Raritan ASMI G4 Module User Manual

Raritan ASMI G4 Module User Manual

Table of Contents

List of Tables

Preface

Copyright

Document Version

Version: 1.8

Date: Tuesday, February 27, 2007

Trademarks

Raritan Corp. acknowledges the following trademarks:

- Raritan is a registered trademark of Raritan 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.

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 license. See Appendix G 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 ASMI G4 Module

The ASMI module (ASMI G4) provides remote server management capabilities: you can use the ASMI add-on card to manage and monitor components in your servers. The ASMI 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 ASMI G4 Module, please 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.

Chapter 1. The Quick Start Guide

About the Raritan ASMI G4 Remote Management Card

Figure 1-1. Front View of the ASMI G4 Module

The ASMI G4 add-on card provides remote server management capabilities. You can use the ASMI G4 add-on card to manage and monitor components in your servers through the WAN/LAN. The ASMI G4 add-on card offers a comprehensive hardware solution for server management.

Connecting the ASMI G4 Module to the Host System

> **Warning**
>
> Please note: the firmware of the ASMI G4 board delivered to you is customized for use with the specified motherboard model. Do not use with other motherboards.

Connecting the ASMI G4 module to the Host System is easy: turn off the host, find the correct slot and carefully insert the ASMI G4 module into the slot.

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

Initial Network Configuration

Initially, the ASMI 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	-
Gateway	-

> **Warning**
>
> If the DHCP connection fails on boot up, the ASMI module 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 ASMI add-on card, you could look into the records on the DHCP server.

There are special tools provided by us to ease the configuration and setup of the ASMI board. One of these tools is called *psetup*. This tool will automatically seek out ASMI devices on your local subnet and allow you to set them up.

Web Interface

The ASMI 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 ASMI add-on card into your web browser.

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

Table 1-2. Login Settings

User	Password
super	pass

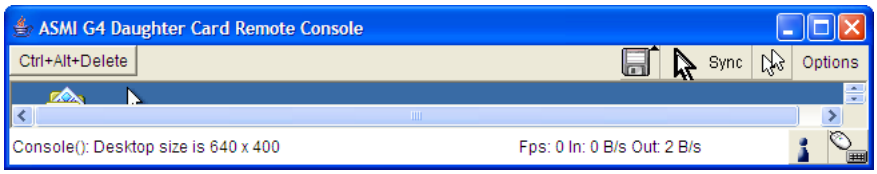
The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system in which the ASMI is installed. The web browser which is used for accessing the ASMI module 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



Generally with modern operating system's mouse devices (usually connected to the USB port) you do not need to worry about the mouse synchronization and similar parameters. This generally applies to all "modern" Windows Operating Systems like Windows 200 and 2003, XP etc. Macintosh OS/X is the same. They use "Absolute Mouse Mode".

Alternatively, there is a so called "Relative Mouse Mode" supported by most Linux and Unix operating systems ("Other Operating Systems"). With this mode, local and remote mouse pointers might get out of sync (i.e. might not point to the same position) when the local mouse or another KVM session has been used at the same time.

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.

Chapter 2. Introduction

General Information

The ASMI module is an integrated solution for your server system.

Based on an embedded operating system, the ASMI G4 add-on card provides both exceptional stability and permanent availability even when your server is down or powered off.

As a system administrator, you can use the ASMI Module to gain location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

Figure 2-1. ASMI G4 Module

Features

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

- ASMI Specification Compliance
- IPMI V2.0 Compliance
- KVM (keyboard, video, mouse) access over TCP/IP networks
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture

- Sophisticated mouse tracking and synchronization
- Local Mouse suppression (only when using SUNs Java Virtual Machine)
- Works independently from the remote host OS. You can access the remote host even in its pre-boot phases like POST and BIOS setup

ASMI add-on Card System Components

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

- The ASMI G4 module
- CD-ROM with documentation: Installation Guide and User Manual
- The Quick Start Guide

When the Server is up and running

The ASMI module 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 remote system (a graceful shutdown)
- Monitor the boot process
- Boot the system from a separate (local) partition to load a 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 ASMI module 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%

Category	Probability
CPU fan failure	8%
RAM failure	4%

Using the ASMI module, 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, main board 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 Intel Corp.

Chapter 3. ASMI Installation Guide

About the ASMI Add-On Card

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

Figure 3-1. ASMI G4 Add-On Module

Connectors

Connecting the ASMI Add-On Card to the Host System

Connecting the ASMI add-on card to the host system is easy: turn off the host, locate the ASMI slot and carefully insert the ASMI add-on card into the slot.

Warning

Please note: the firmware of the ASMI board delivered to you is customized for use with the specified motherboard. Do not use with other motherboards.

Warning

You should turn off the power of the host completely, that includes detaching the power supply cable.

Connecting the Ethernet

The ASMI add-on card has 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 ASMI 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. ASMI G4 Module Configuration

Initial Configuration

The ASMI 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	-
Gateway	-

Warning

If the DHCP connection fails on boot up, the ASMI 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, this chapter describes the initial IP configuration that is necessary to access the ASMI module for the first time.

Using the Psetup Tool

The *psetup* tool is used to determine the IP address assigned to the ASMI by the DHCP server or to change the device's initial network configuration. It allows you to access the ASMI module even when it has no configured IP address.

Psetup can access the ASMI module in two ways:

Locally

Psetup can be invoked directly on the host containing the ASMI module. The *psetup* tool uses USB to connect to the module.

Remotely

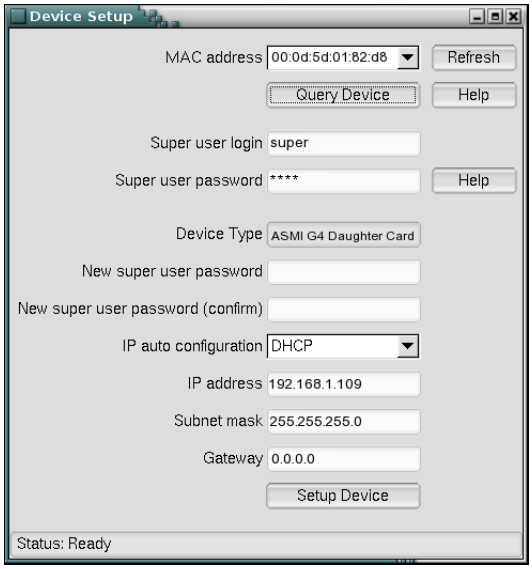
Psetup can be invoked on any host connected to the same subnet (broadcast domain) as the ASMI module. Psetup uses UDP broadcasts to find the module.

Using the Psetup Tool via Graphical User Interface

After invoking *psetup* a window opens as shown in Figure 4-1 (Windows Version) and Figure 4-2 (Linux Version).

Figure 4-1. Psetup Tool (Windows Version)

Figure 4-2. Psetup Tool (Linux Version)



On startup, the *psetup* tool automatically auto-detects all ASMI modules in the local host and on the network subnet. The MAC addresses of all detected modules are available as a drop down list. This list allows you to connect to a specific ASMI module. You can retrigger the auto-detection by hitting "Refresh Devices" or "Refresh".

After selecting a device, the "Device Type" should show "Raritan ASMI G4". You may now query the current network settings of that device using "Query Device".

In order to change the network settings or to assign a new super-user password, you have to authenticate as the super-user. See the Section called *Authentication.*

Running the Linux Psetup Tool via Command Line

The following list shows the command syntax and their usage:

--mac <MAC address of the device>

Shows the current network configuration of the device with the specified MAC (Ethernet) address.

--ip <new IP address>

Set a new IP address.

--ipacp <dhcp|bootp|none>

Set the auto configuration mode to either DHCP or BOOTP. Enter "none" if you want to set the network access parameters manually.

--netmask <net mask>

Set a new netmask.

--gateway <gateway address>

Set a new gateway address.

--login <username>

A valid user name with administration rights is required in order to change the network configuration.

--pw <password>

Password of the user specified in the above --login option.

--pw-new <password>

The user specified with --login gets the new password entered here.

Here is an example of the commands described above and their effects:

Displaying the current network settings

```
test@teststation:~# /home/test/psetup --mac 00:0D:5D:00:65:78
IP auto configuration: dhcp
IP address: 192.168.5.135
Subnet mask: 255.255.255.0
Gateway: 192.168.5.1
```

Changing the network settings

```
test@teststation:~# /home/test/psetup
  --mac 00:0D:5D:00:65:78 --ipacp none --ip 192.168.5.55
  --gateway 192.168.5.1 --netmask 255.255.255.0
  --login super --pw pass
Device configured successfully.
```

MAC Address Detection

Using the Psetup Tool for Windows

The MAC address of the ASMI module is displayed in the top left hand corner. In order to manually detect the MAC address, press "Refresh Devices". The displayed MAC address corresponds to the MAC address printed on the sticker attached to the ASMI module. If this is not the case please contact our Product Support immediately.

The lower right corner of the window shows two buttons: "Query Device" and "Setup Device". Press the "Query Device" button to display the preconfigured values of the network configuration. The values are displayed in the appropriate text fields. If necessary, adjust the network settings to your needs. If you wish to save the changes enter a user name and the proper password, then press the "Setup Device" button.

Using the Linux Psetup Tool

The window the MAC address of the device is displayed in the top edge of the window. In order to manually detect the MAC address, press the button "Refresh". The displayed MAC address corresponds to the MAC address printed on the sticker attached to the ASMI module. If this is not the case please contact our Product Support immediately.

Furthermore, there are two buttons on the window: "Query Device" and "Setup Device". Press the "Query Device" button in order to display the preconfigured values of the network configuration. The values are displayed in the corresponding text fields. If necessary, adjust the network settings to your needs. If you want to save the changes enter a user name and an appropriate password. Press the "Setup Device" button to finish.

Authentication

Enter your login as a super-user and change your password, so you can adjust the authentication settings.

Super-user login

Enter the login name of the super-user. The initial value is "super".

Super-user password

Enter the current password for the super-user. The initial value is "pass".

New super-user password

Enter the new password for the super-user.

New password (confirm)

Re-type the new password for the super-user.

Press the "OK" button to accept the changes and close the window. If you wish to abandon the changes, press the "Cancel" button (on Windows). On a Linux system simply close the window by clicking the required button of the window frame.

Initial Configuration via DHCP Server

By default, the ASMI 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 ASMI module. You can find the MAC address on the outside of the shipping box and labelled on the bottom side.

If this initial configuration does not meet your local requirements, use the setup tool *psetup*to adjust the values to your needs. The *psetup*tool can be found on the CD ROM delivered with this package. You can then employ the procedure described below.

Web Interface

The ASMI module may be accessed using a standard Java enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS to reach the ASMI module. Simply enter the configured IP address of the ASMI module into your web browser.

The initial login settings are:

Table 4-2. Default 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

Three Blind Mice, See How They Run...

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 ASMI module. This is information like: "I am moving to screen co-ordinates X,Y". This mode is very easy to track and most modern Windows versions (XP, 2000, 2003) as well as Mac OS X use it. This mode is also easiest for the ASMI 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.

First and foremost the ASMI module has to know the starting point of the movement (hence you need to press a special "Synchronize" Button, which allows the ASMI module to locate 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 local system/PC you are using to talk to the ASMI module. Hence the ASMI 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 uses this mode.

Remote Mouse Settings

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

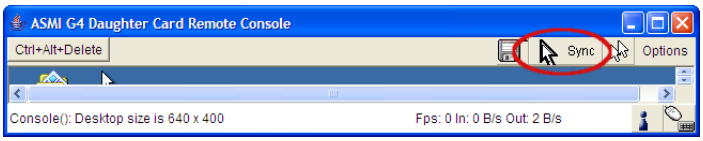
Intelligent Sync

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 longer than the Fast Sync and can be accessed with the appropriate item in the Remote Console Option menu (entry: Mouse Handling).

On top of that please note that 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 almost impossible to find in the transmitted video picture. With the usage of a standard mouse pointer shape the detection is rather simple and the synchronization works best.

Figure 4-3. Remote Console Control Bar: Sync Mouse Button



The "Sync Mouse" button in the Remote Console Tool Bar can behave differently, depending on the current state of the mouse synchronization. Usually pressing this button leads to a Fast Sync, except in situations where the KVM port or the video mode have recently changed. 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.

Note: The following limitations do not apply to USB mice and Mouse Type "MS Windows 2000 and newer" (Absolute Mouse Mode).

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

Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to unsynchronized 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 called "improve mouse acceleration" which has to be deactivated.

Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled, do not use a plain background. Instead use some kind of wallpaper. As an alternative, you can 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 back and forth. This will resynchronize the mouse. If resynchronizing the mouse fails, then 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 ASMI 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

We advise you to use the following mouse settings for different operating systems:

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 "MS Windows 2000 or newer".

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 Mouse Type selection box. Then choose the option Auto Mouse Speed. This applies to both USB and PS/2 mice.

Video Modes

The ASMI module recognizes a 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 ASMI module may not be able to detect them. We recommend using any of the standard VESA video modes instead.

Resetting the ASMI module to its Factory Settings

Using the KiraTool

The ASMI configuration can be reset to factory defaults by using the KiraTool. KiraTool can be used locally on the server hosting the ASMI module or remotely from your admin PC or workstation. E.g. locally:

`kiratool -a -u super -p pass defaults` Remotely: `kiratool -a -l 192.168.1.52 -u super -p pass defaults`

Chapter 5. ASMI Module Usage

Prerequisites

The ASMI module features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe 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 ASMI module environment can be fully managed using a standard web browser. You can access the ASMI module using the insecure HTTP protocol or using the encrypted HTTPS protocol. Whenever possible use the more secure HTTPS.

Telnet

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

SSH

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

The primary interface of the ASMI 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 include a Java Runtime Environment version 1.4 or higher. If the browser has no Java support (for example as found on small handheld devices), you are still able to manage your remote host system using the administration forms displayed by the browser itself.

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

For an insecure connection to the ASMI 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 on Windows 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 old browsers do not offer a strong 128 Bit encryption algorithm. For security reasons you should use a modern browser that supports proper encryption.

Using the Internet Explorer, open the menu entry "?" and "Info" to find out 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

Modern web browsers support strong encryption by default.

Login and Logout to the ASMI Module

Login into the ASMI module

Open your web browser. Type in the address of your ASMI 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 ASMI module a symbolic name in the DNS or another Name Service in your organisation. 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 simply type:

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

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

Figure 5-2. Login screen

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

The ASMI module has a built-in super-user that has all the permissions to administrate your ASMI module. See the following table for the default settings.

Table 5-1. Default User Settings

Parameter	Value
Login	super
Password	pass

Navigation

After a successful login to the ASMI module, the main page of the ASMI module appears (see Figure 5-3). This page consists of three parts, each containing specific information. The buttons on the upper border allow you to navigate inside 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 ASMI module. Within the right frame, task-specific information is displayed that depends on the section you have previously selected.

Figure 5-3. Main Page

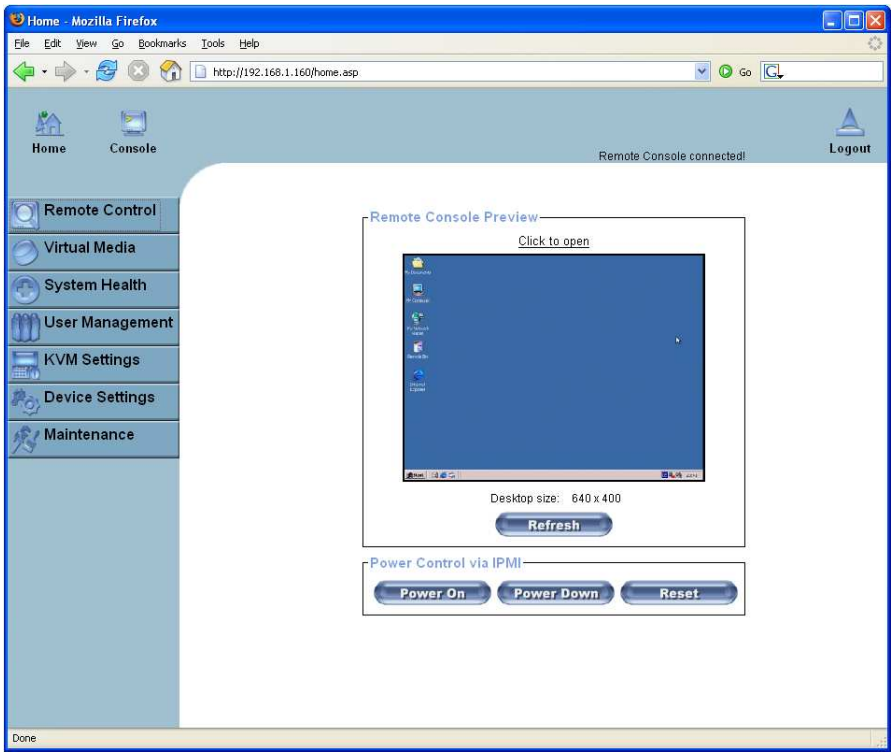


Table 5-2. Front End Buttons

	Return to the main page of the ASMI module.
	Open the ASMI module Remote Console.
	Exit from the ASMI module front end.

Logging out of the ASMI 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.

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

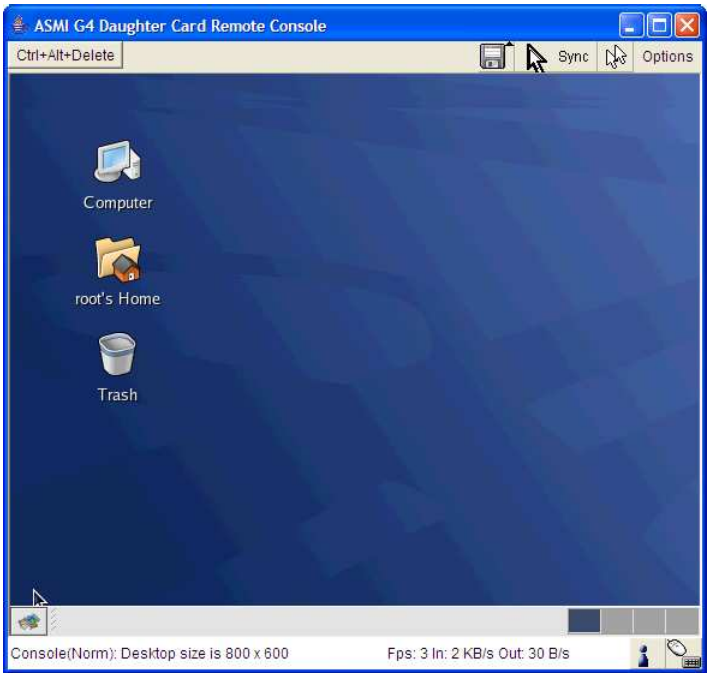
If there is a KVM session active, the Web session will not expire.

