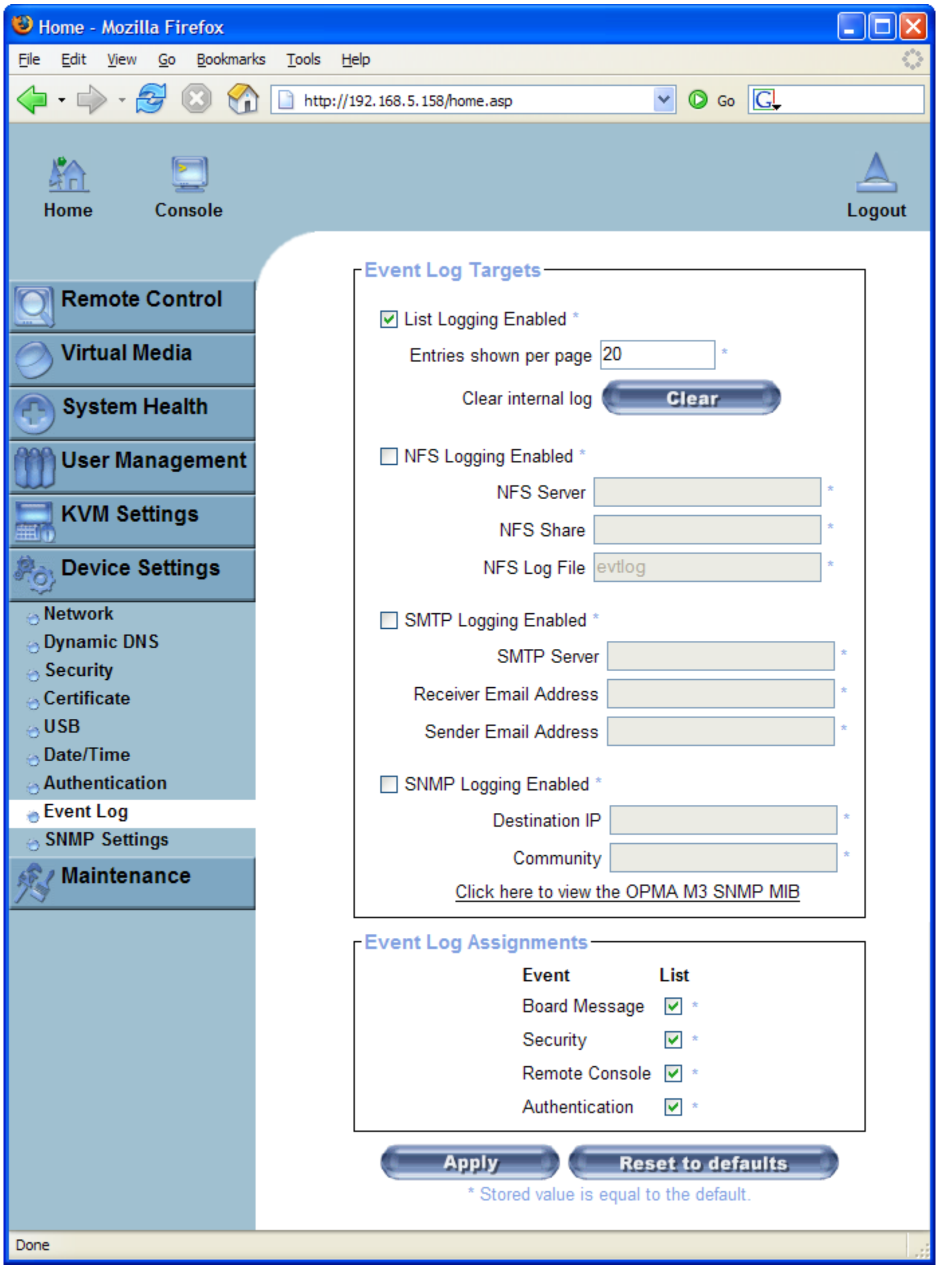
Sets the number of retries if a request could not be completed. The default value is 3 times.

Global Authentication Type

Sets the authentication protocol. This can be the unencrypted PAP (Password Authentication Protocol) or the encrypted CHAP (Challenge Handshake Authentication Protocol).

Event Log

Figure 6 - 41. Event Log



Event Log Targets

☑ List Logging Enabled *

Entries shown per page: 20 *

Clear internal log: Clear

□ NFS Logging Enabled *

NFS Server: *

NFS Share: *

NFS Log File: evtlog *

□ SMTP Logging Enabled *

SMTP Server: *

Receiver Email Address: *

Sender Email Address: *

□ SNMP Logging Enabled *

Destination IP: *

Community: *

Click here to view the OPMA M3 SNMP MIB

Event Log Assignments

Event	List
Board Message	☑ *
Security	☑ *
Remote Console	☑ *
Authentication	☑ *

* Stored value is equal to the default.

Important events like a login failure or a firmware update are logged to a selection of logging destinations (see **Figure 6 - 41**). Each of those events belong to an event group which can be activated separately. For a detailed specification of the existing event groups and the log events belonging to them, use the "help" link in the HTML frontend.

The common way to log events is to use the internal log list of the OPMA module. To show the log list click on the item **Event Log** from the section "Maintenance". In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

Event Log Targets

List logging enabled

To log events you may use the internal log list of the OPMA module. To show the log list click on "Event Log" on the "Maintenance" page.

Since the OPMA module’s system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one automatically.

Warning: If the Reset button on the HTML frontend is used to restart the OPMA module, all logging information is saved permanently and is available after the OPMA module has been started. If the OPMA module loses power or a hard reset is performed, all logging data will be lost. To avoid this use one of the log methods described below.

NFS Logging enabled

Define a NFS server where a directory or a static link has to be exported to, in order to write all logging data to a file that is located there. To write logging data from more than one OPMA module devices to only one NFS share, you have to define a file name that is unique for each device.When you change the NFS settings and press the **Apply** button, the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an error message.

