BELKIN®

OmniView® Remote IP Manager

Control

Control your computer or KVM switch through a web browser—from anywhere

EN

FR

DE

NL

ES

IT

User Manual

F1DE101Hea

BELKIN®

OmniView® Remote IP Manager

Control

Control your computer or KVM switch through a web browser—from anywhere

EN
FR
DE
NL
ES
IT

User Manual

F1DE101Hea

Table of Contents

Table of Contents

1-1 Introduction and Package Contents

Congratulations and thank you for purchasing this Belkin OmniView Remote IP Manager (RIPM). Designed to let businesses easily add KVM-over-IP technology to existing KVM and server configurations, the RIPM offers an efficient way to dramatically reduce server downtime and service costs. Administrators can now troubleshoot faster via round-the-clock remote access from anywhere.

The RIPM sets up easily to work with your existing Local Area Network (LAN), large or small. Consult this User Manual for all the details you'll need to install and operate the RIPM, and for expert troubleshooting advice in the unlikely event of a problem. We appreciate your business and are confident that you will soon see for yourself why over 1 million Belkin OmniView products are in use worldwide.


OmniView Remote IP Manager


PS/2 Cable Kit


VGA Cable


DB9 Null Cable


Mini-USB Cable


One 5V DC, 2A Power Supply


Rack-Mount Bracket with Screws


Software Installation CD


User Manual


Quick Installation Guide

Registration Card

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:32:52 AM

- **Remote Access**
  The RIPM provides remote access to your KVM configuration and all connected servers. It also sets up to provide remote access to an individual computer or server.

- **Digital Users**
  The RIPM allows one digital user to access and control connected KVM switches and servers. It also enables an additional 25 users to simultaneously view digital video for collaborative troubleshooting.

- **Web-Browser Based**
  The RIPM's interface is web-browser-based; any computer can access it, as long as it is connected to the LAN, WAN, or Internet over a standard TCP/IP connection. Setup requires no additional software.

- **User-Friendly Interface**
  The user-friendly interface allows you to set up and change the RIPM's functions quickly and easily through your web browser, without having to install additional software onto your computer.

- **BIOS-Level Access**
  The RIPM allows you to access the basic input/output system (BIOS) of your servers to make adjustments and perform reboots.

- **Serial Device Support**
  The RIPM provides support for one serial device, such as a power distribution unit (PDU), so you can perform hard reboots of your servers remotely.

- **Enhanced Security**
  The RIPM provides 256-bit SSL encryption and multi-user password protection to prevent unauthorized access to your servers.

- **Virtual Media***
  With virtual-media capability, you can transfer images and files between local and remote computers, remotely load software, perform application and operating-system patches, and perform diagnostic testing from a CD.

  *Available on Windows®-based computers only.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:32:53 AM

- **Account Management**
  The RIPM allows the administrator to create multiple user accounts and control access to servers.
- **Event Log**
  The Event Log captures and stores all user activity on the RIPM.
- **Email Notification**
  The RIPM enables the administrator to monitor user activity and sends email notification of logins, invalid logins, and logouts.
- **Multiple Platform Support**
  The RIPM works with KVM switches or servers with PS/2 or USB console connections.
- **Video Resolution**
  With a 117MHz bandwidth, the RIPM is able to support video resolutions of up to 1600x1200@75Hz.
- **0U Rack-Mountable**
  The RIPM is compact enough to be positioned on your desktop or mounted on the back of your server rack for 0U installation.
- **Firmware Updates**
  Flash upgrades allow you to obtain the latest firmware updates for your RIPM. These firmware updates ensure that the RIPM is compatible with the latest devices and hardware and are free for the life of the RIPM. Visit www.belkin.com for upgrade information and support.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:32:53 AM