The Remote Console

General Description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that is controlled by the ASMI module.

Figure 5-4. Remote Console



The Remote Console window is a Java Applet that tries to establish its own TCP connection to the ASMI module. The protocol that is run over this connection is neither HTTP nor HTTPS, but a special KVM protocol. This protocol uses 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 ASMI 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 a connection. This is because today's web proxies are not capable of relaying this KVM protocol.

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

Main Window

Starting the Remote Console opens an additional window. It displays the screen content of your remote 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 ASMI 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 initially adapt its size to the size of the remote screen 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 possess 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 option follows.

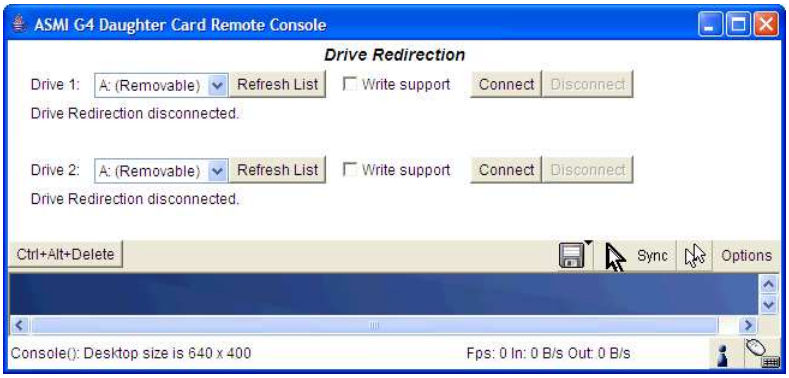
Figure 5-5. Remote Console Control Bar

> **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.

Figure 5-6. Remote Console Applet Drive Redirection Menu



This menu allows you to select a local drive you wish to redirect (only available under Windows):

Figure 5-7. Selecting a Local Drive

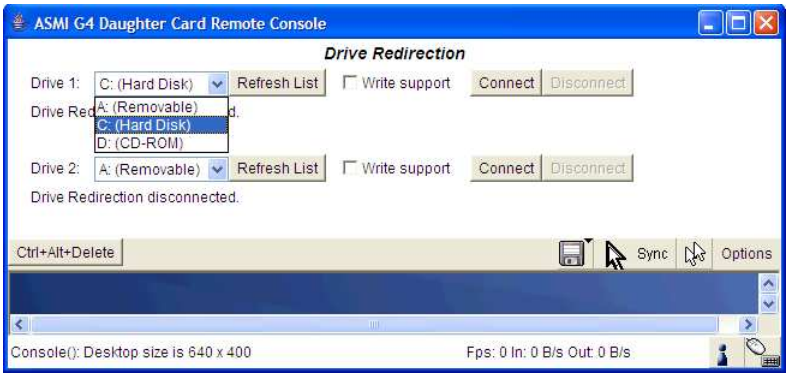
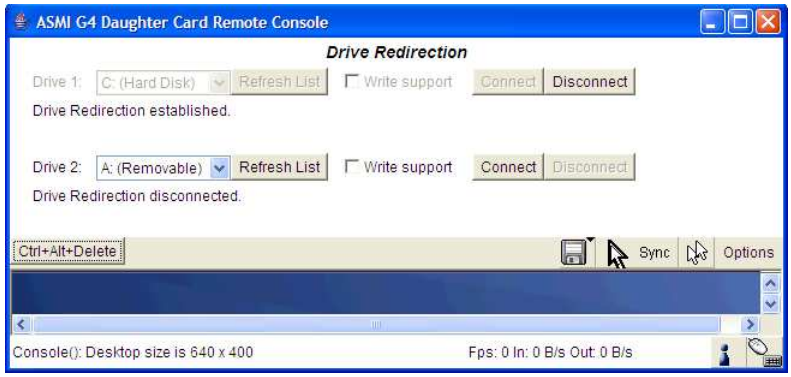


Figure 5-8. Successful Redirection of a Local Drive



This menu shows you an established drive redirection (the second drive is not redirected):

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.

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 synchronized). 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.

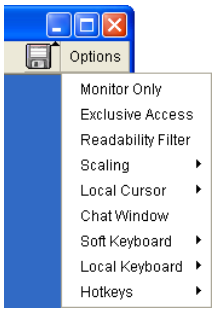
Options 

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

Remote Console Options

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

Figure 5-9. 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. Mouse and keyboard inputs are ignored.

Exclusive Access

If a user has the appropriate permissions he can forcibly close the Remote Consoles of all other users. Noone can then open another Remote Console until this user disables the exclusive access or logs off.

> **Note:** This option is only accessible if the current user privileges allow Exclusive Access.

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 ASMI module will automatically place it onto the "clipboard". This allows you to easily import the screenshot into your documents or other programs.

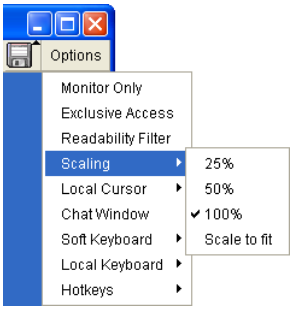
Readability Filter

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 5-10. Remote Console Options Menu: Scaling

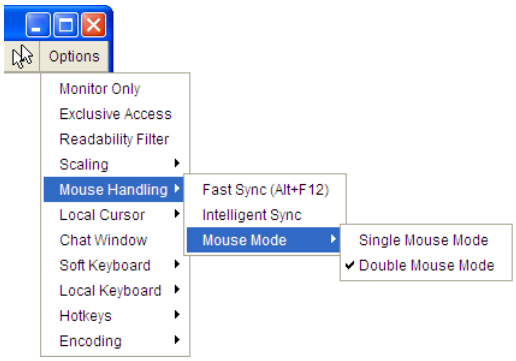


Mouse Handling

Note: This menu is only available when you have selected the option "Other Operating System".

The sub menu 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 5-11. Remote Console Options Menu: Mouse Handling



- Fast Sync

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

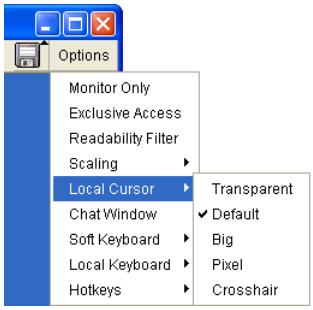
- Intelligent Sync

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

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.

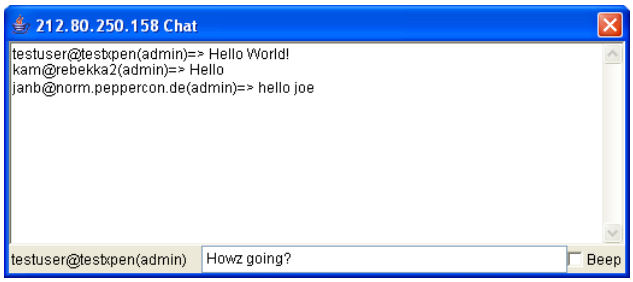
Figure 5-12. Remote Console Options Menu: Cursor



Chat Window

This opens a chat window allowing you to interactively "chat" with other users logged into the ASMI module. This is very useful to tell other users that you are about to terminate their sessions using the Exclusive Access mode.

Figure 5-13. Chat Window



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 appropriate 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 key combinations such as `Ctrl+C` or `AltGr+Shift+F4`.

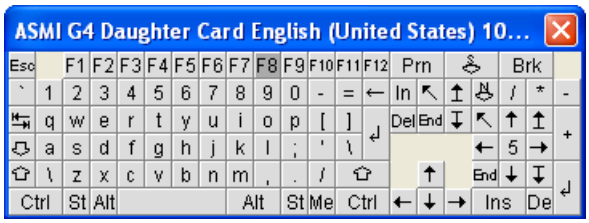
For a single key stroke you can click on the button with the wanted character. Single keys such as regular characters and numbers are sent immediately. Special keys like `Ctrl`, `Shift` as well as the function keys `F1` to `F12` have to be selected twice. The first press sends the signal "key is pressed", 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 czurrently pressed. After the second press the button will revert to its usual look and confirm 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 need 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, click the button `F4` twice. The last press will release all the buttons and send the key combination to the remote system.

Figure 5-14. Soft Keyboard



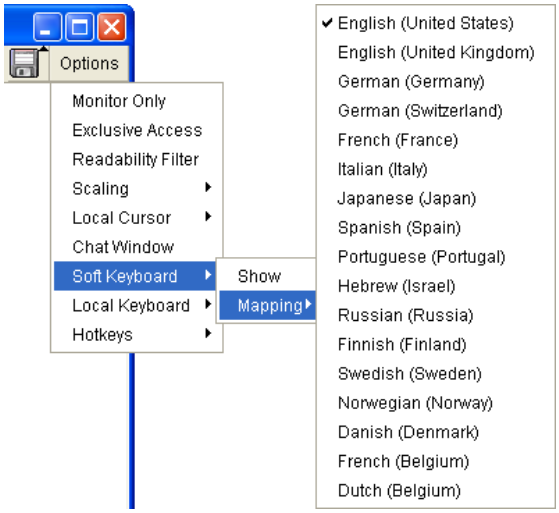
- Show

  Displays the Soft Keyboard.

- Mapping

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

Figure 5-15. 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 for this 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 manually change the Local Keyboard setting to the right language.

Figure 5-16. Local Keyboard

Hotkeys

Opens a list of previously defined hotkeys. In order to send a pre-defined command to the host system simply choose the appropriate entry.

A confirmation dialog 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 5-17. Remote Console Confirmation Dialog

Encoding

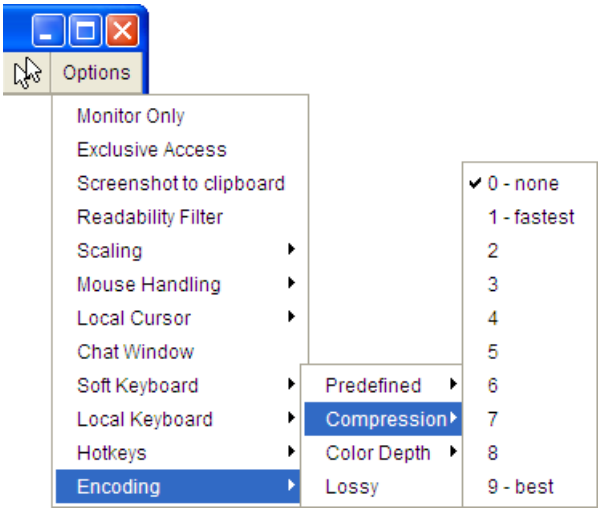
These options are used to adjust the encoding level in terms of compression and color depth. They are only available if "Transmission Encoding" cannot be determined automatically (see the Section called *Transmission Encoding* in Chapter 6).

> **Note:** Please note that these Encoding options are only available if you do not have "Automatic Detection" of the connection quality selected. You need to set a pre-defined level. The relevant menu is "KVM Settings->User Console->Transmission Encoding->Predefined Encoding". This is explained in the following chapter.

- **Compression Level:** you may select a value between 1 and 9 for the desired compression level with level 1 enabling as the fastest compression and level 9 for the best compression. The most suitable compression level should always be seen as a compromise between the network bandwith that is available, for your video picture to be transmitted 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. If the compression level is lower, more data has to be sent and it may take longer to transfer the whole video picture.

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

Figure 5-18. Remote Console Options: 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 5-19. Remote Console Options: Predefined Encoding compression

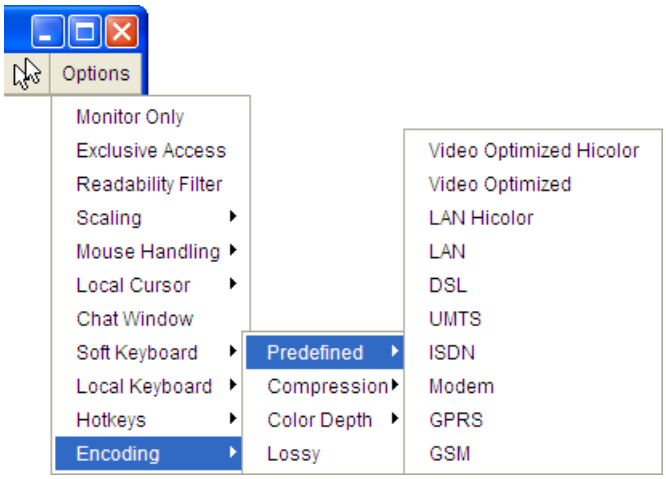
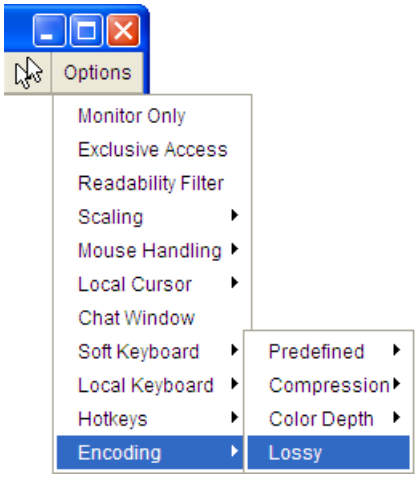
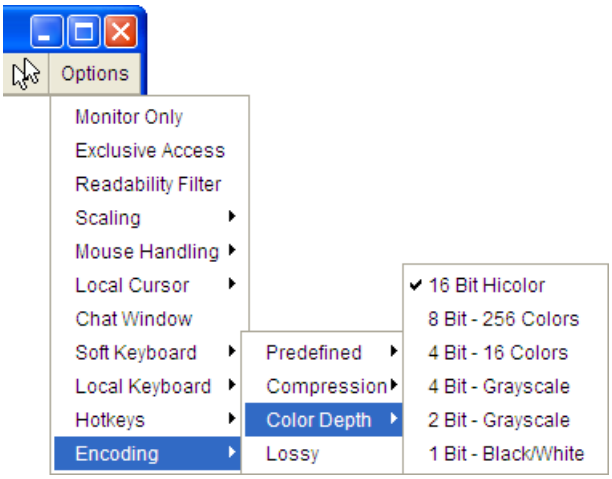


Figure 5-20. Remote Console Options: Lossy Compression



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

Figure 5-21. Remote Console Options: Color Depth



Remote Console Status Line

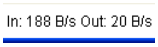
The status line shows both console and the connection state. Figure 5-22 was taken from a Remote Console with a resolution of 800x600 pixels. The value in brackets describes the connection to the

Remote Console. "Norm" means a standard connection without encryption, "SSL" indicates a secure connection using the Secure Socket Layer (SSL).

Figure 5-22. Status line

The status line displays the number of frame buffer updates ("Fps") per second 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, the value in brackets displays the compressed transfer rate.

Figure 5-23. Status line transfer rate



The next button displays the Remote Console Access settings.

Table 5-3. Buttons displaying the access state

	A single user is connected to the Remote Console of the ASMI module.
	One or more users are connected to the Remote Console of the ASMI 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 relevant paragraphs in

the Section called *Remote Console Control Bar*.

Optimizing the Video Picture

The ASMI 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 ASMI module with low bandwidth

The bandwidth of the network connection of the ASMI module is an important influence on the time taken to transmit two consecutive video pictures. A connection with low bandwidth takes longer to transfer the video data from the ASMI module to the Remote Console on the local host. Every time the remote screen has changes requires a new picture to be sent.

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

You can choose a compression level from the sub menu "Compression" in the Options menu of the Remote Console. This reduces the amount of data that has to be transmitted.

Please note that the video data will be compressed on the ASMI module, transmitted to the Remote Console and unpacked in the local Java environment. Depending on the ASMI module and on the local machine this procedure may take some time and may result in slow updates of the picture in the Remote Console.

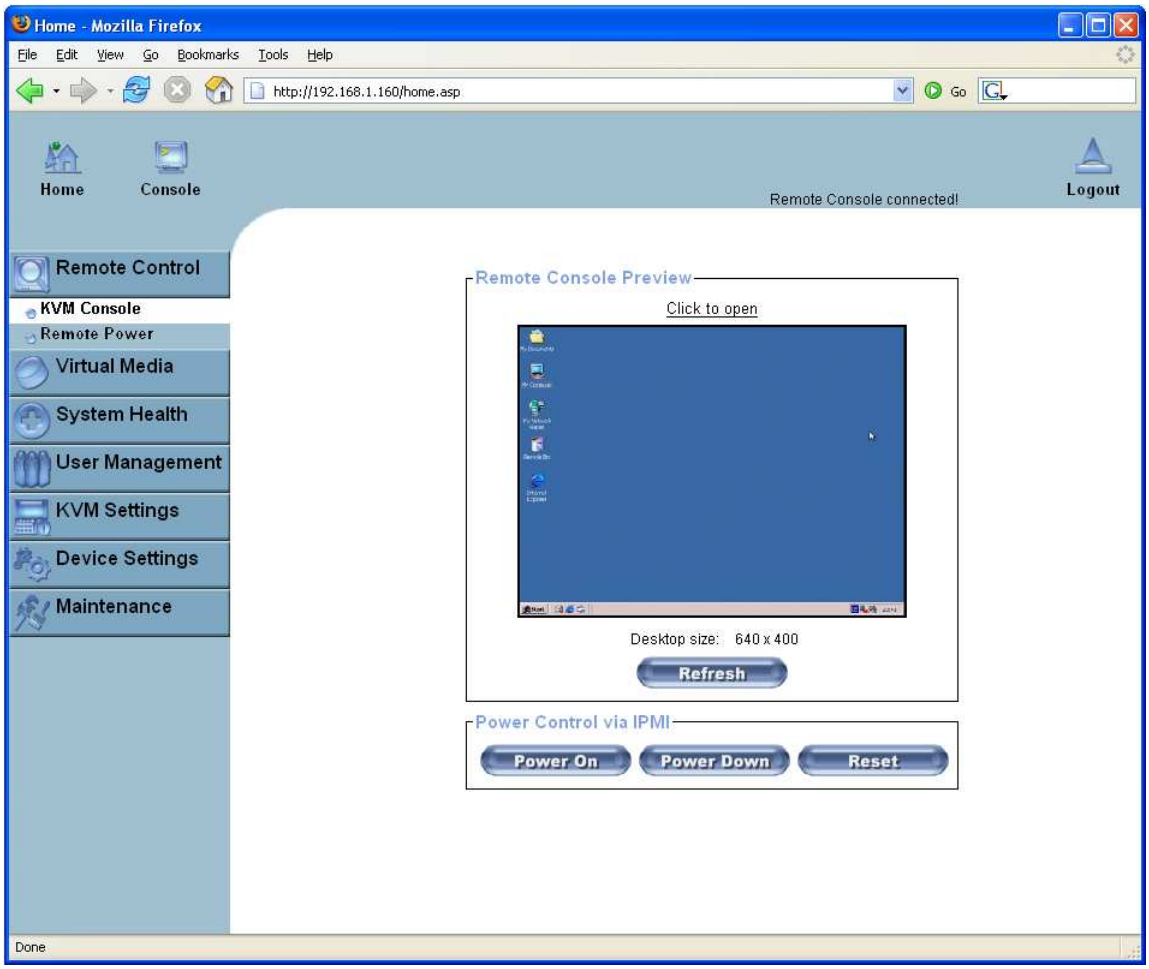
In order to improve the transmission speed you may also reduce the picture quality in the Remote Console to either "8 bit" or even to grayscale. This measure causes less video data to be processed and is likely to be more effective than selecting the highest compression level.