Warning: In contrast to the internal log file on the OPMA module, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

SMTP Logging enabled

With this option the OPMA module is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server that has to be reachable from the OPMA module device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the OPMA module sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps any SNMP trap listener may be used.

Event Log Assignments

You may choose which actions of the OPMA module will be saved in the log file. Tick the desired box(es) and click **Apply** to confirm your selection.

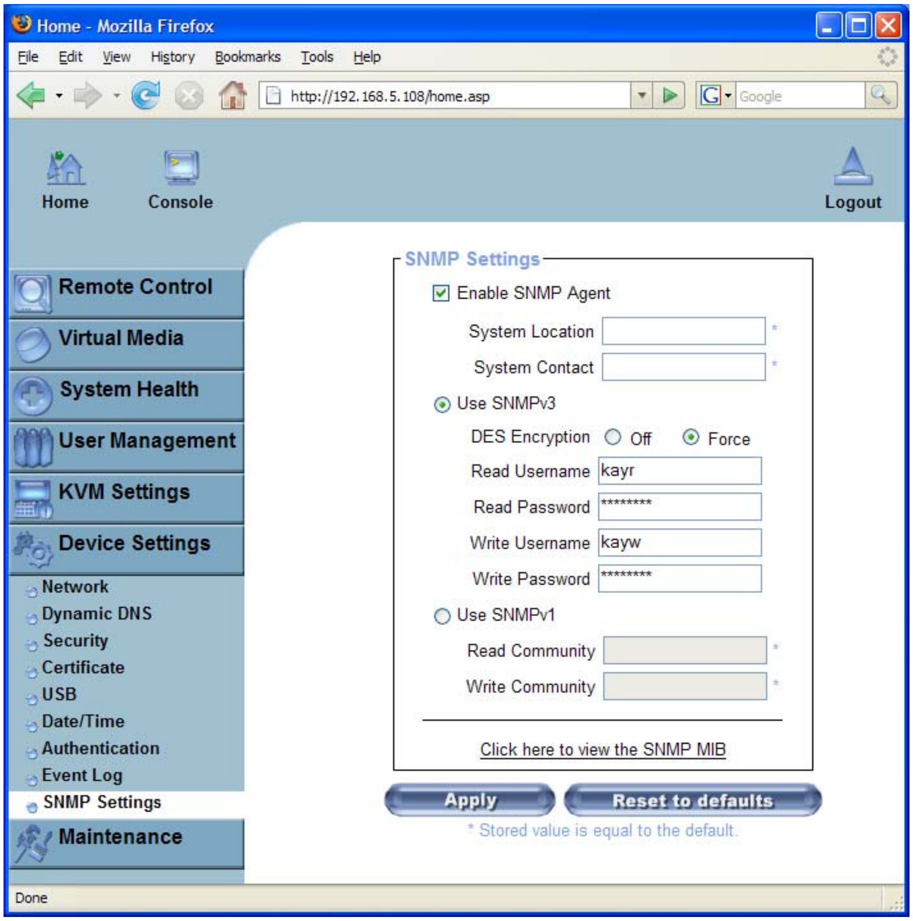
The OPMA module knows the in **Table 6 - 1** listed events. All supported events will be devided into the following groups: Board Message, Security, Remote Console and Authentication.

Table 6 - 1. Event Log Assignments

Event	Group
`Device succesfully started`	Board Message
`Board Reset performed by user…`	Board Message
`Firmware upload failed.`	Board Message
`No firmware file uploaded.`	Board Message
`Uploaded firmware file discarded.`	Board Message
`Firmware validation failed.`	Board Message
`Firmware file uploaded by user…`	Board Message
`Firmware updated by user…`	Board Message
`Internal log file cleared by user…`	Board Message
`Security Violation`	Security
`Connection to Remote Console failed: <reason.>`	Remote Console
`Connection to client ... established.`	Remote Console
`Connection to client ... closed.`	Remote Console
`Login failed.`	Authentication
`Login succeed.`	Authentication
`Login failed.`	Authentication
`Login succeed.`	Authentication

SNMP

Figure 6 - 42. SNMP Settings



SNMP Settings

☑ Enable SNMP Agent

System Location *

System Contact *

● Use SNMPv3

DES Encryption ○ Off ● Force

Read Username kayr

Read Password ********

Write Username kayw

Write Password ********

○ Use SNMPv1

Read Community *

Write Community *

Click here to view the SNMP MIB

* Stored value is equal to the default.

The following information is available via SNMP:

- Serial number
- Firmware version
- MAC address / IP address / Netmask / Gateway of LAN interface
- Server’s power state
- Server’s POST code

The following actions can be initiated via SNMP:

- Reset server
- Power on/off server
- Reset the OPMA module

The following events are reported by the OPMA module via SNMP:

- Login trial at the OPMA module failed.
- Login trial at the OPMA module succeeded.
- Denying access to a particular action.
- Server was reset.
- Server was powered on/off.

The SNMP settings panel as shown in **Figure 6 - 42** are described below, allows you to change SNMP related parameters.

Enable SNMP Agent
If this option is checked, the OPMA module will reply to SNMP requests.

Hint: *If a community is left blank, you cannot perform the according request. E.g. if you want to disable the possibility to reset the OPMA module via SNMP then do not set a write community.*

System Location
Enter a description of the physical location of the host. The description will be used in reply to the SNMP request “ sysLocation.0 ”.

System Contact
Enter a contact person for the host. The value will be used in reply to the SNMP request “ sysContact.0 ”.

Use SNMPv3

The SNMPv3 functionality offers a higher security by DES encrypting of the datas and user authentification.

DES Encryption
This option activates (Force) or deactivates (Off) the DES encryption.

Read Username
The name of the read community user.

Read Password
Insert the password for the read community user.

Write Username
The name of the write community user.

Write Password

Insert the password for the write community user.

Use SNMPv1

Hereby will the datas retrieved without encryption.

Read Community

This is the SNMP community, which allows you to retrieve information via SNMP.

Write Community

This community allows you to set options and to reset the OPMA module or the host via SNMP, i.e. all that affects the host or the OPMA module.