Hardware Requirements

- OmniView Series Remote IP Manager (included)
- PS/2 Cable Kit (included)
- VGA Cable (included)
- Mini-USB Cable (included)
- 5V DC, 2A Power Supply (included)
- Keyboard, monitor, and mouse
- Connection to network using 10/100Base-T Ethernet port (RJ45)
- CAT5 cable
- Rack-mount bracket with screws (included in box for rack-mount-install option)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:32:53 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x and above;
UNIX®; Mac OS® X v10.0 and above (requires KVM);
Sun™ Solaris™ 8.x and above (with Sun adapter—Belkin part# F1DE083)

Browsers Supported

- Microsoft® Internet Explorer 6.0 and above
- Netscape® Navigator® 7.0

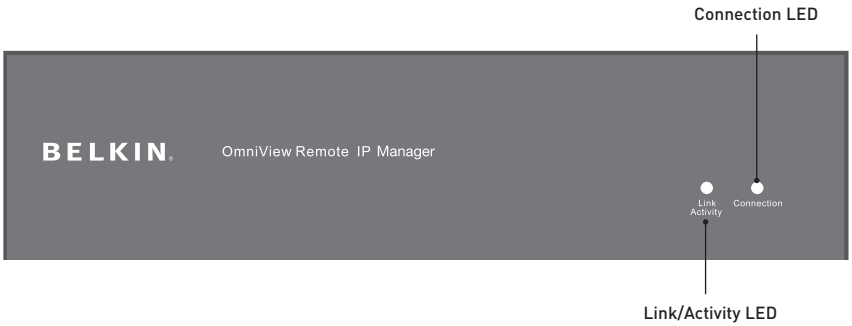
P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:32:53 AM

Part Number:	F1DE101H
Power:	5V DC, 2A
No. of Users Supported:	1 local, 1 digital (1 simultaneous user)
Keyboard Emulation:	PS/2 and USB
Mouse Emulation:	PS/2 and USB
Monitors Supported:	CRT and LCD (with VGA support)
Resolution Support:	Up to 1600x1200@75Hz
Maximum Remote Bandwidth:	5MB
Keyboard Input:	MiniDIN6 (PS/2)
Mouse Input:	MiniDIN6 (PS/2)
Monitor Port:	HDDB15 female (VGA)
CPU USB Port:	Mini USB
Network Connection:	RJ45
Encryption Modes:	256-bit SSL, 128-bit, AES, DES, 3DES
Authentication Support:	LDAP (via local LDAP client), RADIUS, AD
Protocol Support:	SNMP v1, IPv4
Serial Device Port:	DB9
LED Indicators:	2
Enclosure:	Metal
Dimensions:	6.75 (W) x 1.75 (H) x 4.5 (L) in. (171 x 44 x 114mm)
Weight:	1.65 lbs. (0.75kg.)
Operating Temp:	32° F to 120° F (0° C to 48.89° C)
Storage Temp:	-4° F to 140° F (-20° C to 60° C)
Humidity:	5% to 80%
Warranty:	2 years

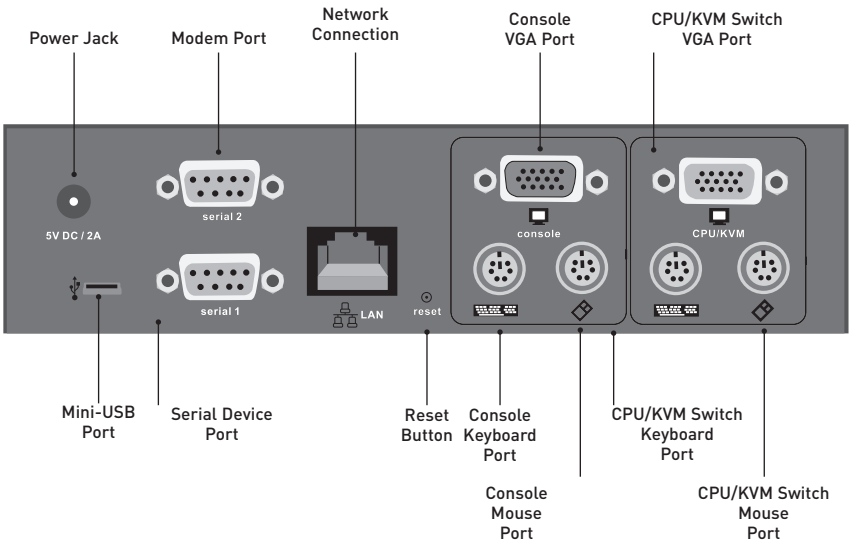
Note: Specifications are subject to change without notice.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:32:53 AM