Chapter 6. Menu Options

Remote Control

KVM Console

Figure 6-1. KVM Console

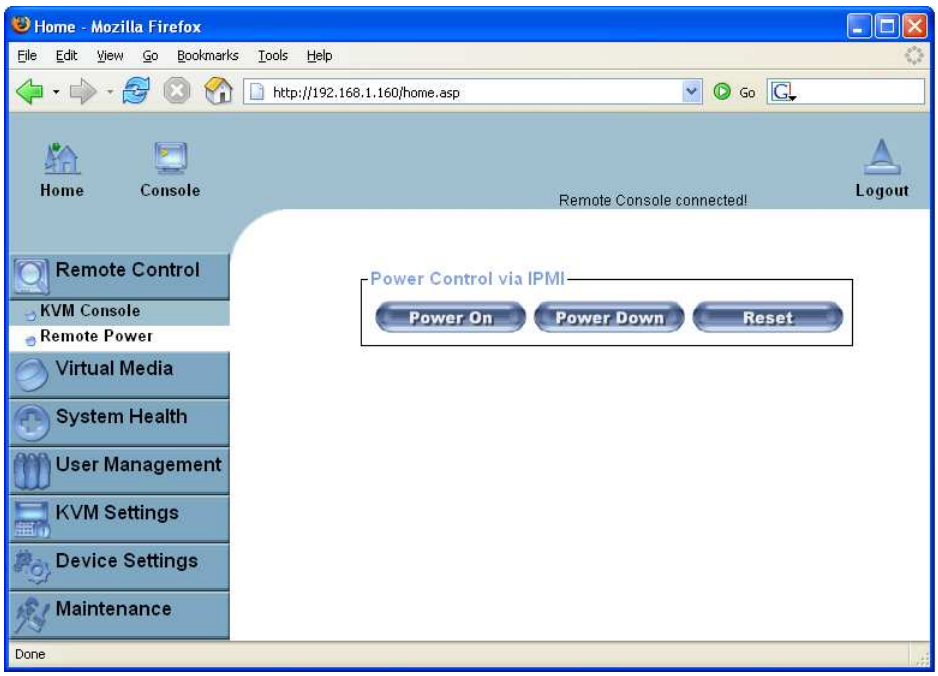


Remote Console Preview

You can open the KVM console by clicking either on the menu entry on the left or on the console picture on the right. If you need to refresh the picture click on the "Refresh" button.

Remote Power

Figure 6-2. Remote Control via IPMI

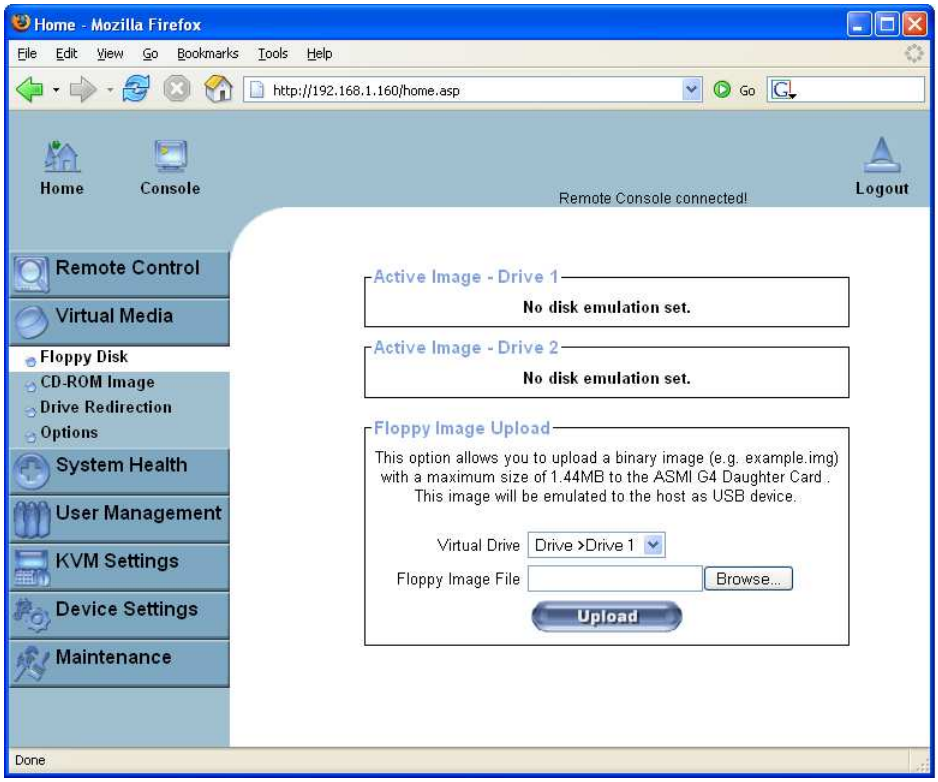


On this screen you will find buttons which allow you to power cycle or reset the remote server. This does not affect the ASMI module! In order to control the ASMI module please consult the section under "Device Settings".

Virtual Media

Floppy Disk

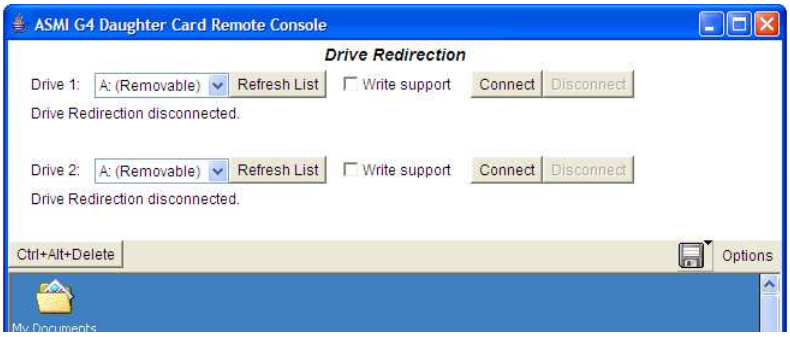
Figure 6-3. Virtual Floppy Area



Dual Floppies

As you can tell from the previous screen, you can actually redirect two virtual floppies using the pop-up.

Figure 6-4. Two Virtual Floppies

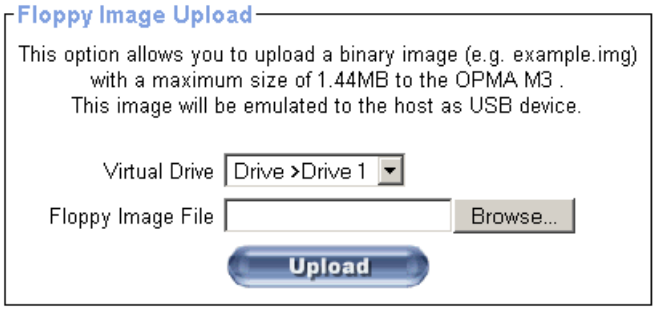


Upload a Floppy Image

With two small working steps a (floppy) image can be uploaded.

1. Specify the path of the images. You can pecify up to two images. You can do that either manually or by using the file selection dialog of your web browser. To open the file selection dialog click on the button "Browse" and select the desired image file.

Figure 6-5. Select Image File



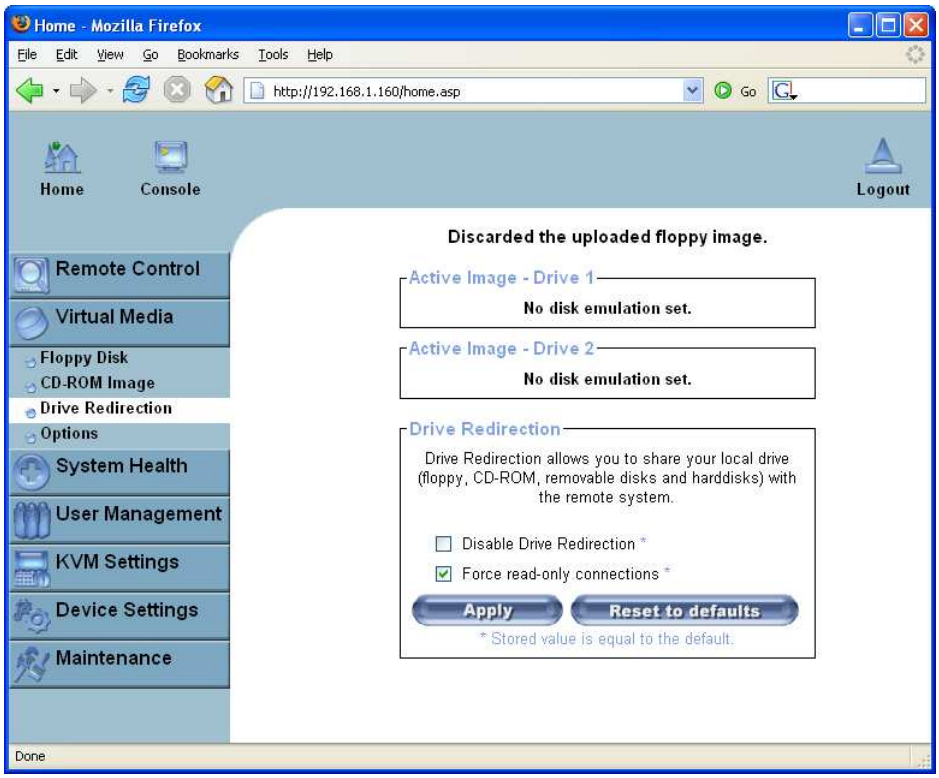
   The maximum image size is limited to 1.44MB. If you want use a larger image then please mount this image using a Windows Share (or SAMBA).

2. Now click the "Upload" button to initiate the transfer of the chosen image file into the ASMI module’s on-board memory. This image file is kept in the on-board memory of the ASMI module until the end of the current session or until you logout or initiate a reboot of the ASMI module.

Drive Redirection

The Drive Redirection is another possibility to use a local 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 then shared over the TCP/IP network connection. Local devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is possible to enable write support so that the remote machine is allowed to write data to your local disk.

Figure 6-6. Drive Redirection



Please note that Drive Redirection works on a level which is far below the operating system. Actually this means that neither the local nor the remote operating system is aware that the drive is currently redirected. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine or 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 well contain older data. This may confuse the remote host's operating system. We advise you to use the Drive Redirection with care, especially when you use write support.

Drive Redirection Options

As shown in Figure 6-6 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 to the redirected device.

Click "Apply" to submit your changes.

Software Requirements

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

Drive Redirection Tool

Configuration

Figure 6-7. Drive Redirection configuration

Specify the parameters of the network connection (see Figure 6-7).

Device

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

Port

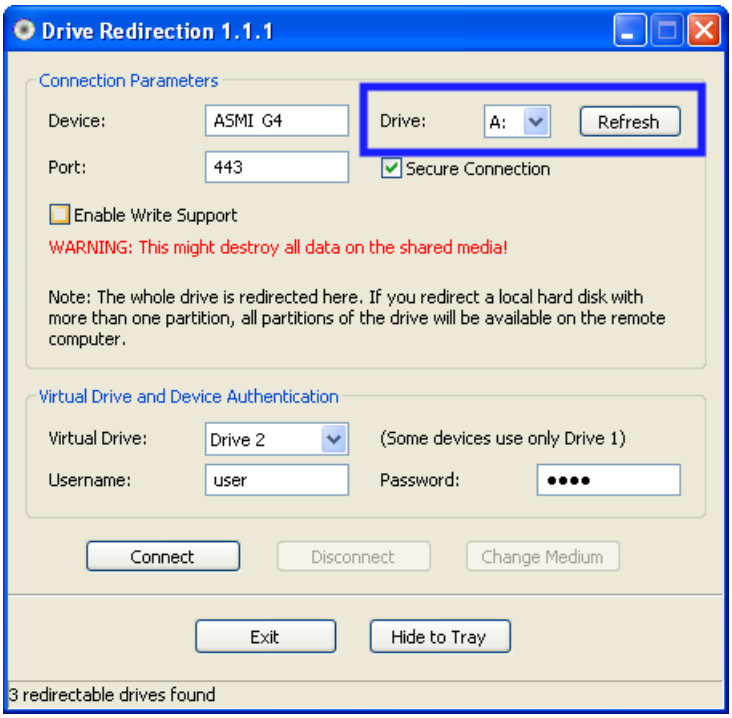
This is the network port. By default the ASMI module uses the remote console port (#443) here. You need to change this value if you have changed the remote console port in your ASMI module's network settings.

Secure Connection

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

Drive Selection

Figure 6-8. Selecting the desired drive

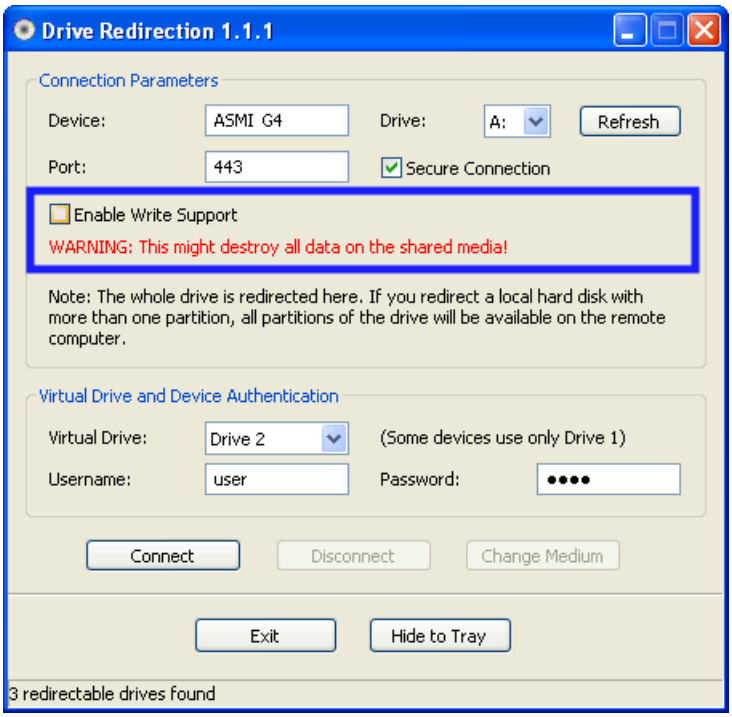


Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected.

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

Write Support

Figure 6-9. Selecting write support

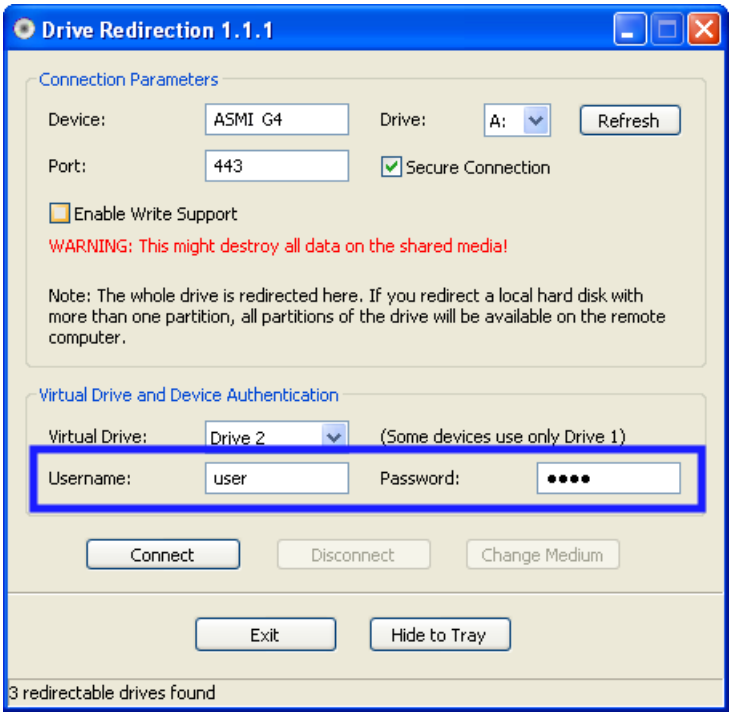


This feature may be enabled here. Write support means that the remote computer is allowed to write onto your local drive. As you can imagine, this is very dangerous (see above).

> **Warning**
>
> If both the remote and the local system try to write data onto the same device, this will certainly destroy the file system on the drive. Please use this only when you REALLY know what you are doing.

Device Authentication

Figure 6-10. Device Authentication



You have to authenticate on the ASMI module using a valid username and password in order to use Drive Redirection. You also 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 shows that the connection has been established. Consequently 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 operation may fail, especially if a file on the drive is currently open. In case of a locking failure, you will be prompted if you want to establish the connection anyway. This should not be a serious problem when the above warning is respected. If write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

With the "Disconnect" button, the connection via Drive Redirection connection is terminated.

Exit/Hide

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

Using the "Hide to Tray" button the application is hidden, but not terminated completely. This means that an active connection will be kept alive until it is explicitly closed. You can access the software by clicking 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 6-11).