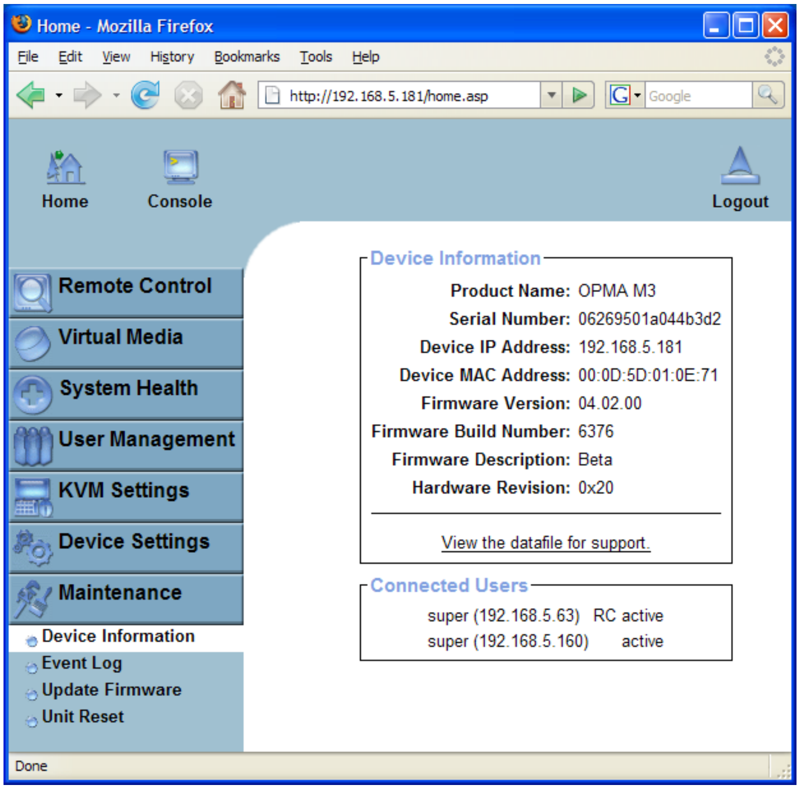
The OPMA module SNMP MIB

This link allows you to download the OPMA module SNMP MIB file. This file may be necessary for an SNMP client to communicate with the OPMA module.

Maintenance

Device Information

Figure 6 - 43. Device Information



Device Information

Product Name:	OPMA M3
Serial Number:	06269501a044b3d2
Device IP Address:	192.168.5.181
Device MAC Address:	00:0D:5D:01:0E:71
Firmware Version:	04.02.00
Firmware Build Number:	6376
Firmware Description:	Beta
Hardware Revision:	0x20

View the datafile for support.

Connected Users

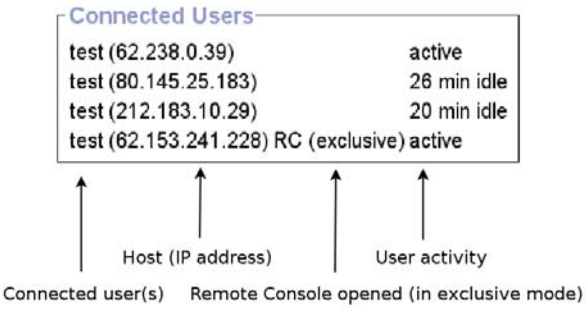
super (192.168.5.63) RC active
super (192.168.5.160) active

This section contains a summary with various information about this OPMA module and its current firmware and allows you to reset the card. You may have a look at **Figure 6 - 43** for an example.

The Data file for support allows you to download the OPMA module data file with specific support information. This is an XML file with certain customized support information like the serial number etc.

You may send us this information together with a support request. It will help us to locate and solve your reported problem.

Figure 6 - 44. Connected Users



Connected Users

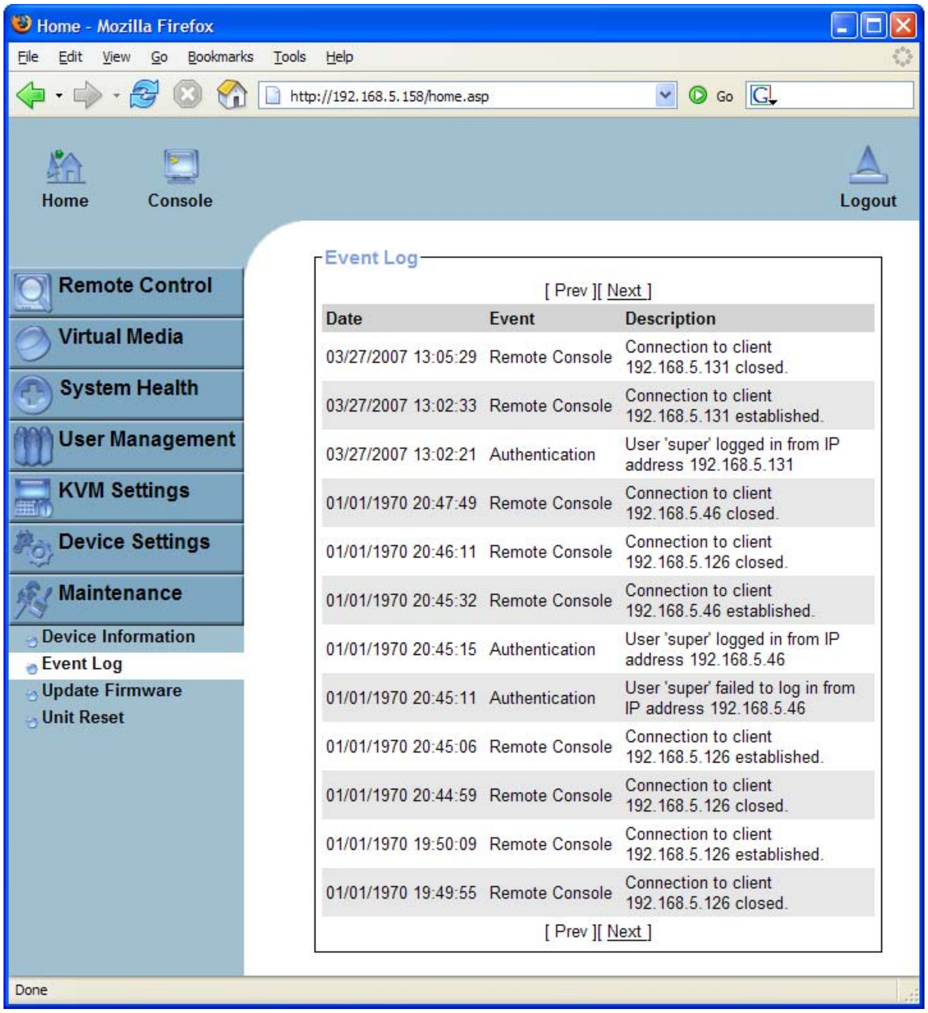
test (62.238.0.39) active
test (80.145.25.183) 26 min idle
test (212.183.10.29) 20 min idle
test (62.153.241.228) RC (exclusive) active