Front of Unit

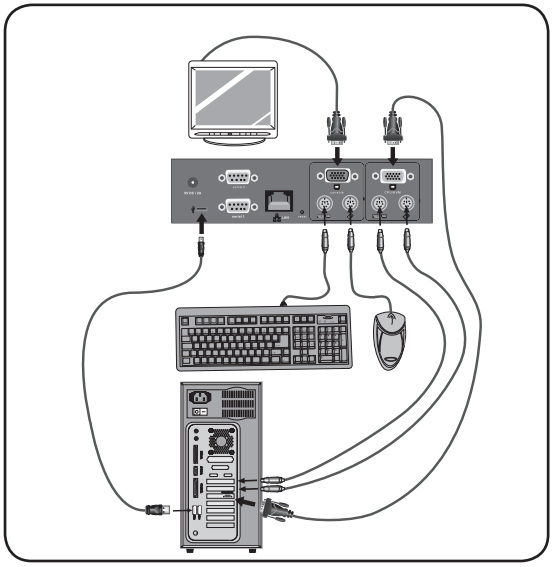


Back of Unit

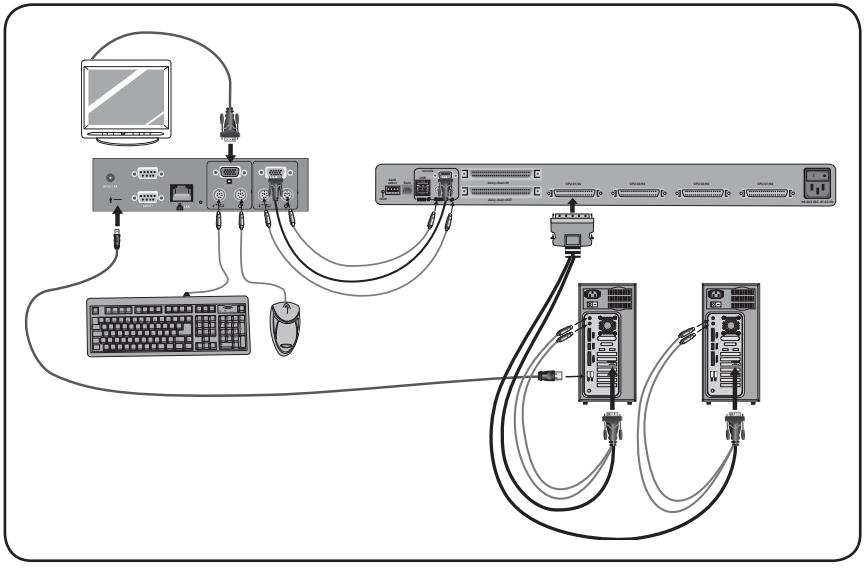


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:32:54 AM

Typical RIPM Configuration with a Computer



Typical RIPM Configuration with a KVM Switch



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:32:58 AM

Step 1 | Installing the RIPM into a Server Rack

The RIPM includes mounting brackets for installation in 19-inch racks.

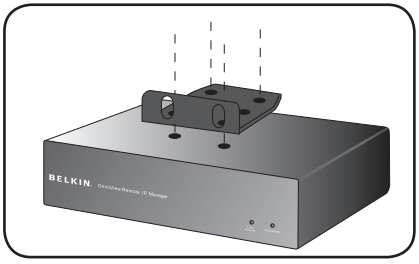


Fig. 1

1.1 Attach the included bracket to the top or bottom of the RIPM with the provided screws.

1.2 Mount the RIPM to the rack. See **Fig. 1.**

Note: Mounting screws for the rack are not included. Please use the specified screws from your rack's manufacturer.