Figure 6-11. Tray Info

Creating an Image

Floppy Images

UNIX and UNIX-like OS

To create an image file make use of "dd". This is one of the core 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:

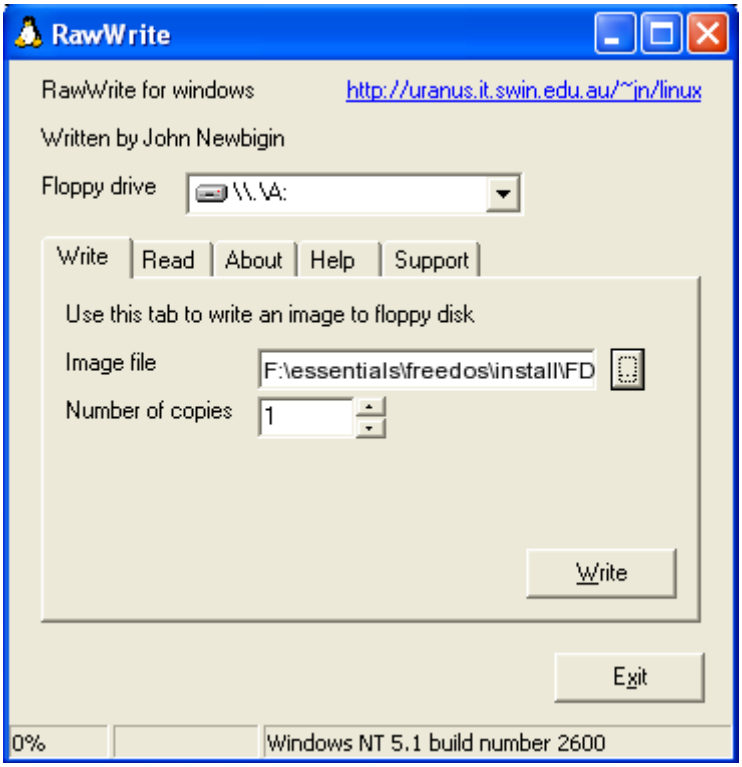
dd [*if=/dev/fd0*] [*of=/tmp/floppy.image*]

dd reads the entire disc from the device `/dev/fd0` and saves the output to 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 ASMI module.

Figure 6-12. RawWrite for Windows selection dialog



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 button "Copy" 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 core UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux).

To create a CD ROM image file you have to copy the contents of the CD ROM 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 to the specified output file `/tmp/cdrom.image`. Adjust both parameters to suit your needs (input device etc.).

MS Windows

Create the image file using your favorite CD imaging tool to copy 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.

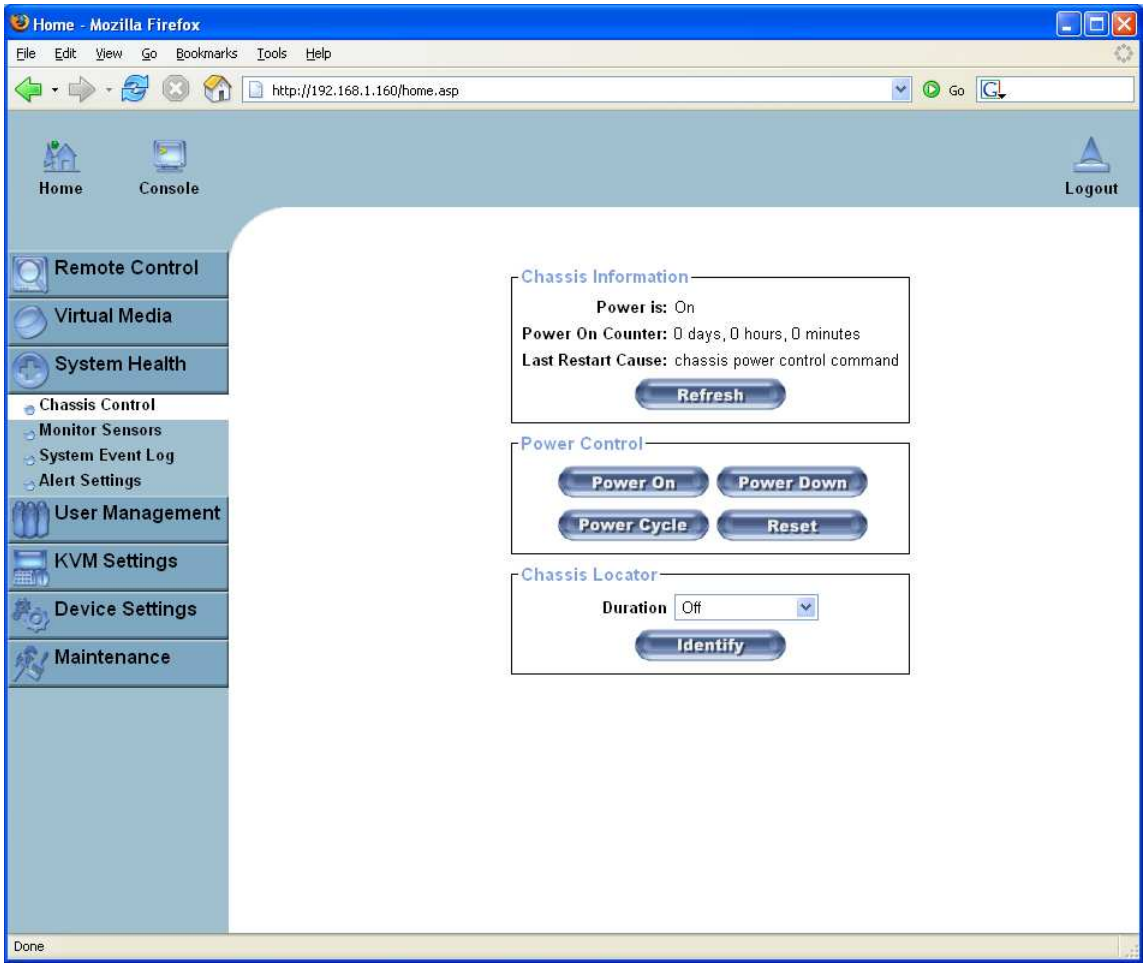
Figure 6-13. Nero selection dialog

System Health

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

Chassis Control

Figure 6-14. Chassis Control

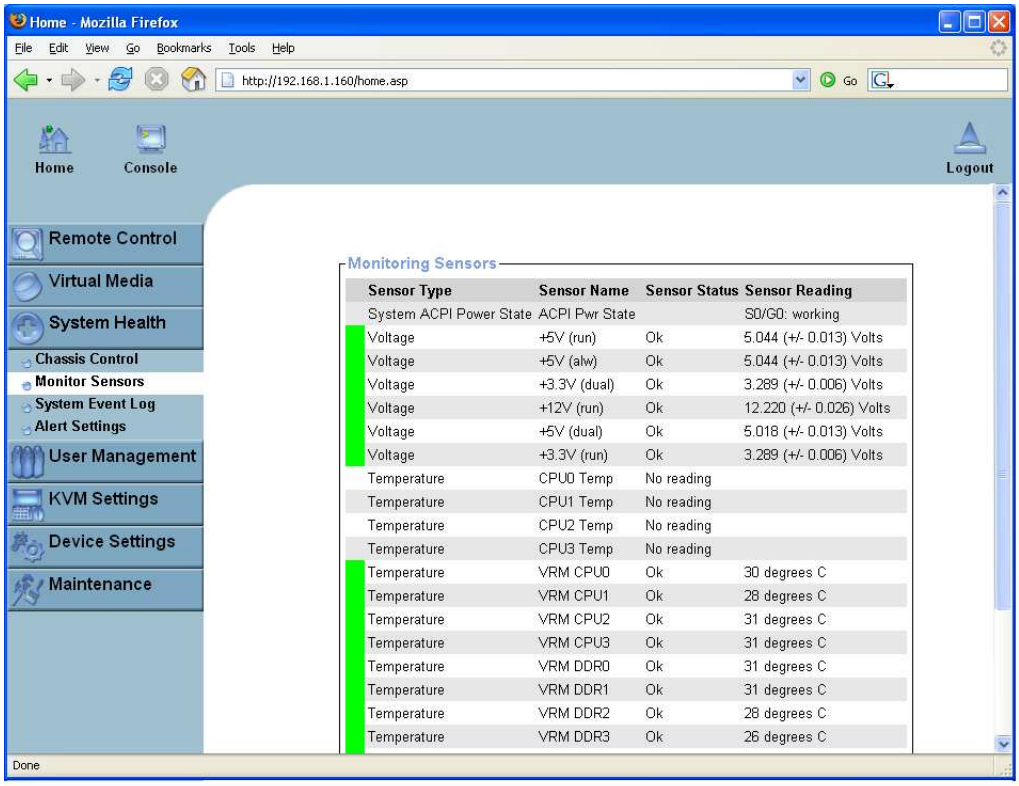


Using Chassis Control you can:

- Obtain information about the selected chassis
- Switch the remote power on and off (power cycle)
- Locate the remote host chassis

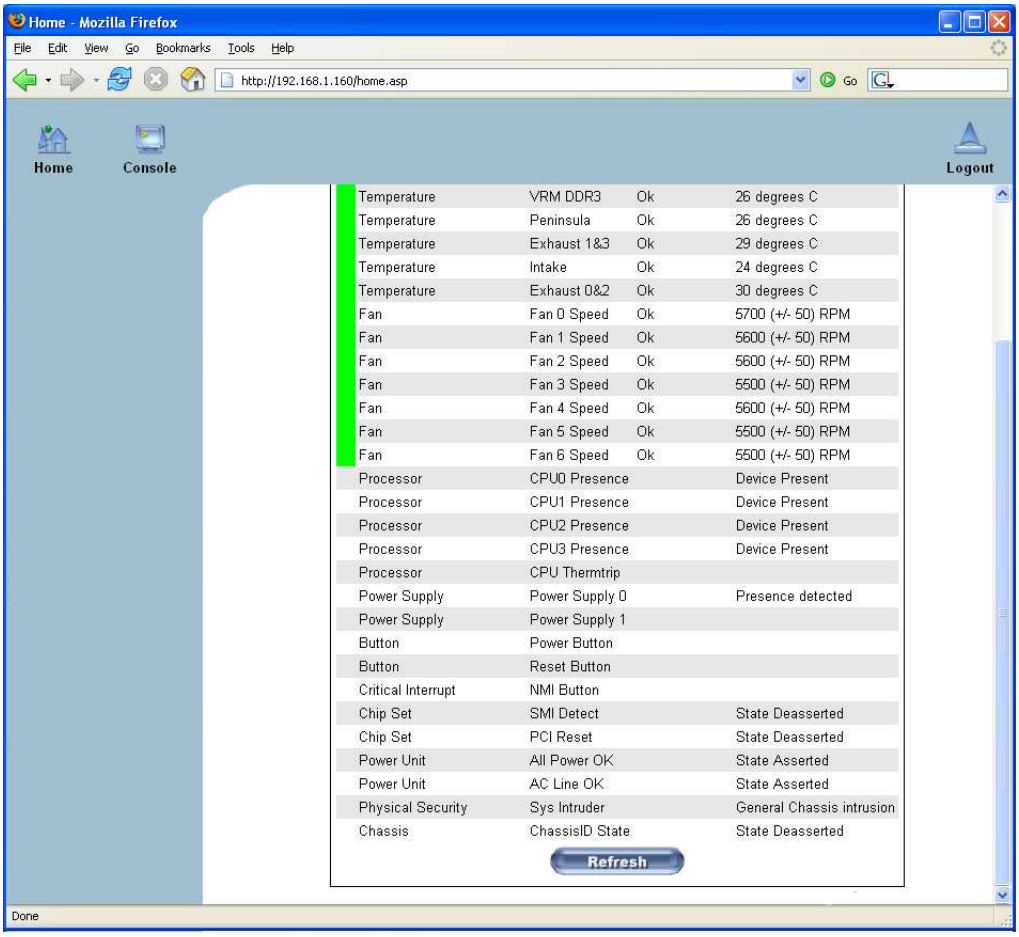
Monitor Sensors

Figure 6-15. Monitoring Remote Sensors Screen 1



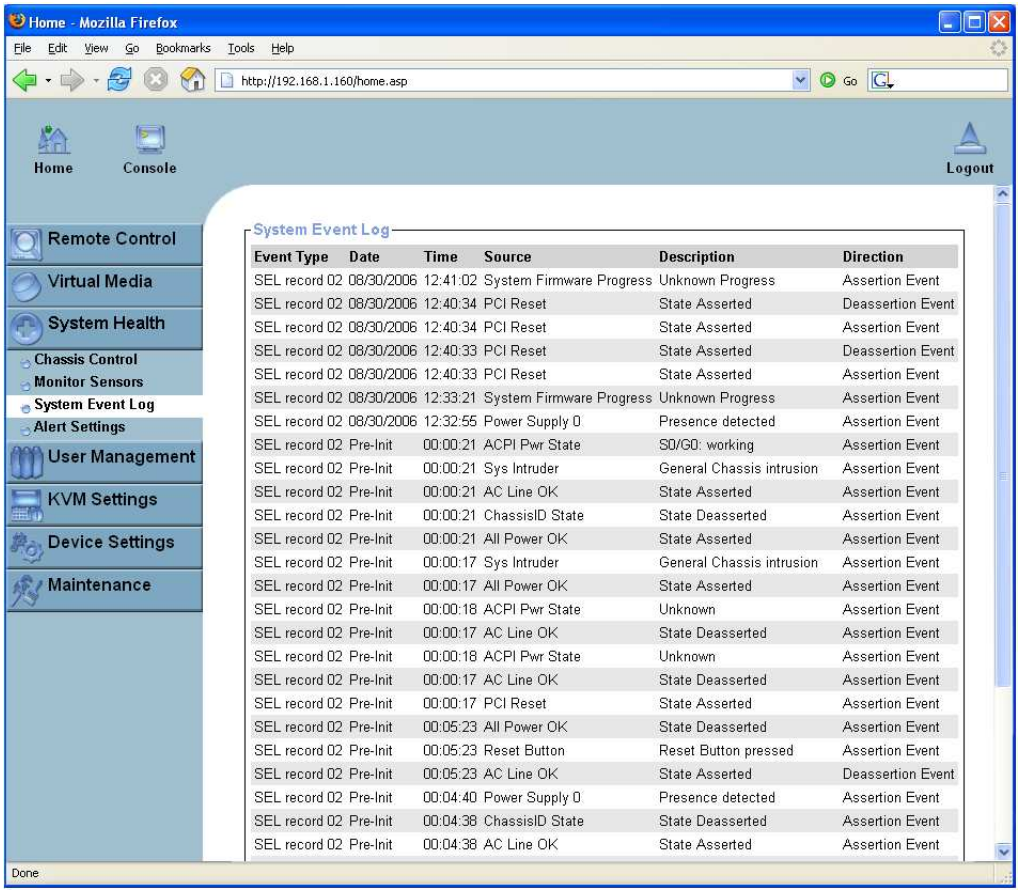
On this screen you can see some of the remote hosts sensors and their values or state.

Figure 6-16. Monitoring Remote Sensors Screen 2



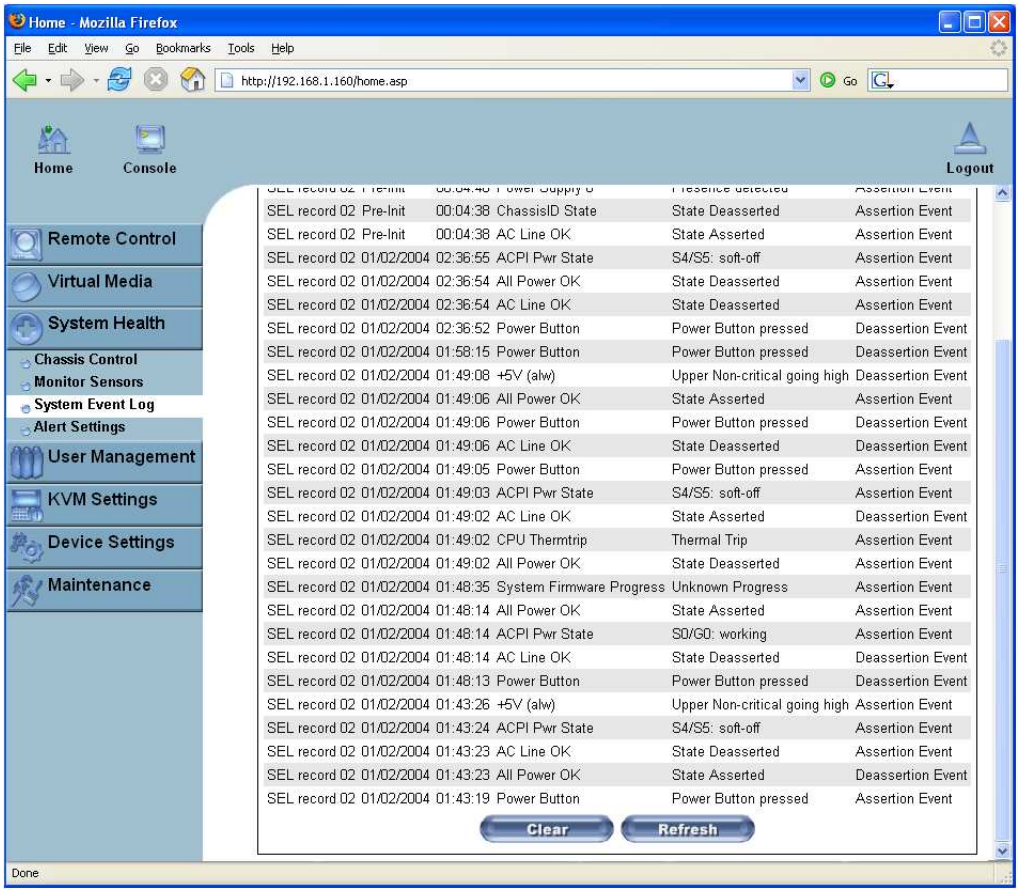
System Event Log

Figure 6-17. System Event Log Screen 1



You can browse the System Event Logs here. Note: these logs are for IPMI events. These are different to the ASMI module's own system logs.

Figure 6-18. System Event Log Screen 2



User Management

The ASMI module comes with a pre-configured user account for the administrator also referred as the super-user. The super-user has the default login name "super" and a fixed set of permissions. This user has all possible rights needed to configure the device and to access all of the functions of the ASMI module.

Upon delivery of the ASMI module the account for the super-user "super" has the password "pass".