Figure 6 - 44 displays the OPMA module activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. "RC" indicates that the Remote Console is open. If the Remote Console is opened in "exclusive mode" the term "(exclusive)" is added. For more information about this option see the Section called **Remote Console Control Bar** in Chapter 5.

To display the user activity the last column is used. It contains either the term "active" for an active user or the according idle time for an inactive user.

Event Log

Figure 6 - 45. Event Log List



Event Log

[Prev][Next]

Date	Event	Description
03/27/2007 13:05:29	Remote Console	Connection to client 192.168.5.131 closed.
03/27/2007 13:02:33	Remote Console	Connection to client 192.168.5.131 established.
03/27/2007 13:02:21	Authentication	User 'super' logged in from IP address 192.168.5.131
01/01/1970 20:47:49	Remote Console	Connection to client 192.168.5.46 closed.
01/01/1970 20:46:11	Remote Console	Connection to client 192.168.5.126 closed.
01/01/1970 20:45:32	Remote Console	Connection to client 192.168.5.46 established.
01/01/1970 20:45:15	Authentication	User 'super' logged in from IP address 192.168.5.46
01/01/1970 20:45:11	Authentication	User 'super' failed to log in from IP address 192.168.5.46
01/01/1970 20:45:06	Remote Console	Connection to client 192.168.5.126 established.
01/01/1970 20:44:59	Remote Console	Connection to client 192.168.5.126 closed.
01/01/1970 19:50:09	Remote Console	Connection to client 192.168.5.126 established.
01/01/1970 19:49:55	Remote Console	Connection to client 192.168.5.126 closed.

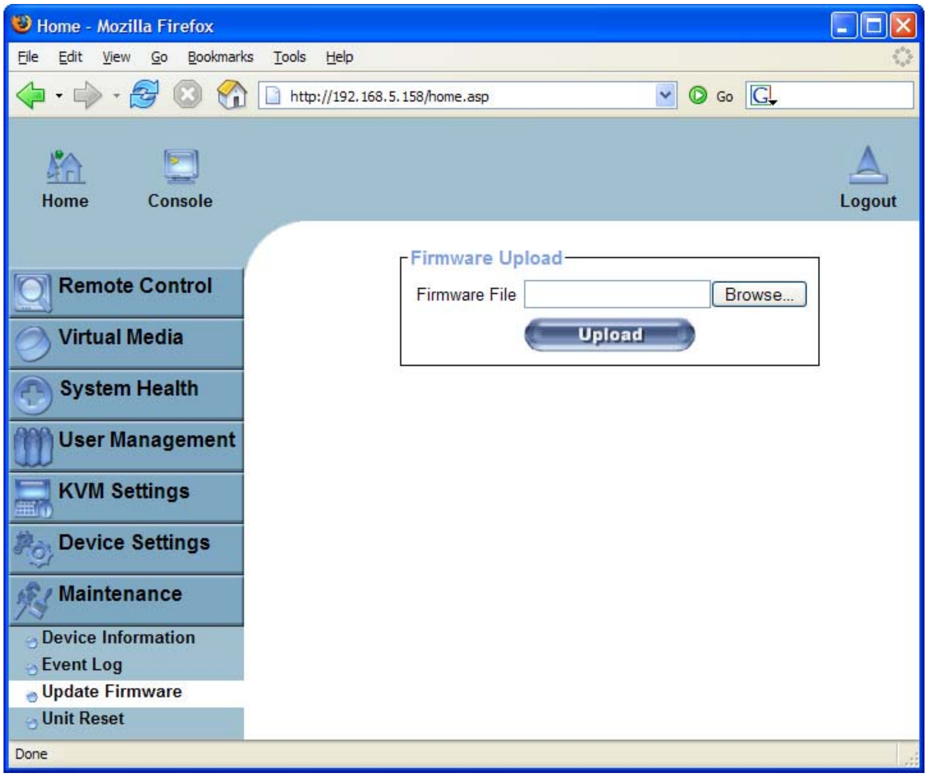
[Prev][Next]

Figure 6 - 45 displays the Event Log list. It includes the events that are kept by the OPMA module extended by the event date, a short event description and an IP address the request was sent from.

You may use the text buttons **Prev** and **Next** to browse within the data. The **Prev** button displays the previous page with newer log information whereas the **Next** button switches to the following page with older log information.

Update Firmware

Figure 6 - 46. Update Firmware



The OPMA module is a complete standalone computer. The software it runs is called the firmware. The firmware of the OPMA module can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email or you can download it from the Raritan Web Site. If the firmware file is a compressed file with suffix .zip you have to unzip it before you can proceed. In order to extract the archive you may use WinZip from http://www.winzip.com/ (for Windows OS) or a tool named unzip that might be already provided in your OS (UNIX, Linux, OS X).

Before you can start updating the firmware of your OPMA module the new and uncompressed firmware file has to be accessible on the system that you use for connecting to the OPMA module.