Warning: Before attempting to connect anything to the RIPM or your computer(s), please ensure that all your computer equipment and devices are powered off. Belkin Corporation is not responsible for damage caused by your failure to do so.

Step 2 | Connecting your Console to the RIPM

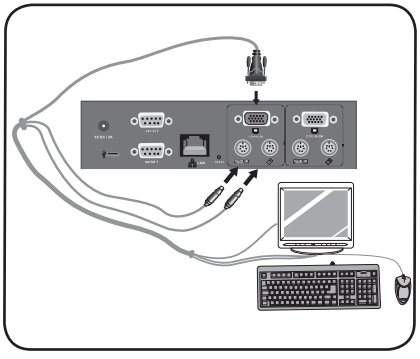


Fig. 2

2.1 Connect your keyboard and mouse to the "Console" keyboard and mouse ports on the RIPM.

2.2 Connect your monitor to the "Console" VGA port on the RIPM. See **Fig. 2.**

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:33:02 AM

Step 3 | Option 1: Connecting the RIPM to a KVM Switch (Host System)

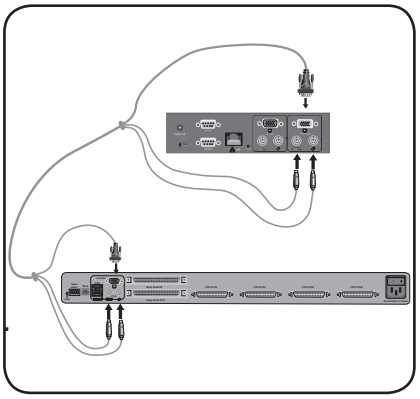


Fig. 3

3.1 Power down the KVM switch.

3.2 Using the provided PS/2 and VGA cable kit, connect one end to the “CPU/KVM switch” monitor, keyboard, and mouse ports on the RIPM. See **Fig. 3.**

3.3 Connect the other end to the monitor, keyboard, and mouse ports on your KVM switch.

Step 3 | Option 2: Connecting the RIPM to a Computer (Host System)

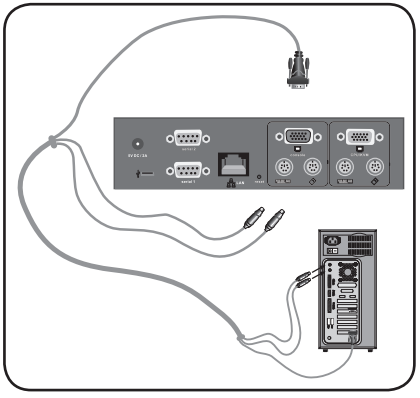


Fig. 4

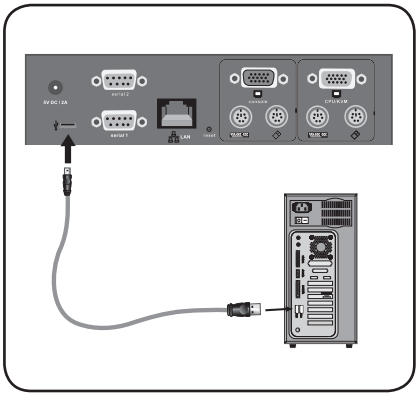
3.1 Power down the computer.

3.2 Using the provided PS/2 and VGA cables, connect one end to the “CPU/KVM switch” monitor, keyboard, and mouse ports on the RIPM. See **Fig. 4.**

3.3 Connect the other end to the monitor, keyboard, and mouse ports on your computer.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:33:03 AM

Step 4 | Connecting the Mini-USB Cable to Support Virtual Media



4.1 Power down the computer.

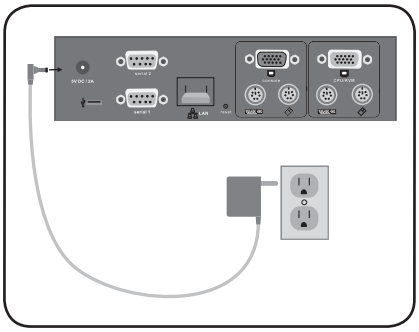
4.2 Using the provided mini-USB cable, connect one end to the mini-USB port on the RIPM and the other end to an available USB port on your computer. See **Fig. 5.**

Fig. 5

Note: You can connect any computer running the Windows OS to the RIPM to support virtual media—the computer does not need to be the host system.