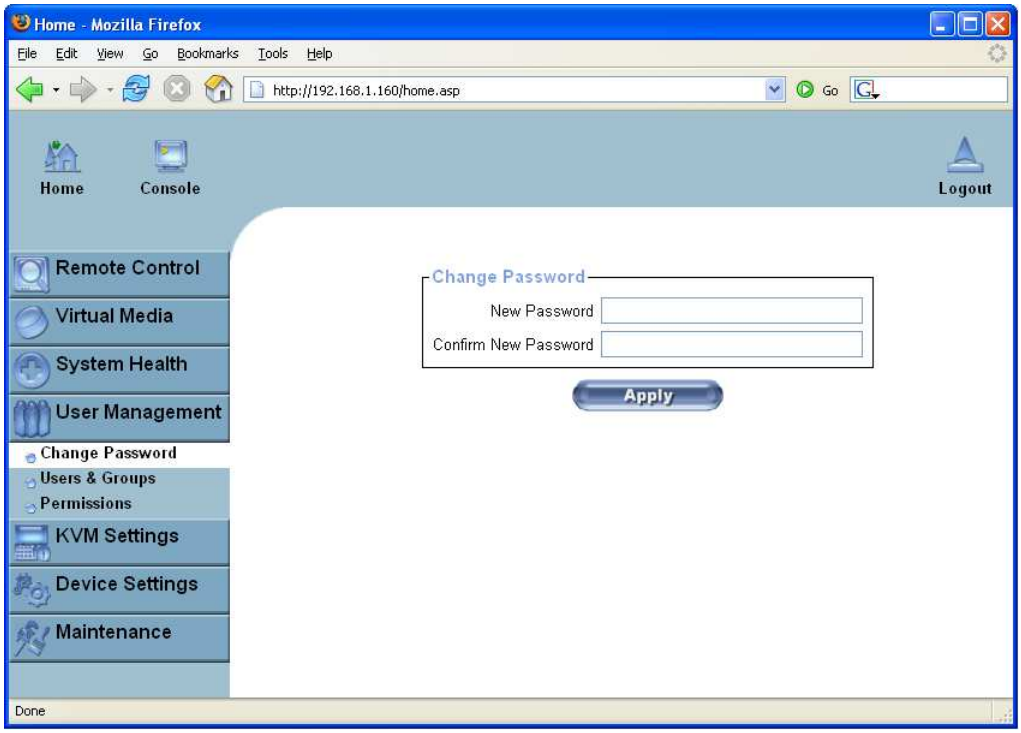
The ASMI module has two pre-defined user groups:

- **Admin** - User group for the administrative super-user
- **<Unknown>** - A restricted group for useres without a specific group.
- **None** - Not really a group. This indicates that a user is not a member of any group and thus owns a private set of permissions.

Note: Even acting as the super-user you cannot delete any of the pre-defined groups. You may create and delete other groups as you wish.

Change Password

Figure 6-19. Set password

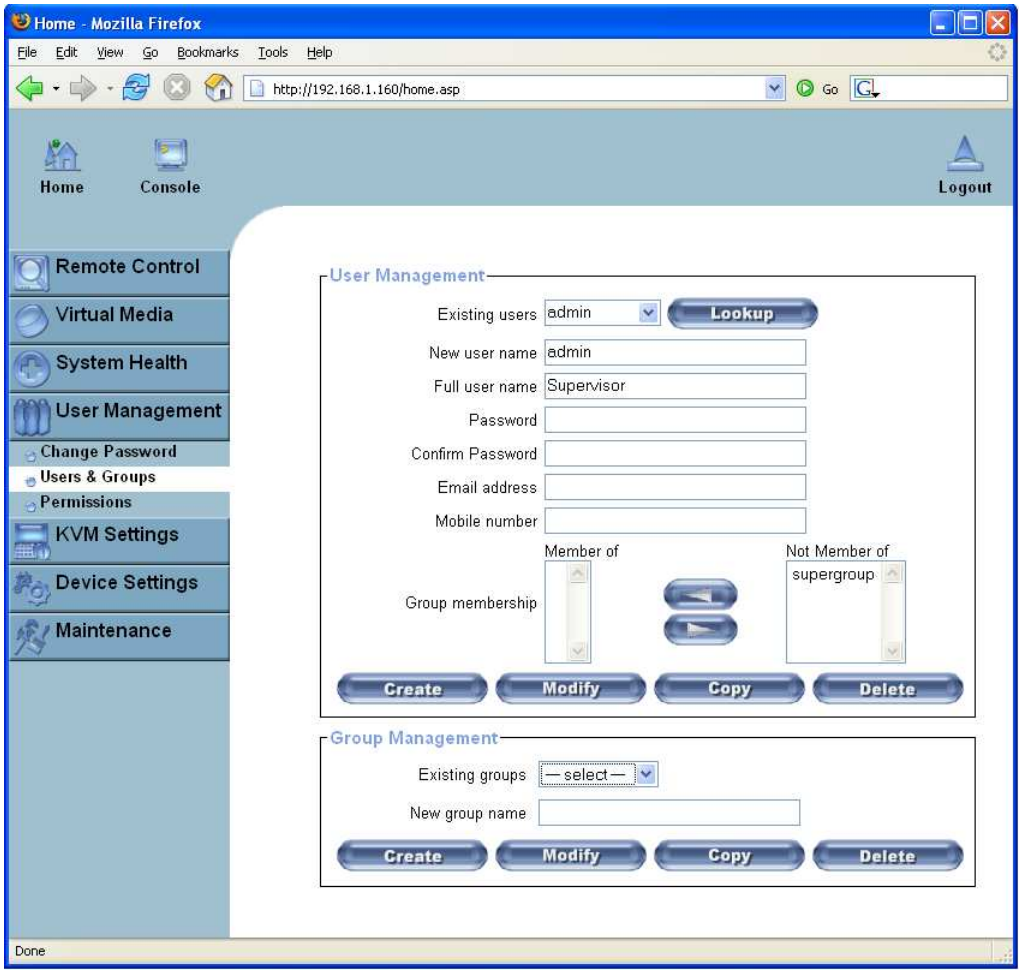


Change your password by entering the new password in the upper entry field. Retype the password in the field below in order to confirm it.

Click "Apply" to submit your changes.

Users And Groups

Figure 6-20. Set User



List of Available Options

A full list of available options follows. This list can only be seen by the super-user.

Existing users

Select an existing user for modification. Once a user has been selected, click the "Lookup" button to see the user information.

New User Name

The new user login name for the account currently selected or being created.

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.

User Group

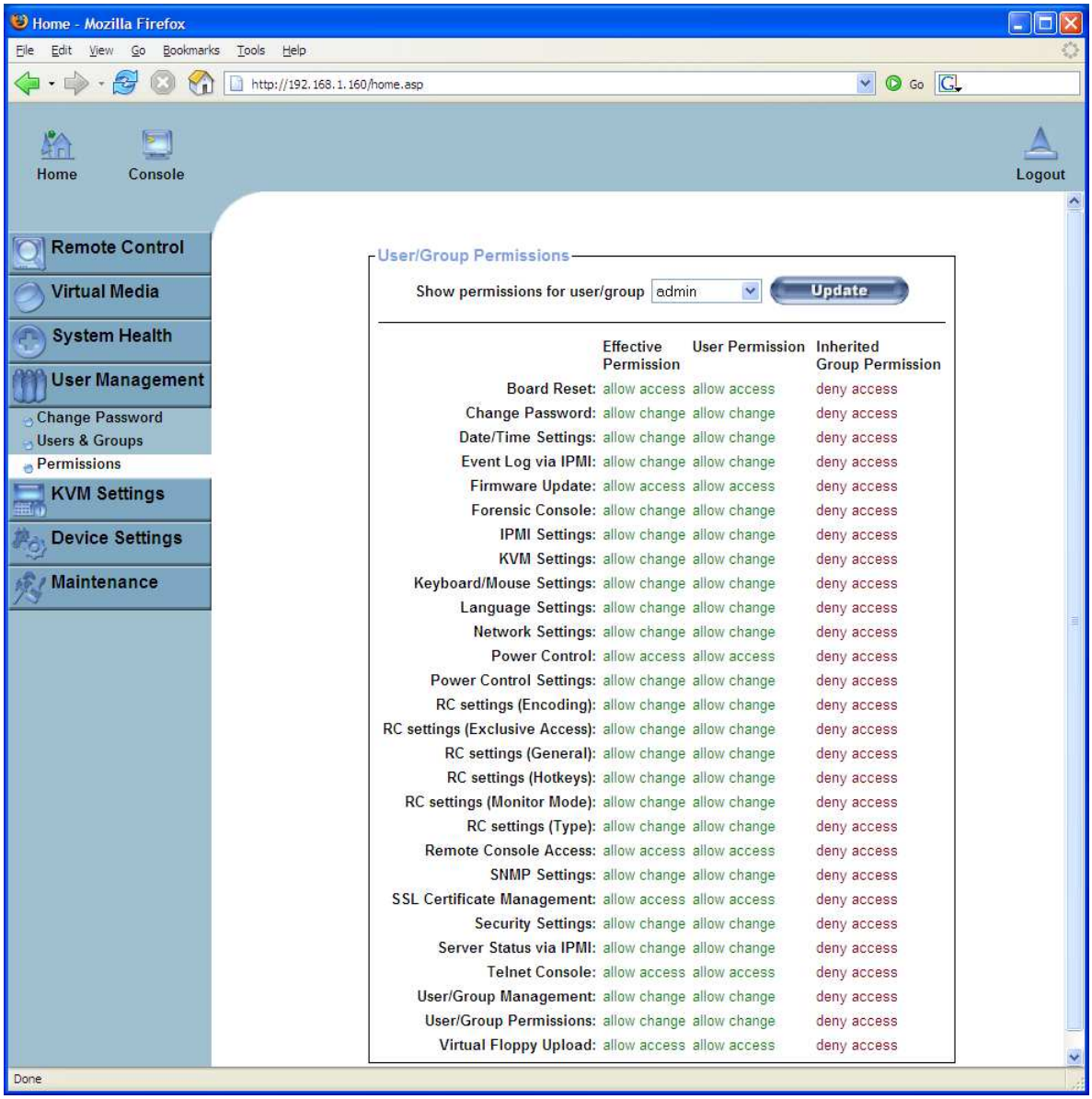
Each user can be a member of one group. This can be one of the built-in groups or a newly created one. A group defines a set of privilege levels (see there) for the user. If a user is in no group the individual privilege level set can be set for this user.

Press the button "Create" to create a user account. The button "Modify" changes the displayed user settings. Delete a user by pressing the button "Delete".

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

Permissions

Figure 6-21. Set Permissions



Only one permission set per user is allowed. Either the user inherits permissions from his/her group or if the user does not belong to a group, the permissions can be set individually for this user.

This page allows you to set these permissions for each group or group-less user. First select the item (group or group-less user) from the drop-down lists. All changes you make then affect the permission set of the selected entity.

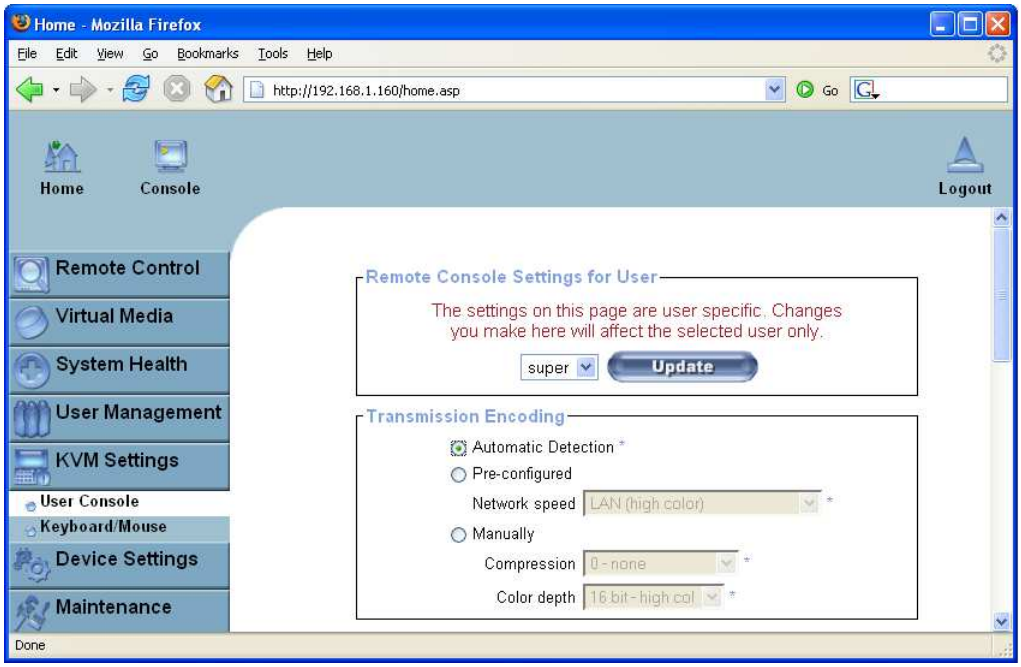
Each entry allows or denies the usage of a certain functionality. The fields labelled "RC Settings" pertain to the settings of the Remote Console.

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 6-22. User Console Settings (Part 1)



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 button "Update". This will result in displaying the proper user settings shown 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 network connection (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

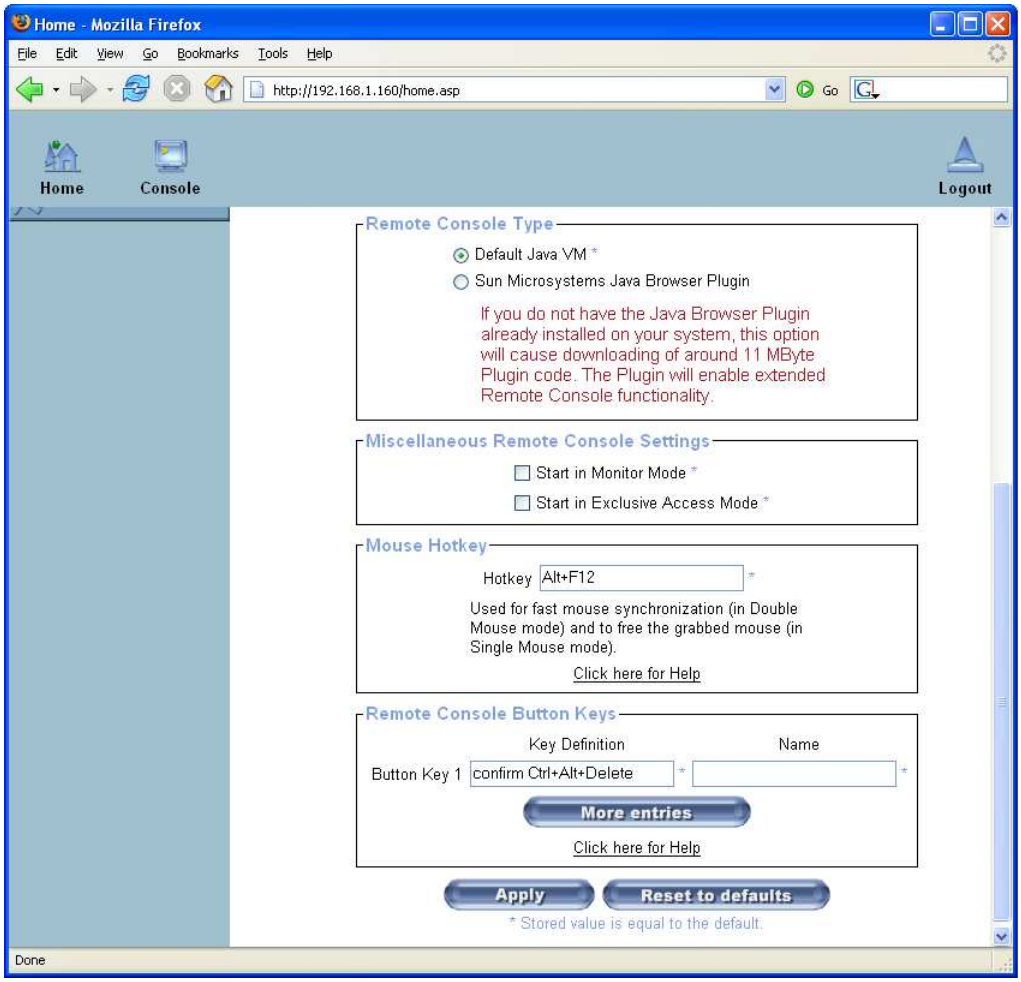
The pre-configured settings deliver the best result due to the optimized adjustment of the compression level and color depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the color depth individually. Depending on the selected compression rate the data stream between the ASMI 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 ASMI 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. For 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 6-23. User Console Settings (Part 2)



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 will be downloaded and installed automatically.

However, in order to make the installation possible you still have to answer the required 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.

> **Tip:** 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 ASMI module.

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is disabled. If case you switch it on the Remote Console window will be started in a read-only mode, i.e. only remote video is visible - remote keyboard and mouse are not connected.

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 asterisk at the end means that you may add further keys as is often required in your case. The term "confirm" adds an confirmation dialog 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 asterisk 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

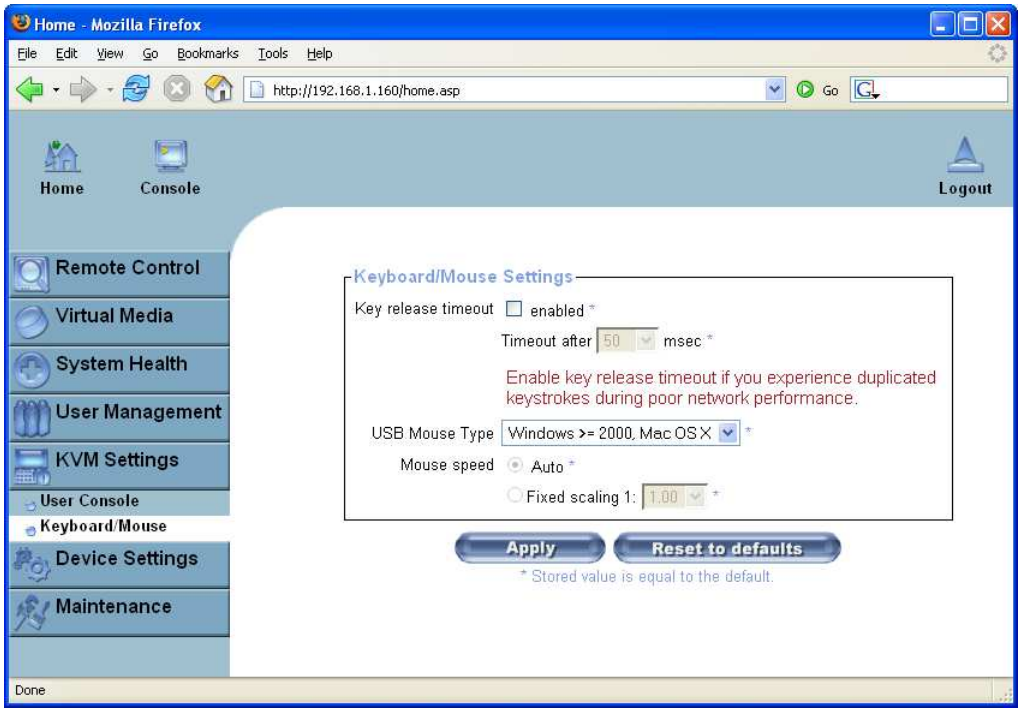
```
Ctrl+Alt+F2
```

For a full list of key codes and aliases please refer to the Appendix D.