Updating the firmware is a three-stage process:

- Firstly, the new firmware file is uploaded onto the OPMA module. In order to do that you need to select the file on your local system using the **Browse** button of the Upload Firmware panel (see **Figure 6 - 46**). Then, click **Upload** to transfer the previously selected file from your local file system onto the OPMA module. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted and the current firmware is kept as is.

- Secondly, if everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware.

- Pressing the **Update** button will store the new version and substitute the old one completely.

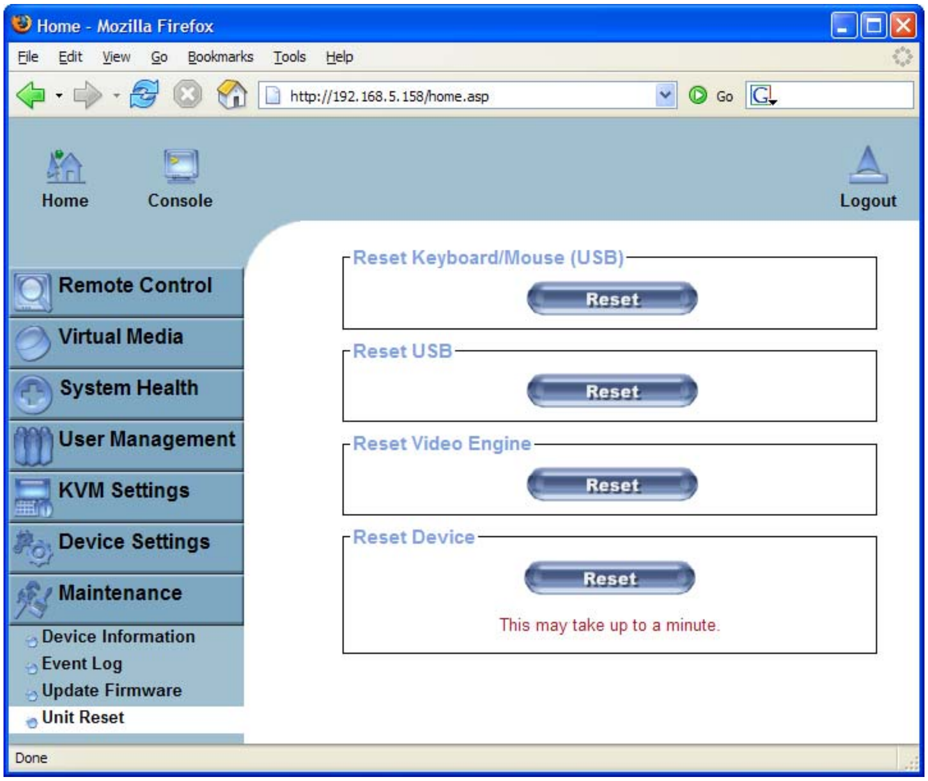
Warning: This process is not reversible and might take some minutes. Make sure the OPMA module's power supply will not be interrupted during the update process, because this may cause an unusable device.

- Thirdly, after the firmware has been stored, the OPMA module will reset automatically. After about one minute you will be redirected to the Login page and requested to login once again.

Warning: The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the OPMA module's power supply will not be interrupted!

Unit Reset

Figure 6 - 47. Unit Reset



http://192.168.5.158/home.asp

This may take up to a minute.

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the OPMA module itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole process will take about half a minute. Resetting subdevices (e.g. video engine) will take some seconds only and does not result in closing connections.

To reset a certain OPMA module functionality click on the **Reset** button as displayed in **Figure 6 - 47**.

Note: Only the user "admin" is allowed to reset the OPMA module.

Appendix A: Troubleshooting

1. **The mouse does not react correctly in the applet screen. The mouse is not in sync with the mouse of the host.**
   Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If resynchronizing fails, disable the mouse acceleration and repeat the procedure.

2. **I have a crazy mouse.**
   Verify your mouse settings. Disable the mouse acceleration. For instance in Windows 2000 this can be done in ’Settings -> System control -> Mouse’. Make sure that your mouse settings match your mouse model, i.e. PS/2 or wheel mouse.

3. **Login to the OPMA module fails.**
   Verify both your user login and your password. By default, the user "super" has the password "pass" . Moreover, your web browser has to be configured to accept cookies.

4. **The Remote Console window of the OPMA module does not open.**
   A firewall may prevent the access to the Remote Console. The TCP ports #80 (for HTTP) and #443 (for both HTTPS and RFB) have to be open (the server providing the firewall has to accept incoming TCP connections on these ports).

5. **Remote console is unable to connect and displays a timeout error.**
   Have a look on your hardware. If there is a proxy server between the OPMA module and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the OPMA module and the client.
   Furthermore, check the settings of the OPMA module and choose a different server port used for RFB transfer. If you use a firewall then check the according port for accepting connections. You may restrict these connections for the IP addresses used by the OPMA module and your client.

6. **No connection can be established to the OPMA module.**
   Have a look on your hardware. Is the OPMA module attached to a power supply? Verify your network configuration (IP address, router). You may send a "ping" request to the OPMA module to find out whether the OPMA module is reachable via network.

7. **Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.**
   You have to define a so-called "Button Key". This can be done in the Remote Console settings (see the Section called **Remote Console Control Bar** in Chapter 5). Alternatively you can use the soft keyboard feature (see the Section called **Soft Keyboard** in Chapter 5).

8. **The OPMA module web pages are not displayed correctly.**
   Check your browser’s cache settings. Make sure the cache settings are not set to something like "never check for newer pages". Otherwise the OPMA module pages may be loaded from your browser cache and not from the card.

9. **Windows XP does not awake from standby mode.**
   This is possibly a Windows XP problem. Try not to move the mouse pointer while XP switches into standby mode.

10. **For SUN computers a USB keyboard does not work.**
The OPMA module emulates a USB keyboard. If you attach a USB keyboard to your host two keyboards are detected. It cannot be predicted which one of these comes first and you will be able to work with.
SUN supports only one USB keyboard.

11. **Cannot upload the signed certificate in MacOS X.**
If an "internal error" occurs while uploading the signed certificate either change the extension of the file to `.txt` or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to "plain text" and the checkbox "use for outgoing" is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).