Note: If your computer is NOT running Windows, you do not need to do the above setup.

Step 5 | Powering Up the RIPM



5.1 Connect the provided power supply into an available power outlet.

5.2 Connect the barrel plug into the power jack on the RIPM. See **Fig. 6.**

5.3 Turn on your KVM switch or computer.

Fig 6

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:33:05 AM

There are two ways to set up and configure the RIPM. You can use the device-setup software provided on the CD enclosed in the box, or you can connect a serial interface cable to the RIPM and use terminal software (e.g., HyperTerminal®).

Note: Belkin recommends using the device-setup software provided.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:33:06 AM

Device-Setup Software

The software contained on the enclosed CD will help to configure the RIPM to your network so that you can access it remotely.

1. Connect the RIPM to your computer via local network. Start the setup tool from the CD-ROM on the computer where the RIPM is installed.
2. Follow the setup wizard to configure the RIPM. You will need to have the IP address, subnet mask, and gateway information that will be assigned to the RIPM. You may need to get this information from your network administrator. When the configuration has been completed, you will receive a “successful” notification. Your RIPM is now configured and can be accessed.
3. This CD-ROM also contains the software that is needed to transfer files between the local and remote computers. This will be covered in more detail in the “Virtual Media” section of this User Manual.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:33:06 AM

To configure the RIPM via serial interface, a null modem cable is required (provided). Connect the null modem cable to the “Serial 01” port on the RIPM and the other end to the serial port on the computer. The serial interface needs to be adjusted with the parameters as shown below:

Parameter	Value
Bits/second	115200
Data bits	8
Parity	no
Stop bits	1
Flow control	none

Use a terminal software program (e.g., HyperTerminal) to connect to the RIPM. Reset the RIPM and immediately press the “ESC” key. You will see a “=>” prompt. Enter the command “config” and press the “ENTER” key. You will be asked to adjust the IP auto configuration, the IP address, the net mask, and the default gateway. Pressing the “ENTER” key without entering values does not change settings. The gateway value has to be set to “0.0.0.0” (for no gateway) or any other value for the IP address of the gateway. After the confirmation, the RIPM performs a reset using the new values as set before.

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:33:06 AM

Web Interface

The RIPM 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 RIPM into your web browser. The initial login settings are:

Parameter	Value
Login	administrator
Password	belkin

Changing these settings to user-specific values is strongly recommended and can be done on the “User Management” page.

Telnet

A standard Telnet client can be used to access an arbitrary device connected to the RIPM serial port via a terminal mode.

The primary interface of the RIPM is the HTTP interface. In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

For an unsecured connection to the RIPM, we can recommend the following web browsers:

- Microsoft Internet Explorer version 5.0 or higher on Windows 2000 and XP
- Netscape Navigator 7.0 on Windows 2000 and XP

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 ensured by using a 128-bit key length.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:33:07 AM

Open your web browser. Type in the address of your RIPM that you configured during the installation process. For this, you can use an IP address or a host and domain name, in the event that you have given your RIPM a symbolic name in the Domain Name Server (DNS).