> **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 6-24. Keyboard and Mouse Settings



Key Release Timeout

This is an important option if you are accessing the ASMI module over a slow or congested network. In such a situation you transmit a network packet containing the key PRESS to the ASMI module. When you release the key, then the ASMI 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 ASMI module to replicate the key press, this is like you holding down the desired key.

The Key Release Timeout in milli-seconds tells the ASMI module to consider the key released even when no RELEASE packet has arrived. This avoids keys being unintentionally repeated.

USB Mouse Type

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

In "MS Windows 2000 or newer" mode the remote mouse is always synchronized with the local mouse. For a detailed description of 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 ASMI 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.

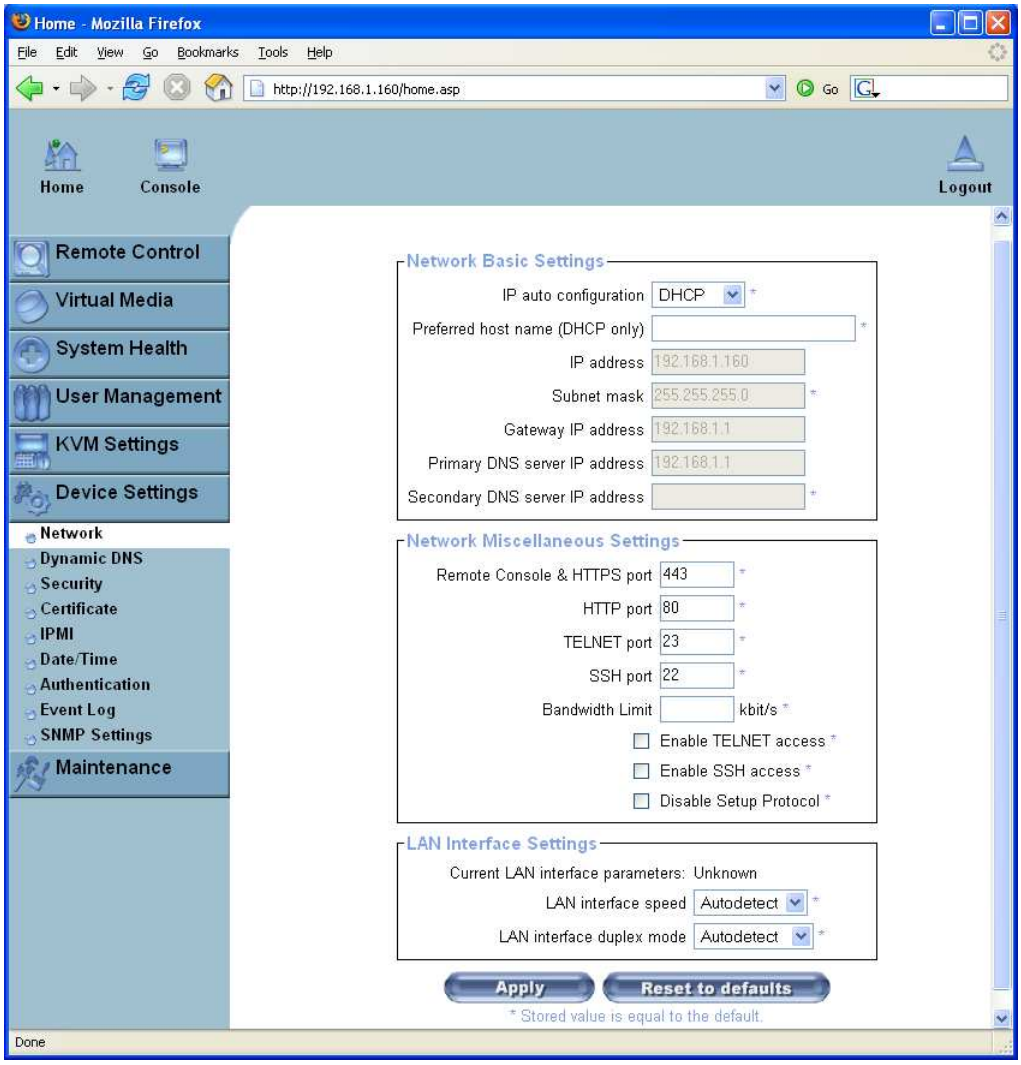
To set the options click on the button "Apply".

Device Settings

Network

The Network Settings panel as shown in Figure 6-25 allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

Figure 6-25. Network Settings



Warning

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

Warning

Changing the network settings of the ASMI module might result in losing the connection to it. In case you change the settings remotely make sure that all the values are correct and you still have a way to access the ASMI module.

Basic Network Settings

IP auto configuration

With this option you can define whether the ASMI 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. In this case the IP address and netmask have to be configured manually. If necessary, gateway and DNS server IP addresses have to be set as well.

Preferred host name

Preferred host name to request from DHCP server. Whether the DHCP server takes the ASMI module's suggestion into account or not depends on the DHCP 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 ASMI 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. If this option is left empty, the ASMI 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 ASMI module's Remote Console server and HTTPS server are listening. If left empty the default value (port 443) will be used.

HTTP port

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

Telnet port

Port number at which the ASMI module's Telnet server is listening. If left empty the default value (port 23) will be used.

SSH port

Port number at which the ASMI 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 ASMI 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 ASMI module from the setup protocol.

LAN Interface Settings

This entry field displays the current settings for the Ethernet/LAN interface of the ASMI 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

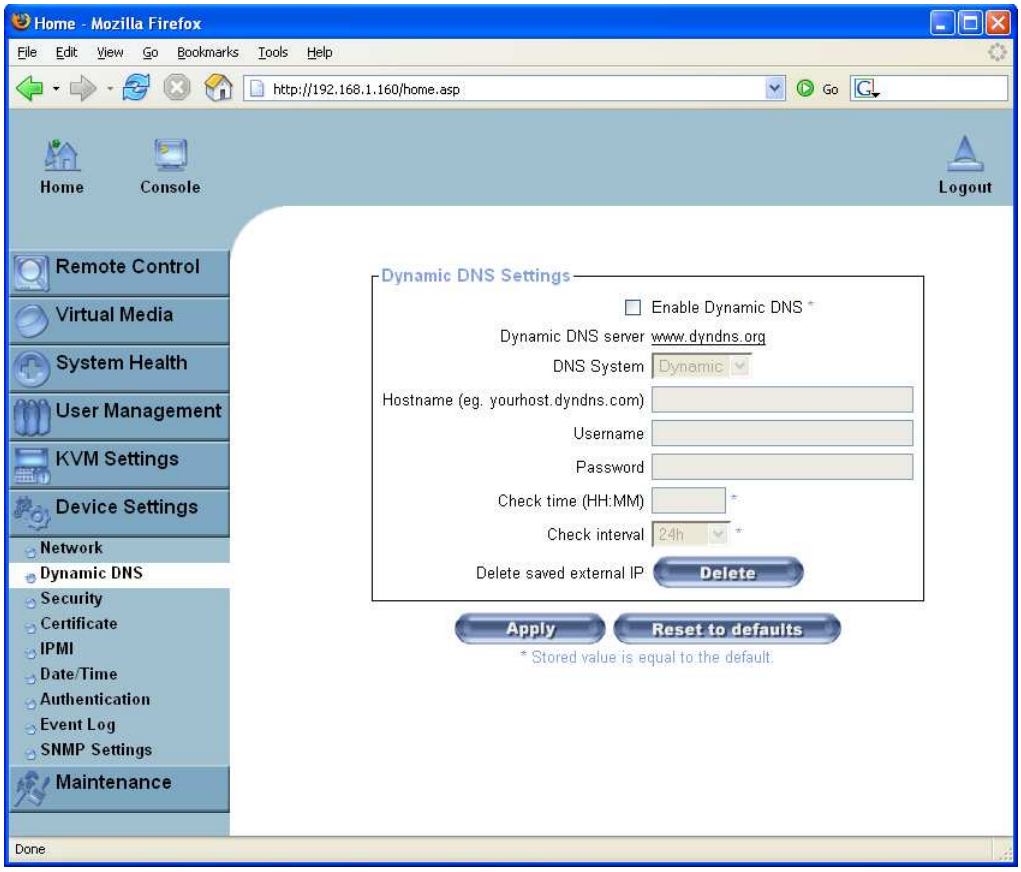
Depending on your network connection you may select an appropriate speed value for this interface. To adjust the interface automatically choose "autodetect" (default value). If this selection results in misbehavior of the interface, choose one of other speed options to work with. The interface will transmit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

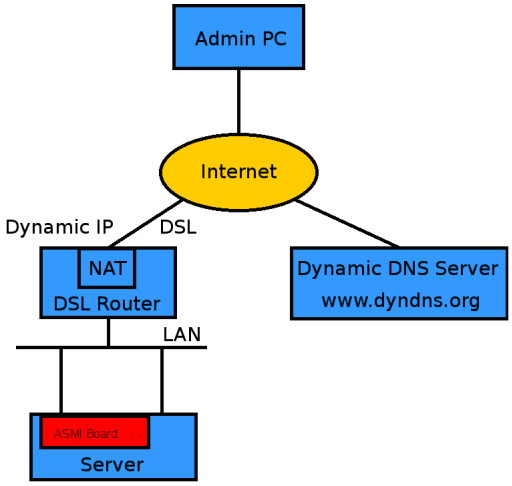
Dynamic DNS

Figure 6-26. Dynamic DNS



A freely available Dynamic DNS service (`dyndns.org`) can be used in the following scenario (see Figure 6-27):

Figure 6-27. Dynamic DNS Scenario



The ASMI 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 ASMI 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 selected ASMI module with the Dynamic DNS Server and give it a hostname. The Dynamic DNS Server will return a nickname and password to the registration process. This account information (together with the hostname) is needed in order to determine the IP address of the registered ASMI module.

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

1. Make sure that the LAN interface of the ASMI module is properly configured.
2. Enter the Dynamic DNS Settings configuration dialog as shown in Figure 6-26.
3. Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

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

Dynamic DNS server

This is the server name where ASMI 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 ASMI module that is provided by the Dynamic DNS Server.

Tip: Use the fully qualified host name (including the domain, e.g. `testserver.dyndns.org`) not just

the abbreviated 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 ASMI module card registers itself with the Dynamic DNS server at this time.

Check interval

This is the report interval to the Dynamic DNS server by the ASMI module.

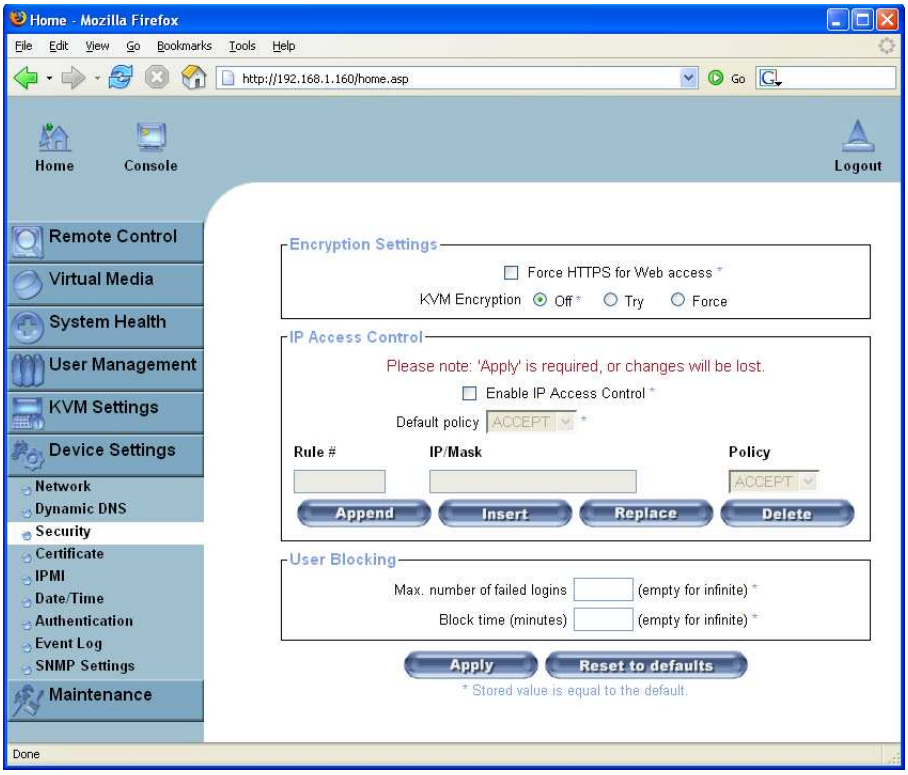
Warning

The ASMI module has its own independent real time clock. Make sure the time setting of the ASMI 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 button "Delete".

Security

Figure 6-28. Device Security



KVM Encryption

If this option is enabled, access to the web front-end is only possible using a HTTPS connection. The ASMI 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 ASMI 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 ASMI 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.

> **Tip:** It is a good idea to DROP everything and then only ACCEPT a few connections. This is a lot more secure, than the other way around.

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).

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.

User Blocking

When someone attempts to login to the ASMI module and fails, you can specify how many failed login attempts the ASMI 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.

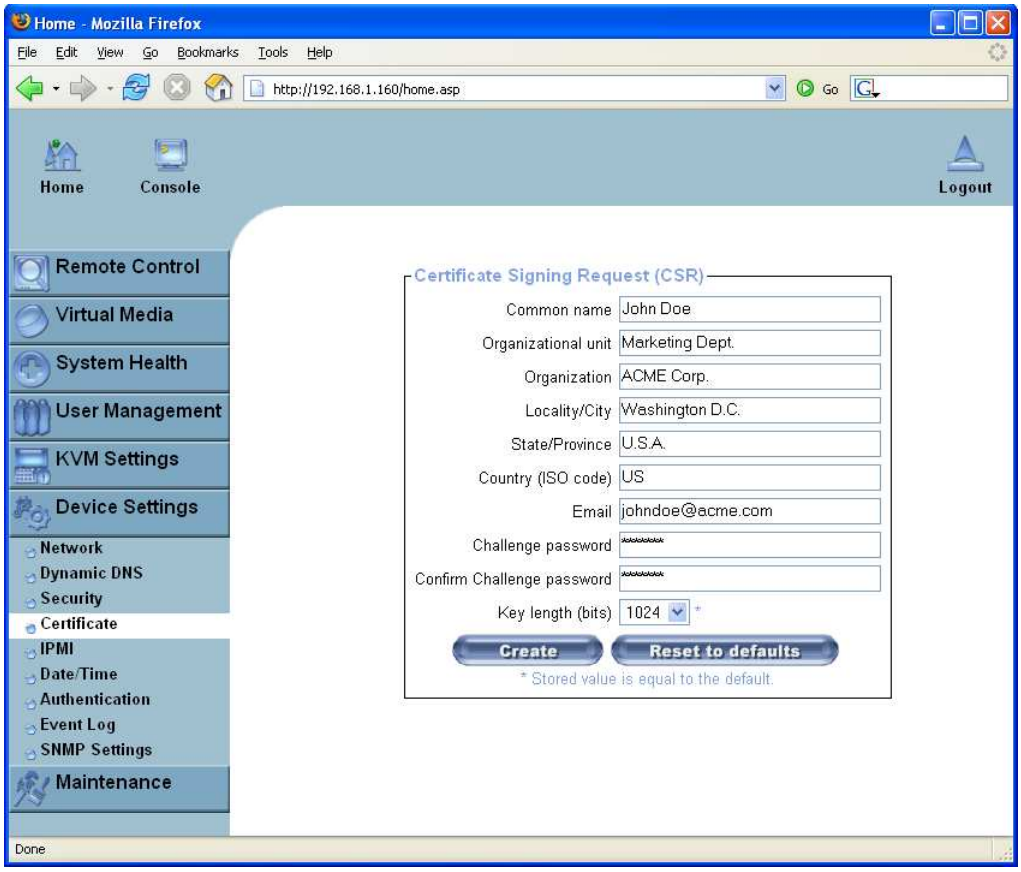
Login Limitations

You can specify if only a single user is allowed to login to the ASMI module at one time. Note that if you do so, this greatly reduces the usefulness of for example the chat window, because you can then only talk to yourself. Also if another administrator is logged in from a different location, then you will be blocked acessing the ASMI module.

Password aging is the time interval at which users are required to change their password. Some systems refer to this as "Password Expiry".

Certificate

Figure 6-29. Certificate Settings



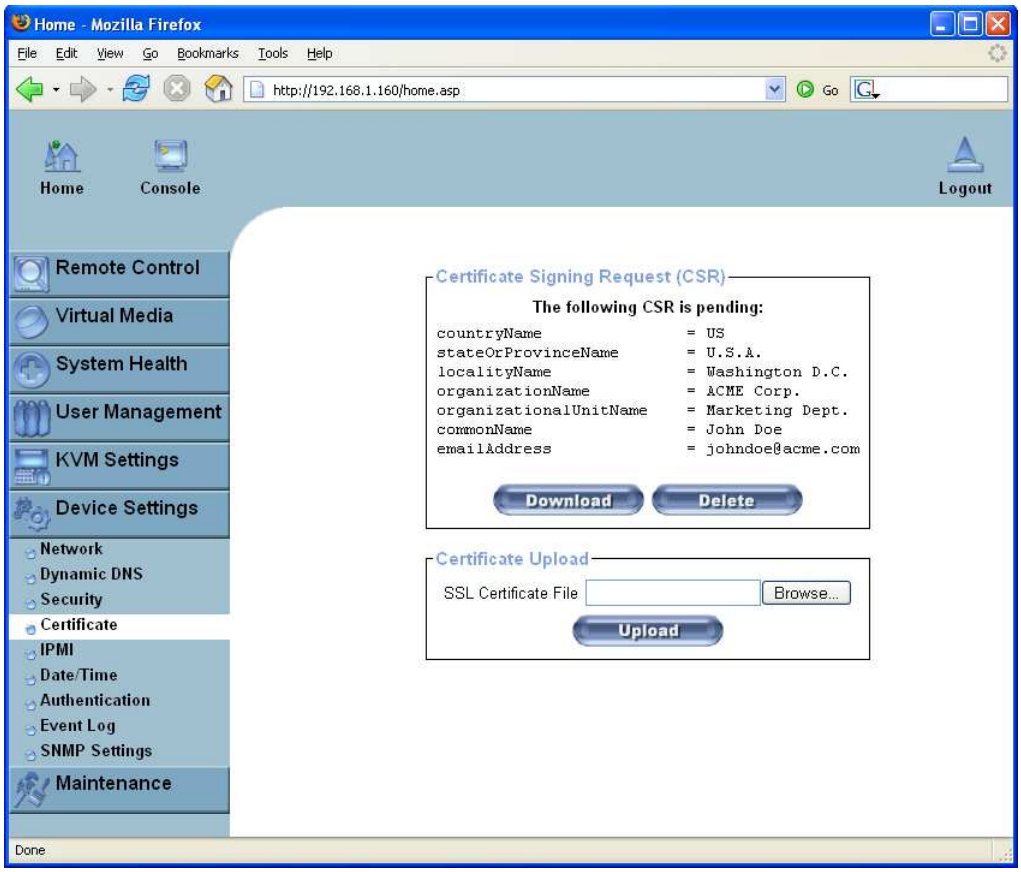
The ASMI module uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the ASMI module has to expose its identity to a client using a cryptographic certificate. After delivery this certificate and the underlying secret key is the same for all ASMI module ever produced and certainly will not match the network configuration that will be applied to the ASMI 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 ASMI module card. In order to do that, the ASMI 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 to be and signs and issues the SSL certificate to you.