12. **Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore.**
Disable the setting "Automatically move mouse pointer to the default button of dialog boxes" in the mouse settings of your operating system.

13. **The Remote Console does not open with Opera in Linux.**
Some versions of Opera do not grant enough permissions if the signature of the applet cannot be verified.
To solve the problem, add the lines

```
grant codeBase "nn.pp.rc.RemoteConsoleApplet" {
permission java.lang.RuntimePermission
"accessClassInPackage.sun.*";
```

to the java policy file of opera (e.g. `/usr/share/opera/java/opera.policy`).

14. **The video data on the local monitor is surrounded by a black border.**
This is not a failure. The local monitor is programmed to a fixed video mode that can be selected in the video settings of the OPMA module. Refer to the Section called **Remote Console Control Bar** in Chapter 5 for further planation.

15. **The local monitor displays video data but the remote screen remains blank.**
If the Remote Console is connected (look at the status line of the Remote Console) you should verify that the flat panel interface is not switched off by the video driver of your operating system.

16. **I forgot my password. How can I reset the OPMA module to factory defaults?**
You may use the serial interface or the reset pins . For a detailed description see the Section called **Resetting the OPMA module to its Factory Settings** in Chapter 4.

Appendix B. Glossary

ACPI

Advanced Configuration and Power Interface
A specification that enables the operating system to implement power management and system configuration.

ATX

Advanced Technology Extended
A specification that covers the style of motherboards and enclosures introduced by Intel in 1995.

DHCP

Dynamic Host Configuration Protocol
A protocol for dynamically assigning IP addresses to host names, especially used in a local network.

DNS

Domain Name System
A protocol used to locate computers on the Internet by their name.

FAQ

Frequently Asked Questions

HTTP

Hypertext Transfer Protocol
One of the protocols used for communication between single computers, especially between web browsers and web servers.

HTTPS

Hypertext Transfer Protocol Secure
The secure version of HTTP.

IPMI

Intelligent Platform Management Interface
A specification defining a set of common interfaces for operating system independent platform management and health monitoring.

LED

Light Emitting Diode
A semiconductor device that emits incoherent monochromatic light when electrically biased in the forward direction.

PS/2

Personal System/2
IBM's second generation of personal computers, which was released to the public in 1987. Today, PS/2 is known as a device interface for mouse and keyboard.

SNMP

Simple Network Management Protocol
A widely used network monitoring and control protocol.

SSH

Secure Shell
An encrypted network protocol providing a secure replacement for Telnet.

SSL

Secure Socket Layer
An encryption technology for the Internet used to provide secured data transmissions.

SVGA

Super Video Graphics Array
A refinement of the Video Graphics Array (VGA) that provides increased pitch and resolution performance.

UTP

Unshielded Twisted Pair
A cable with two conductors twisted as a pair and bundled within the same outer PVC covering.

Appendix C. KiraTool Commands

Supported Operating Systems

- Windows (2000 or newer)
- EFI Shell
- Linux
- DOS

Supported Interfaces

- Remote: LAN (only Windows and Linux version)
- Local: - SCSI over USB
  - SMI (KCS)

Supported Functionality

- Network configuration (IP/mask/gw/MAC)
- Changing admin's name & password
- Showing serial number
- Resetting to factory defaults
- Firmware information and upgrade
- Device self-test

Usage

```
kiratool [options]  [cmd args]
```

Table C - 1. Options Overview

Options	
`-l <ip>`	use remote LAN interface instead of local one
`-s`	use IPMI-over-SCSI interface
`-d <device>`	use specified SCSI device; default: auto-detect
`-u <username>`	user name for login
`-p <password>`	password for login
`-P`	prompt for password
`-f`	force: never prompt for user confirmation
`-v`	verbose: does additional logging
`-c`	calm: does not print out anything (silent)
`-h / -?`	help: shows help and usage information

Note: If no interface is given, local interface is used

Table C - 2. Commands Overview

Commands	
`ver`	shows version of kiratool
`info`	shows vendor and device ID of the connected device
`ipsrc set static | dhcp | bios`	sets IP address source
`ipsrc [show]`	shows current IP address source
`ip set <ip addr>`	sets IP address (e.g. 192.169.1.123)
`ip [show]`	shows current IP address
`netmask set <netmask>`	sets netmask (e.g. 255.255.255.0)
`netmask [show]`	shows current netmask
`gw set <gw addr>`	sets gateway address (e.g. 192.169.1.1)
`gw [show]`	shows current gateway address
`mac set <mac addr>`	sets MAC address (e.g. "FE:00:00:12:34:56" or "FE0000123456")
`mac [show] [-c]`	shows current MAC address (-c = compact mode, e.g. "87654321DCBA" instead of "87:65:43:21:DC:BA")
`fw upgrade [-h] [-o] <fw bin file>`	upgrades firmware (-h = cross-hwid, -o = cross-oem)
`fw validate [-h] [-o] <fw bin file>`	checks firmware compatibility (-h = cross-hwid, -o = cross-oem)
`fw [ver]`	shows firmware version information
`serial [show]`	shows device's serial number
`defaults`	resets all settings to factory defaults
`reset`	hard-resets the module
`admin name <name>`	changes new admin name
`admin passwd <passwd>`	changes admin's password
`admin [show]`	shows admin's name
`raw <hex bytes>`	send raw command and prints raw response (<netfn> <cmd> [<d1>] [<d2>] ... [<dN>]: e.g. 06 01)
`test <test>`	performs module self test and shows results (return value is ==0 on success and =0 in failure)