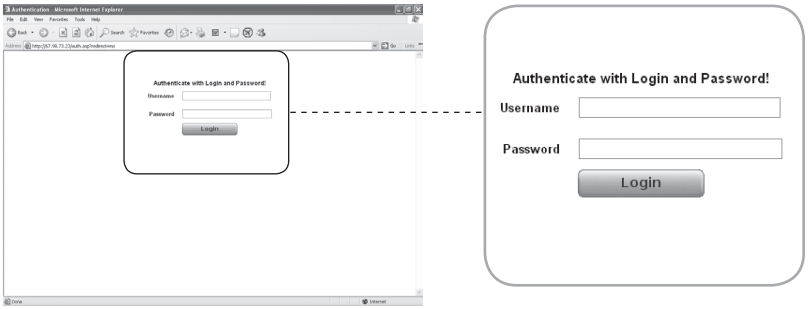
For example, type the following into the address line of your web browser when establishing an unsecured connection:

http://192.168.1.22/

When using a secure connection, type in:

http://192.168.1.22/

This will lead you to the RIPM login page as shown below:



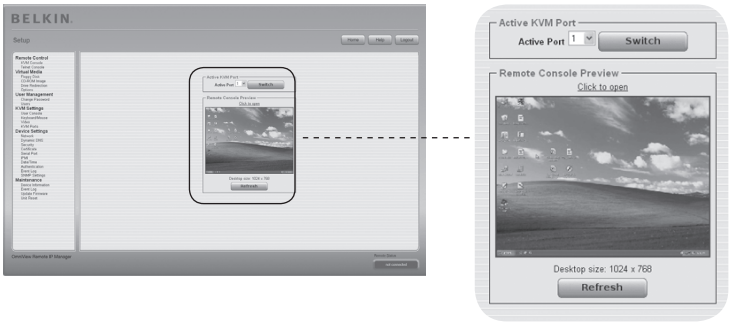
The RIPM has a built-in administrator account that has all permissions to administrate your RIPM:

Parameter	Value
Login	administrator
Password	belkin

Note: Your web browser has to be able to accept cookies; otherwise, login is not possible.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:33:07 AM

The Remote Console is the redirected screen, keyboard, and mouse of the remote host system in which the RIPM is installed. The web browser that is used for accessing the RIPM must supply a Java Runtime Environment version 1.1 or higher. However, it is strongly recommended that you install Sun JVM (Java Virtual Machine) 1.4. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system; you can use the keyboard and mouse as usual. Open the Remote Console by selecting the preview picture on the main site of the HTML front end.



Some of the available menu options include:

Auto-Adjust Button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the RIPM adjusts itself for the best possible video quality.

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.

Video Settings in Options Menu

This opens a new window with elements to control the RIPM video settings. You can change some values, for instance, those related to brightness and contrast of the picture displayed, and this may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

Note: At first boot, if the local mouse pointer is not synchronized with the remote mouse pointer, press the “Auto-Adjust” button once.

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:33:08 AM

Between the RIPM and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2 (available separately). The correct operation of the remote mouse depends on several settings, which will be discussed in the following subsections.

Remote IP Manager USB Interface

To use the USB interface, you need to use correct cabling between the managed host and the managing device. For example, if the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only, then you will have no remote-keyboard access during the boot process of the host. Please see the “Keyboard/Mouse” section on page 48.

Remote IP Manager Keyboard Settings

The RIPM settings for the host’s keyboard type must be correct in order to make the remote keyboard work properly. Check the settings in the RIPM front end. See the “Keyboard/Mouse” section on page 48.

Remote-Mouse Settings

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

- **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 translates the mouse movements from the Remote Console in such a way that one pixel move will lead to pixel moves on the remote system. This parameter 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 Modes**
  This mode is described in the “Single- and Double-Mouse Modes” section on page 20.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:33:08 AM

Auto-Mouse-Speed and Mouse Synchronization

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

- **Fast Sync**
  The fast sync is used to correct a temporary but fixed skew. Choose this option from the Remote Console Options menu. If defined, you may also press the mouse-synchronization hot-key sequence (see the "Remote Console Control Bar" section on page 23).