To create and install an SSL certificate for the ASMI module the following steps are necessary:

1. Create a SSL Certificate Signing Request using the panel shown in Figure 6-29. You need to fill out a number of fields that are explained below. Once this is done, click on the button "Create" which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the "Download CSR" button (see Figure 6-30).
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 ASMI module using the "Upload" button as shown in Figure 6-30.

Figure 6-30. SSL Certificate Upload



After completing these three steps the ASMI module has its own certificate that can be used to identify the card to its clients.

> **Warning**
>
> If you destroy the CSR on the ASMI module there is no way to get it back! In case you delete it by mistake, you have to repeat the three steps described above.

Common name

This is the network name of the ASMI 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 ASMI 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 ASMI module is accessed using HTTPS.

Organizational Unit

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

Organization

The name of the organization to which the ASMI 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 USA.

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

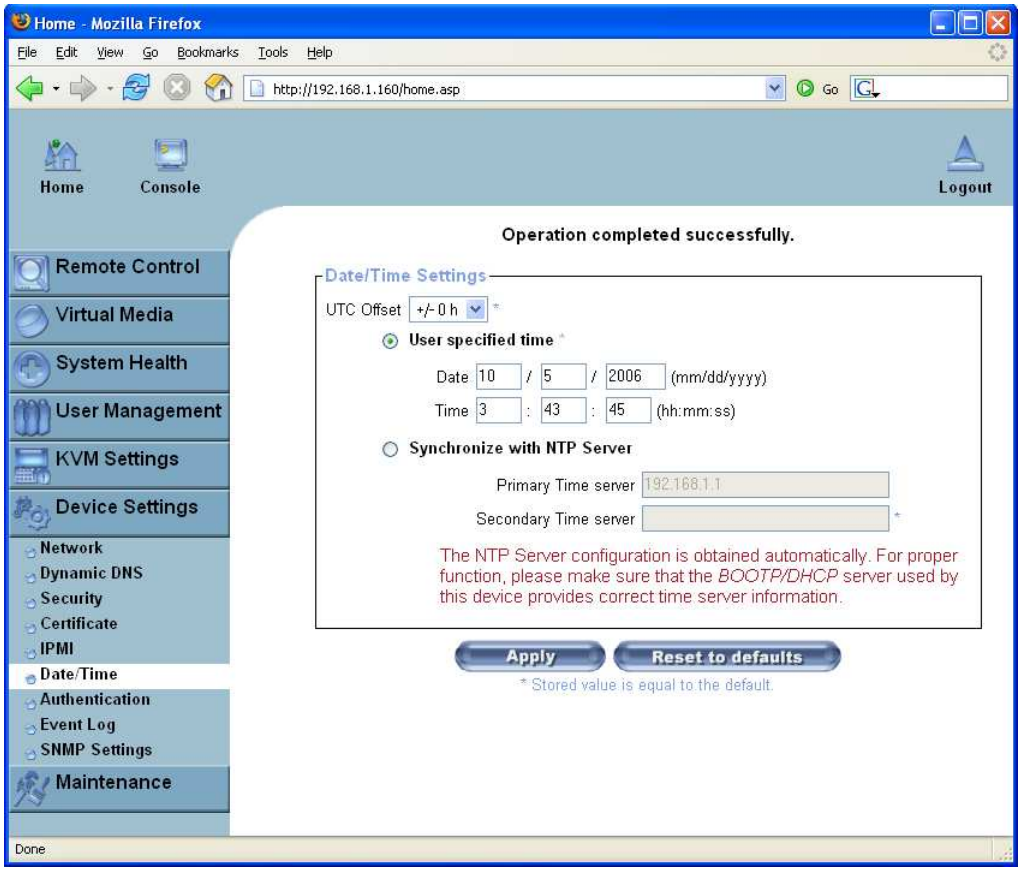
The email address of a contact person that is responsible for the ASMI module and its security.

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 ASMI module during connection establishment.

Date And Time

Figure 6-31. Date and Time



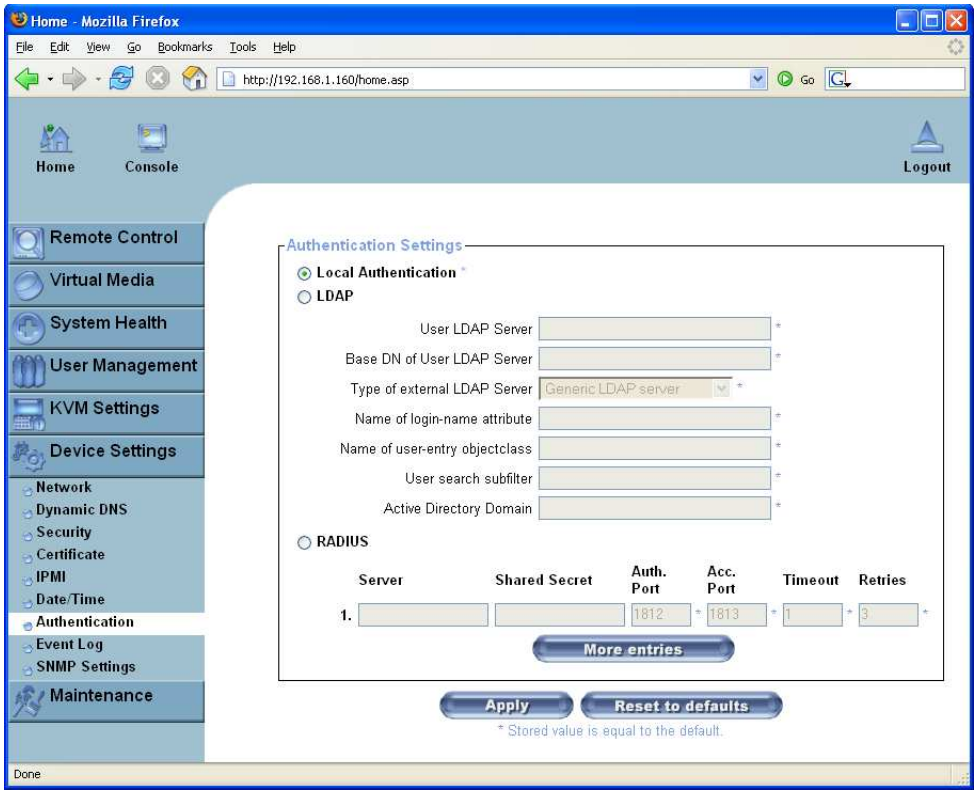
This link refers to a page where the internal realtime clock of the ASMI module can be set up (see Figure 6-31). You have the possibility to adjust the clock manually or to use an NTP time server. Without a time server your time setting will not be persistent, so you have to adjust it again after the ASMI 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 automatically adjust the daylight savings time. So you have to set up the UTC offset twice a year properly to suit the local rules of your country.

Authentication Settings

Figure 6-32. LDAP and other Authentication Settings



On this screen you can specify where the ASMI 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 ASMI module and the user/group information residing on the ASMI module will be used for authentication.

The other options allow you to specify an LDAP or 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 already existing groups, rather than having to re-enter everything into the ASMI module.

> **Note:** Whatever you configure you can always login over the network as the super-user "super". The super-user is always authenticated and authorized locally, so you always have a "back door" to access the ASMI module.

LDAP Access

The ASMI module uses LDAP only for authentication (password verification). User privileges and private settings are still stored locally in the ASMI module. That’s why, a user account has to be created

on the ASMI module before this user can login via LDAP. Also, all privilege configurations have to be done within the ASMI 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 should enter the name or IP address of the LDAP server containing 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 the 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.
- Here you can refine the search for users that should be known to the ASMI 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 C.

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

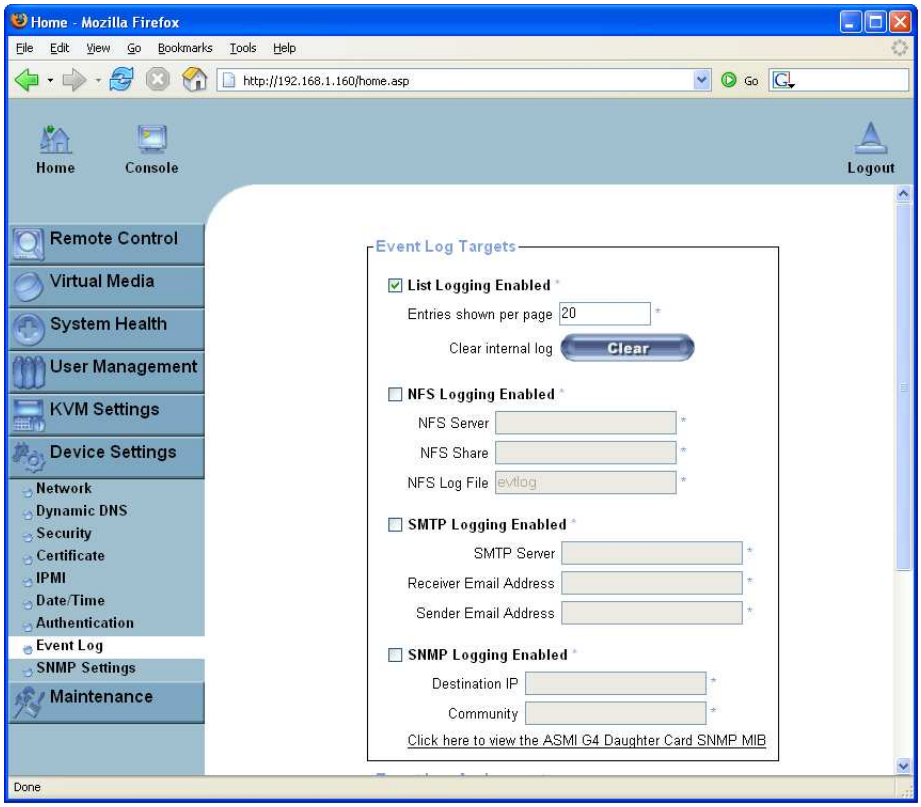
In order to access a remote device using the RADIUS protocol you have to login first. You are then asked to specify your user name and password. The RADIUS server reads your input data (Authentication) and the ASMI module looks for your profile (Authorization). The profile defines (or limits) your actions 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 similarly to the

Remote Console. If there is no activity for half an hour your connection to the ASMI module will be terminated and closed.

- Server: enter either the IP address or the hostname of the RADIUS Server to connect to. If you use 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 ASMI module acts 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 uses to listen for authentication requests. The default value is #1812.
- Accounting Port: the port the RADIUS server uses to listen for accounting requests.
- Timeout: sets the request TTL (time-to-live) in seconds. The TTL 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 when a request cannot be completed. The default value is to retry 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

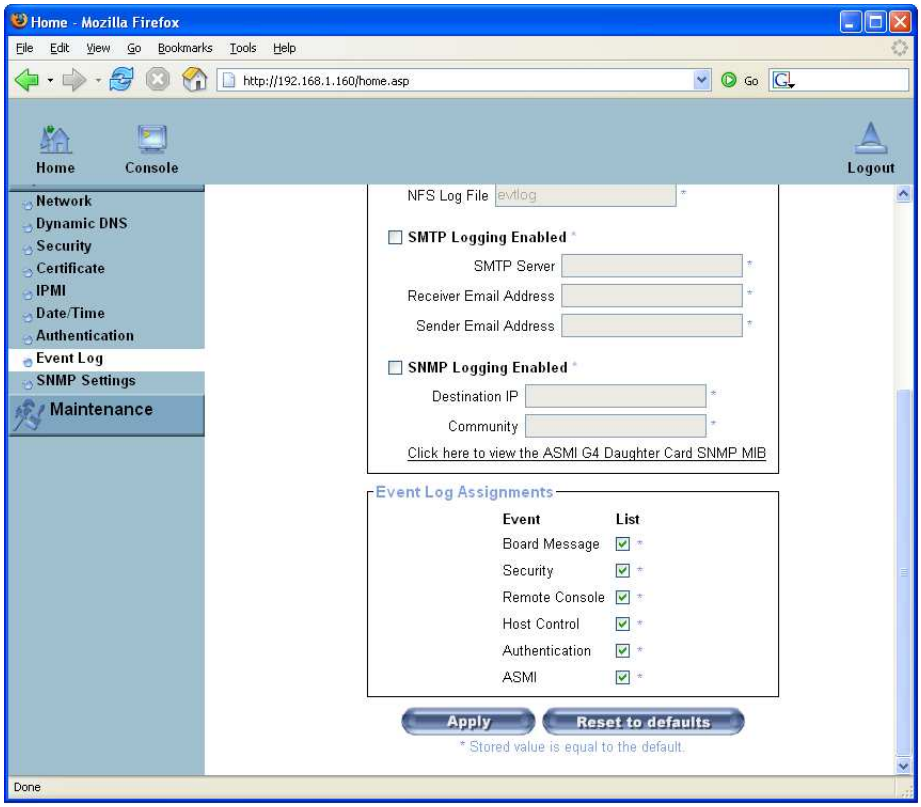
Figure 6-33. Event Log Screen Part 1



ASMI internal events (like a login failure or a firmware update) are logged to a selection of logging destinations (see Figure 6-33 and Figure 6-34).

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.

Figure 6-34. Event Log Screen Part 2



The common way to log events is to use the internal log list of the ASMI 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. You can also clear the log file here.

Event Log Targets

List logging enabled

If you wish to log events you may use the internal log list of the ASMI module. Click on "Event Log" on the "Maintenance" page to show the log list.

Since the ASMI 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 overwrites the oldest one automatically.

Warning

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

NFS Logging enabled

Defines an NFS server which exports a directory allowing the ASMI module to write all of its logging data to a file that is located there. If you need to write logging data from more than one ASMI module device to a single NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button "Apply", the NFS share will be mounted immediately. Therefore the NFS share and the NFS server fields must be filled with valid values or you will get an error message.

Warning

In contrast to the internal log file on the ASMI 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 ASMI module is able to send emails to an address given by the Email address text field in the Event Log Settings. These emails contain the same description strings as the internal log file and the email subject is set to the event group of the log event. In order to use this log destination you have to specify an SMTP server that has to be reachable from the ASMI module device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

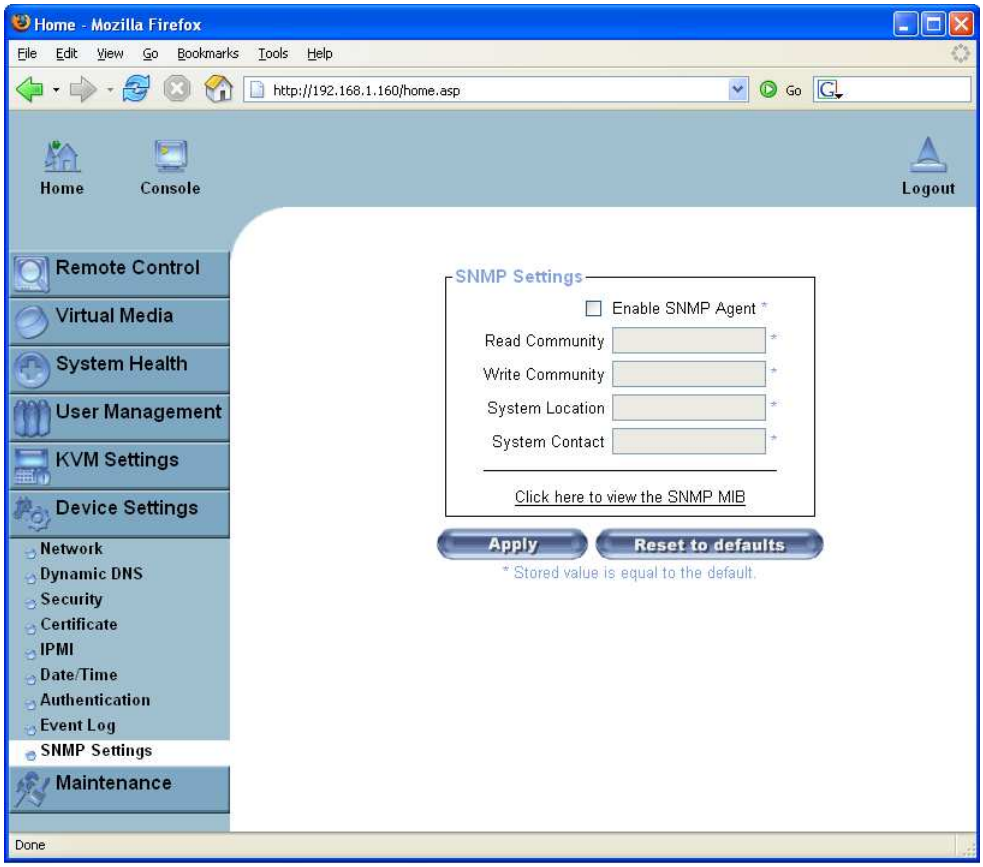
If this is activated, the ASMI module sends an SNMP trap to the specified destination IP address every time a log event occurs. If the receiver requires a community string you can define it in the appropriate text field. Most of the event traps only contain one descriptive string with all information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

Event Log Assignments

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

SNMP

Figure 6-35. SNMP settings



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 server on/off
- Reset the ASMI module

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

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

The SNMP settings panel as shown in Figure 6-35 is described below. It allows you to change SNMP related parameters.