Commands

`device`	tests whether the device is vailable at all
`video <subtest>`	tests video interface (DVO/DVI)
`status`	checks detected video signal and resolution
`crc`	calculate CRC sum over the captured screen
`ddc <subtest>`	tests DDC interface
`info`	queries EDID information from the device and compares it to the EDID information known by the OS (only available under Windows)
`ipmb <subtest>`	tests IPMB interface
`bmc`	test whether a BMC responds over IPMB
`fml <subtest>`	tests FML interface
`esb2`	test whether an ESB2 is responding on FML when TPT (TCP Pass-Through) is active
`usb [-c <channel>] <subtest>`	tests USB interface
`status`	test whether the device's USB modul is enumerated
`nic [-c <channel>] <subtest>`	test NIC interface
`status`	test NIC status and parameters
`loopback`	test NIC loopback functionality
`ping <host>`	Test whether pinging a host works
`broadcast`	Broadcast ping (not yet implemented)
`all`	performs all tests and subtests one after another
`-s <test to skip>`	Single tests can be skipped using the -s parameter. You can both skip a whole component (e.g. -s ddc) and skip a single test (e.g. -s video crc) Included tests: • ddc info • video status • ipmb bmc • fml esb2 • usb status • nic status

Return Code

To let the caller know whether an error occured and what went wrong, the tool returns a return code:

- If everything went well, 0 is returned
- For all commands except test, -1 is returned if an error occurs
- If a test fails, the return code indicated which test failed:

Table C - 3. Return Codes Overview

Test	Return Code
device	1
video status	2
video crc	3
ddc info	4
ipmb ddc	5
fml esb2	6
usb status	7
nic status	8
nic loopback	9
nic ping	10
nic broadcast	11

- if test all fails, the return code of the first error which occured is returned; the test will not be stopped after the first error!

Appendix D. Configuring the RADIUS Server

This appendix describes the necessary steps to configure a RADIUS server in order to be able to use remote authentication on the OPMA module. This is shown for a Windows 2003 Server Standard Edition system with Active Directory enabled.

Prerequisites

1. Please check if Active Directory is enabled. If not, got to Start -> Run and type "dcpromo" to enable Active Directory function. Follow the instructions to enable AD.
2. Make sure Internet Authentication Service is installed, enabled and registered to Active Directory.
    - To install Internet Authentication Service (IAS), go to **Start -> Control Panel -> Add or Remove Programs -> Add/Remove Windows Components**. Select **Networking Services** by double click on it. Tick **Internet Authentication Service** and then click **OK**. Then Click **Next** to install IAS.
    - To register IAS to Active Directory, go to **Start -> Administrative Tools -> Internet Authentication Service**. Then right click on **Internet Authentication Service (Local)**, select **Register Server in Active Directory**.
3. Create a Windows user group which will hold all users that are allowed to login on the OPMA module. You can allow/deny login for a user just by adding/removing him/her to/from this group. For this group there will be a custom remote access policy configured later on.

   Groups can be maintained by the Active Directory Users and Groups tool: **Start -> Administrative Tools -> Active Directory Users and Computers -> Users**.
4. Create all users to be authenticated from OPMA module. Make sure **Remote Access Permission (Dial-in or VPN)** access is set to **Allow access** where default is **Deny access.** To check, double click on user an select the **Dial-in** tabulator.

   Make all users member of the above group.

Add and configure a RADIUS client

This step is necessary to give the RADIUS server some information about the client (OPMA module) and define a password phrase.

Go to **Start -> Administrator Tools -> Internet Authentication Service**. Right click on **RADIUS Clients** and select **New RADIUS Client**.

Type a friendly name for this client. In this example, "OPMA at Server3" is used. And type the IP address of the OPMA module that will be used as RADIUS client. In this example "192.168.1.198" is used. Select **Next** after this is done.

Type the share secret that will be used between this RADIUS server and OPMA module.

Note: please keep this secret in mind, this same secret will be asked to key in during configuration of RADIUS function on OPMA module.

Select **Finish** after this is done.

A new RADIUS client will now be shown on the display window.

Setup a custom remote access policy

This step explicitly allows the group configured above to login remotely.

Go to **Start -> Administrator Tools -> Internet Authentication Service**. Right click on **Remote Access Policies** and select **New Remote Access Policy**.

Select **Next** to get on the **Policy Configuration Method** page. Switch to **Set up custom policy** and enter a friendly policy name, e.g. "OPMA Access".

Select **Next** to get on the **Policy Conditions** page. Press **Add.**.. to add a new policy. Select **Windows-Groups** and press **Add** to create this condition. Now add the previously created user group by pressing **Add**... and typing the group name in **Enter object name to select**. Leave the sub dialogs and so return to the wizard by pressing **OK** two times.

Select **Next** to get to the **Permissions** page. Select **Grant remote access permission**.

Select **Next** to get to the **Profile** page. Select **Edit Profile**.... Make sure that both **Encrypted authentication (CHAP)** and **Unencrypted authentication (PAP, SPAP)** is enabled. And leave with **OK**.

Select **Next** and **Finish** to complete the wizard.

Appendix E. Key Codes

Fehler! Verweisquelle konnte nicht gefunden werden. shows the key codes used to define the key strokes or hotkeys for several functions. Please note that these key codes do not necessarily represent the key characters that are used on international keyboards. A key on a standard 104 key PC keyboard with a US English language mapping is named. The layout for this keyboard is shown in **Figure E - 1**. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on a similar position, no matter what language mapping you are using. Some of the keys also have aliases. This means that a key can be named by two different key codes.

Figure E - 1. English (US) Keyboard Layout, used for the Key Codes

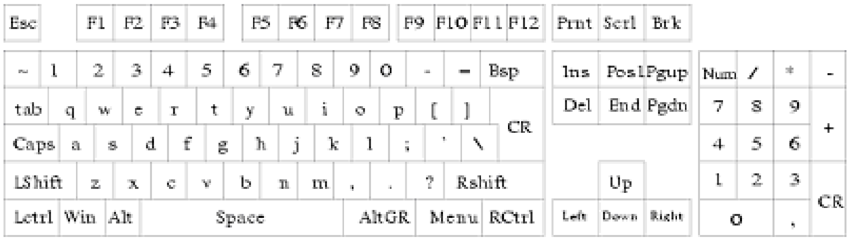

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prnt Scrl Brk
~ 1 2 3 4 5 6 7 8 9 0 - = Bsp Ins Pos1 Pgup Num / * -
tab q w e r t y u i o p [ ] Del End Pgdn 7 8 9 +
Caps a s d f g h j k l ; ' \ CR 4 5 6
LShift z x c v b n m , . ? Rshift Up 1 2 3
Lctrl Win Alt Space AltGR Menu RCtrl Left Down Right 0 , CR