Enable SNMP Agent

If this option is checked the ASMI module will reply to SNMP requests.

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

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 ASMI module or the host via SNMP, i.e. everything that affects the remote host or the ASMI module.

System Location

Enter a description of the physical location of the host. The description will be used in the reply to an 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".

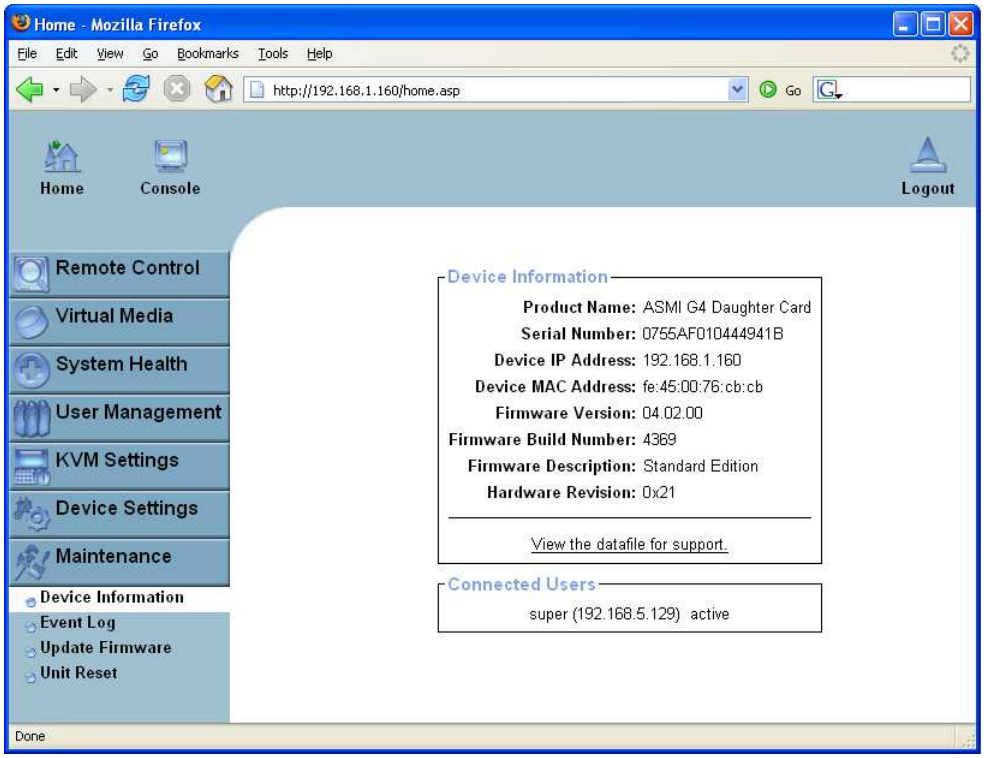
The ASMI module SNMP MIB

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

Maintenance

Device Information

Figure 6-36. Device Information



This section contains a summary of various information about this ASMI module and its current firmware and allows you to reset the card. You may have a look at Figure 6-36 for an example.

The data file for support allows you to download the ASMI module data file with specific support information. This is an XML file with specifically 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 faster.

Figure 6-37. Connected Users

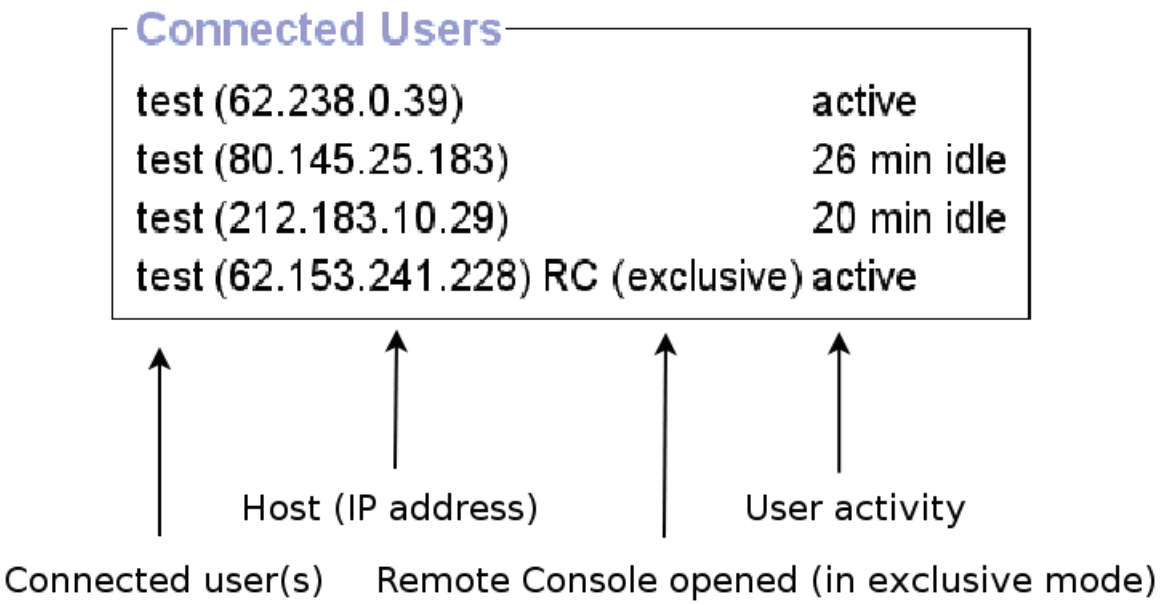


Figure 6-37 displays the ASMI module activity. From left to right the connected user(s), its IP address (from which host the user comes from) and their activity status is displayed. "RC" indicates that the Remote Console is open. If the Remote Console is opened in "exclusive mode" the term "(exclusive)" is added. For more information about this option see
the Section called *Remote Console Control Bar* in Chapter 5. User activitiy is displayed in the last column. It contains either the term "active" for an active user or the idle time for an inactive user.

Event Log

Figure 6-38. Event Log List

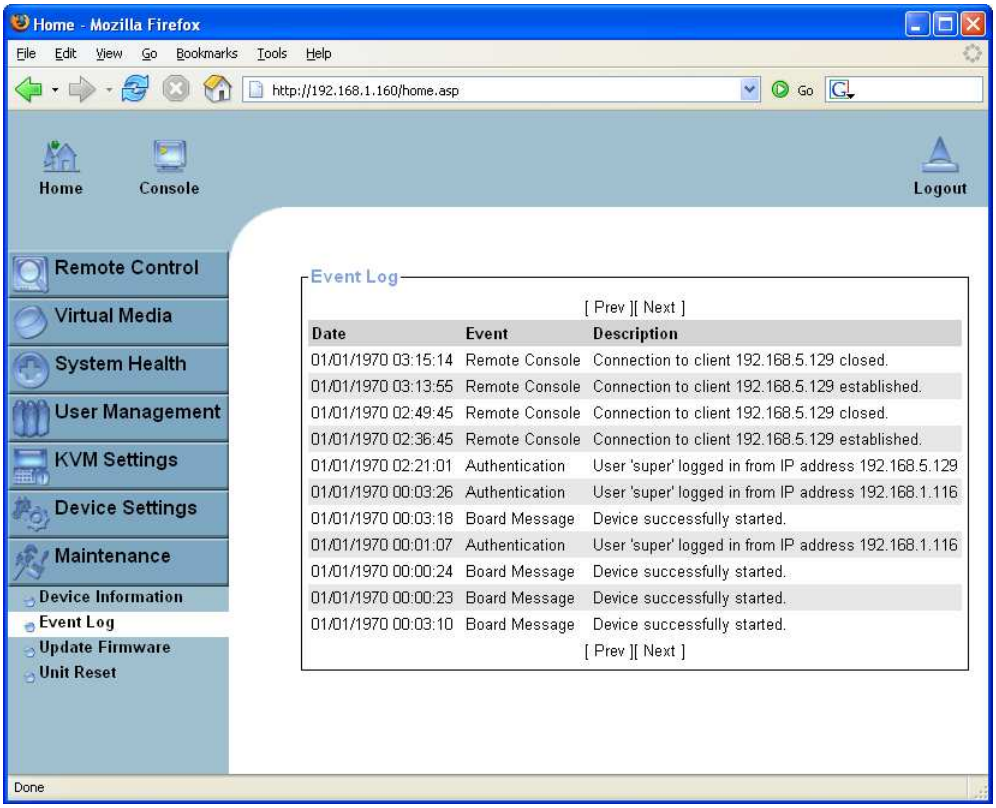
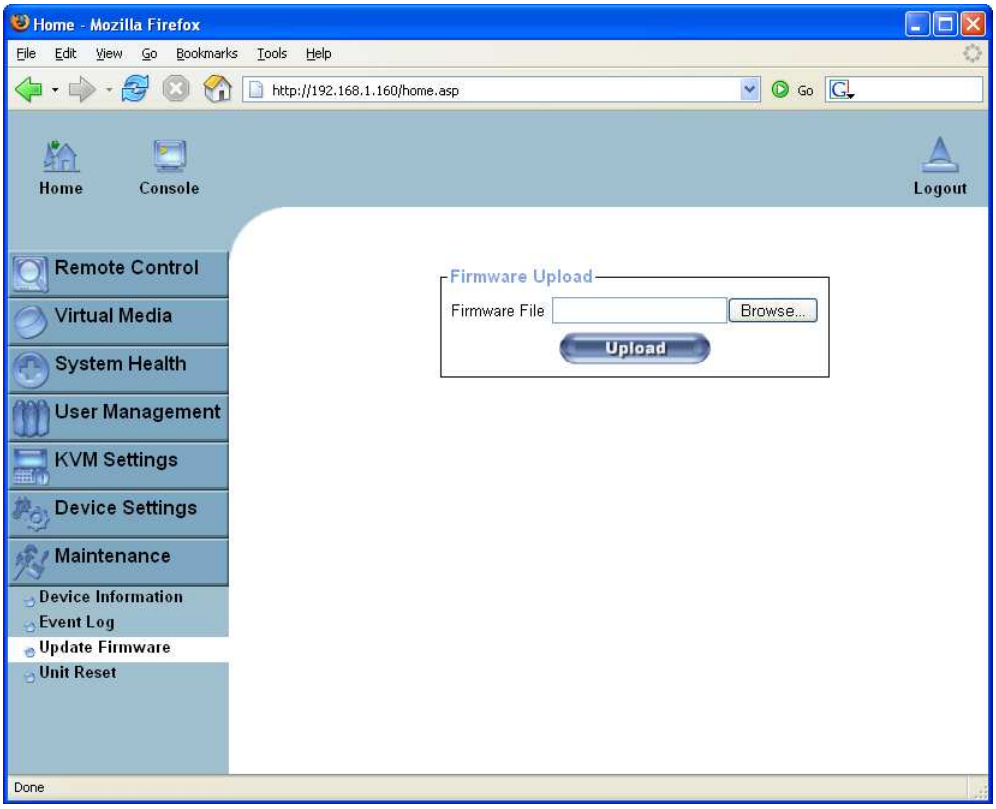


Figure 6-38 displays the Event Log list. It includes the events that are kept by the ASMI module extended by the event date, a short event description and the IP address that the request was sent from.

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

Update Firmware

Figure 6-39. Update Firmware



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

New releases of the ASMI G4 module firmware are available from http://support.raritan.com by searching for Raritan ASMI G4 Module. 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 by your OS (UNIX, Linux, OS X).

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

Updating the firmware is a three-stage process:

1. The new firmware file needs to be uploaded to the ASMI module. In order to do that you need to select the file on your local system using the button "Browse" of the Upload Firmware panel (see Figure 6-39). Then click "Upload" to transfer the selected file from your local file system to the ASMI 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 left in place. No update will take place.

2. Then, if everything in step 1 went well, you will see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the newly uploaded firmware. Pressing the button "Update" will store the new version and substitute the old one completely.

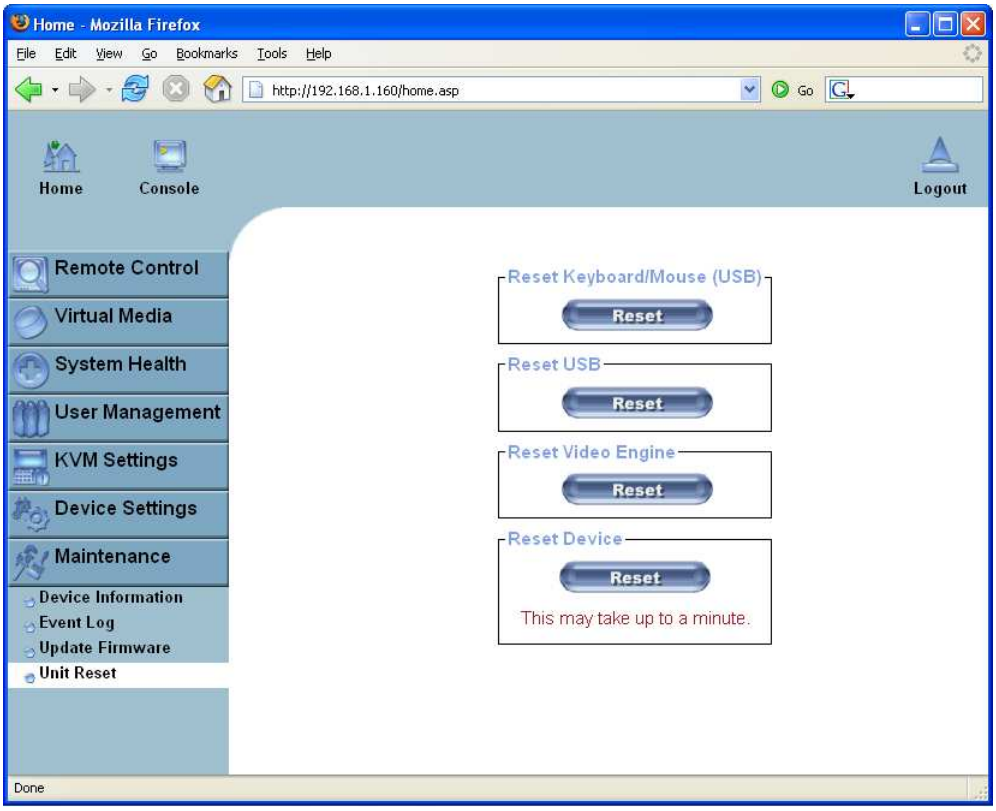
> **Warning**
>
> This process is not reversible and might take several minutes. Make sure the ASMI module's power supply will not be interrupted during the update process because this may result in an unusable device.

3. Finally, after the firmware has been stored, the ASMI module will be 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 the complete consistency check make mistakes during the firmware update almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the ASMI module's power supply will not be interrupted!

Unit Reset

Figure 6-40. Unit Reset



This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the ASMI 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 takes about half a minute. Resetting subdevices (e.g. video engine) will take mere seconds only and does not result in connections being closed.

To reset a certain ASMI module function click on the desired "Reset" button as displayed in Figure 6-40.

Note: Only the super-user "super" is allowed to reset the ASMI module.

Appendix A. Frequently Asked Questions

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 ASMI G4 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 ASMI G4 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 the KVM protocol) 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 ASMI G4 module and your host, then you may not be able to transfer the video data using a KVM protocol. Establish a direct connection between the ASMI G4 module and the client.

Furthermore, check the settings of the ASMI G4 module and choose a different server port used for KVM 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 ASMI G4 module and your client.

6. No connection can be established to the ASMI G4 module.

Have a look on your hardware. Is the ASMI G4 module attached to a power supply? Verify your network configuration (IP address, router). You may send a "ping" request to the ASMI G4 module to find out whether the ASMI G4 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 ASMI G4 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 ASMI G4 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 ASMI G4 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 ASMI G4 module. Refer to
the Section called *Remote Console Control Bar* in Chapter 5 for further explanation.

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.

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 particular specification that covers the style of motherboards and enclosure introduced by Raritan in 1995.

DHCP

Dynamic Host Configuration Protocol

A protocol for dynamically assigning IP configurations 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. 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 ASMI G4 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 to the ASMI 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 ASMI G4. 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 (ASMI 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, "ASMI at Server3" is used. And type the IP address of the ASMI 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 ASMI module. (Note: please memorize this secret, as the same secret will be requested for the configuration of RADIUS function on ASMI 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. "ASMI 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 D. Key Codes

Table D-1 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 D-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 D-1. English (US) keyboard Layout, used for the key codes

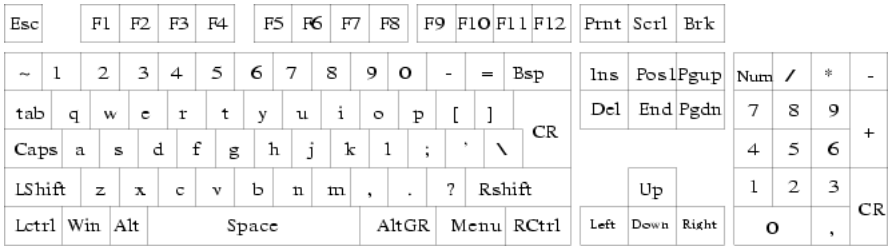


Table D-1. Key Names

Key	Alias Key(s)
0 - 9	
A - Z	
~	TILDE
_	MINUS
=	EQUALS
;	
’	
<	LESS
,	
.	
/	SLASH
BACKSPACE	
TAB	
[	
]	
ENTER	
CAPS LOCK	
\	BACK SLASH
LSHIFT	SHIFT

Key	Alias Key(s)
RCTRL	CTRL, STRG
RSHIFT	SHIFT
LCTRL	CTRL, STRG
LALT	ALT
SPACE	
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	

Key	Alias Key(s)
NUMPAD7	
NUMPAD8	
NUMPAD9	
NUMPADPLUS	NUMPAD_PLUS, +
NUMPAD /	/
NUMPADMUL	NUMPAD_MUL, x
NUMPADMINUS	NUMPAD_MINUS, -
NUMPADENTER	
WINDOWS	
MENU	

Appendix E. Specifications

Sizes and Weight

Table E-1. ASMI G4 Specification

Attribute	Value
Height	13mm
Width	173.4mm
Depth	64.4mm
Weight	110g (w/o replicator cable)
Power Consumption	up to 1A

Environment

Temperature

Table E-2. Temperature

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

Humidity Range

Table E-3. Humidity Range

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

Appendix F. Raritan Corp. Warranty Information

Limited Warranty

Raritan Corp. 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 G. 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 IMPLIED WARRANTIES 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 H. 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.