Table E - 1. Key Names

Key	Alias Key(s)
0 - 9	
A - Z	
~	TILDE
_	MINUS
=	EQUALS
;	
´	
<	LESS
,	
.	
/	SLASH
Backspace	
TAB	
[	
]	
ENTER	
CAPS LOCK	
\	BACK SLASH
LSHIFT	SHIFT
RCTRL	CTRL, STRG
RSHIFT	SHIFT
LCTRL	CTRL, STRG
LALT	ALT
SPACE	

Key	Alias Key(s)
ALT Gr	
ESCAPE	ESC
F1	
F2	
F3	
F4	
F5	
F6	
F7	
F8	
F9	
F10	
F11	
F12	
PRINTSCREEN	
SCROLL LOCK	
BREAK	
INSERT	
HOME	POS 1
PAGE_UP	
PAGE_DOWN	
DELETE	DEL
END	
UP	
LEFT	
DOWN	
RIGHT	
NUM_LOCK	
NUMPAD0	
NUMPAD1	
NUMPAD2	
NUMPAD3	
NUMPAD4	
NUMPAD5	
NUMPAD6	
NUMPAD7	
NUMPAD8	
NUMPAD9	
NUMPADPLUS	NUMPAD_PLUS, +
NUMPAD /	/
NUMPADMUL	NUMPAD_MUL, *
NUMPADMINUS	NUMPAD_MINUS, -
NUMPADENTER	
WINDOWS	
MENU	

Appendix F. Pin Assignment

OPMA Connector

The “Open Platform Management Architecture Specification” from AMD with a detailed description of the OPMA connector structure can be downloaded from the following Website:

http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8796_12498,00.html?redir=CPPR31.

In Chapter 4 „OPMA Connector Specification and Pin Assignments” all pins are listed and described.

RJ45 Connetcor Ethernet

Figure F - 1. RJ45 Connector

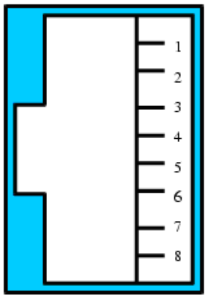


Table F - 1. RJ45

PIN	Assignment	PIN	Assignment
1	TX +	5	Not connected
2	TX -	6	RX -
3	RX +	7	Not connected
4	Not connected	8	Not connected

Serial SUB-D9 Connectors

Figure F - 2. Serial Connector

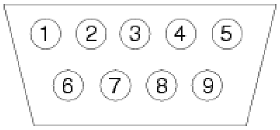


Table F - 2. Serial Sub D9 Connector 1

PIN	Assignment	PIN	Assignment
1	DCD	6	DSR
2	RX	7	RTS
3	TX	8	CTS
4	DTR	9	RI
5	GND		

Table F - 3. Serial Sub D9 Connector 2

PIN	Assignment	PIN	Assignment
1	Not connected	6	Not connected
2	RX	7	Not connected
3	TX	8	Not connected
4	Not connected	9	Not connected
5	GND		

Appendix G. Specifications

Sizes and Weights

Table G - 1. OPMA Specification

Attribute	Value
Height	8.5mm (0.335‘’)
Width	70mm (2.756‘’)
Depth	67.6mmm (2.661’’)
Weight	16g (0.035lb)
Power Consumption	Up to 1A

Environment

Temperature

Table G - 2. Temperature

Attribute	Value
Operating	0°C to 55°C (32°F to 131°F)
Storage	-18°C to 70°C (-0.4°F to 158°F)

Humidity

Table G - 3. Humidity

Attribute	Value
Operating	10% to 90% (non-condensing)
Storage	5% to 95% (non-condensing)

Appendix H. Raritan Inc. Warrenty Information

Limited Warranty

Raritan Inc. manufactures its hardware products from parts and components that are new or equivalent to new in accordance with industry-standard practices. Raritan warrants that the hardware products including the firmware will be free from defects in materials and workmanship under normal use. Any implied warranties on the Raritan firmware and hardware are limited to 24 months, respectively, beginning on the date of invoice. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. Additionally Raritan grants a special warranty for 6 months.

Customer Remedies

Raritan's entire liability and exclusive remedy shall be, at Raritan's option, either (a) return of the price paid, or (b) repair or replacement of the firmware or hardware that does not meet this Limited Warranty and which is returned to Raritan with a copy of your receipt. Damage due to shipping the products to you is covered under this warranty. Otherwise warranty does not cover damage due to external causes, including accident, abuse, misuse, problems with electrical power, servicing not authorized by Raritan , usage not in accordance with product instructions, failure to perform required preventive maintenance and problems caused by use of parts and components not supplied by Raritan . Any replacement hardware will be warranted for the remainder of the original period or thirty (30) days, whichever is longer. Raritan will repair or replace products returned to Raritan's facility. To request warranty service you must inform Raritan within the warranty period. If warranty service is required, Raritan will issue a Return Material Authorization Number. You must ship the products back to Raritan in their original or an equivalent packaging, prepay shipping charges, and insure the shipment or accept the possibility of loss or damage during shipment.

No Other Warranties

To the maximum extend permitted by applicable law, Raritan disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose, with regard to the firmware, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

No Liability For Consequential Damages

To the maximum extent permitted by applicable law, in no event shall Raritan be liable for any damages whatsoever (including without limitation, special, incidental, consequential or indirect damages for personal injury, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Raritan has been advised of the possibility of such damages. In any case, Raritan's entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the firmware and/or hardware. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Appendix I. GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type "show w". This is free software, and you are welcome to redistribute it under certain conditions; type "show c" for details.

The hypothetical commands "show w" and "show c" should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than "show w" and "show c"; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program "Gnomovision" (which makes passes at compilers) written by James Hacker.

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Appendix J. The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.