- **Intelligent Sync**
  If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent sync instead. This method adjusts the parameters for the actual movement of the mouse pointer so that the mouse pointer is displayed at the correct position on the screen. This method takes more time than the fast sync and can be accessed with the appropriate item in the Remote Console Options menu. The intelligent sync requires a correctly adjusted picture. Use the auto-adjustment function or the manual correction in the Video Settings panel to set up the picture. The shape of the mouse pointer has a significant influence on the pointer detection. Belkin recommends that you 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 figure out in the transferred video picture. Using a standard mouse-pointer shape ensures that the detection process is rather simple, and that the synchronization is at its best.

The "Mouse" button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually, pressing this button leads to a fast sync, except in situations where the video mode has recently changed. See also the "Remote Console Control Bar" section on page 23.

Note: At first startup, if the local-mouse pointer is not synchronized with the remote-mouse pointer, press the "Auto-Adjust" button once.

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:33:08 AM

Host System Mouse Settings

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

While the RIPM works with accelerated mice and is able to synchronize the local- with the remote-mouse pointer, the following limitations may prevent this synchronization from working properly:

- **Special Mouse Driver**
  There are mouse drivers that influence the synchronization process and lead to de-synchronized 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 has a setting named "improve mouse acceleration" that must 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 could also disable the Active Desktop completely.

  Navigate your mouse pointer into the upper-left corner of the applet screen and move it slightly back and forth. This will re-synchronize the mouse. If re-synchronizing fails, disable the mouse acceleration and repeat the procedure.

- **Single- and Double-Mouse Modes**
  The information above applies to the double-mouse mode where remote- and local-mouse pointers are visible and need to be synchronized. The RIPM features another mode, the single-mouse mode, where only the remote-mouse pointer is visible. Activate this mode in the Remote Console (see the "Remote Console Control Bar" section on page 23) 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 hot key in the Remote Console Settings panel. Press this key to free the captured local-mouse pointer.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:33:08 AM

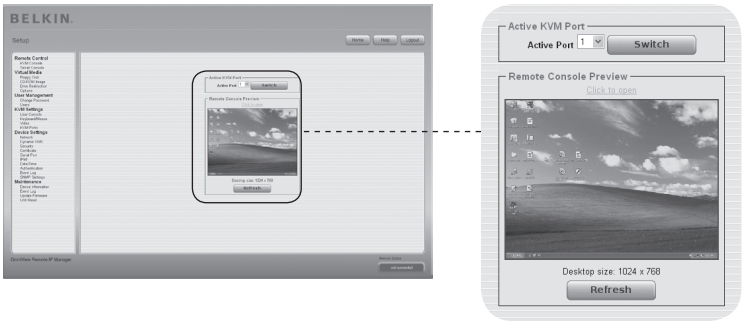
Recommended Mouse Settings

Windows 2000, 2003, XP (all versions)	In general, Belkin recommends the usage of a mouse via USB. Choose USB without mouse sync.
Mac OS X	Belkin recommends using the single-mouse mode.
Sun Solaris	Adjust the mouse settings either via “xset m 1” or by using the CDE Control Panel to set the mouse to “1:1, no acceleration”. As an alternative, you may also use the single-mouse mode.
Linux	First, choose the option “Other Operating Systems” from the “Mouse Type” selection box. Second, choose the option “Auto Mouse Speed”. This applies for both USB and PS/2 mice.

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:33:08 AM

Navigation

Once you have logged into the RIPM successfully, the main page of the RIPM appears. This page consists of three parts, each of them containing specific information. The buttons on the top allow you to navigate within the front end (see Table for details). The lower-left frame contains a navigation bar that allows you to switch between the different sections of the RIPM. Task-specific information, which depends on the section you have chosen before, is displayed within the right frame.



Note: If there is no activity for 30 minutes, the RIPM automatically logs you out. A click on one of the links will bring you back to the login screen.

P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:33:09 AM

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

- **Auto-Adjust Button**

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while the RIPM adjusts itself for the best possible video quality.

- **Sync Mouse**

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

- **Single-/Double-Mouse Modes**

Choose this mode to switch 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 must be synchronized). Single-mouse mode is available only if using Sun JVM 1.4 or higher.

- **Options**

To open the Options menu, click on the “Options” button.

A short description of the options follows:

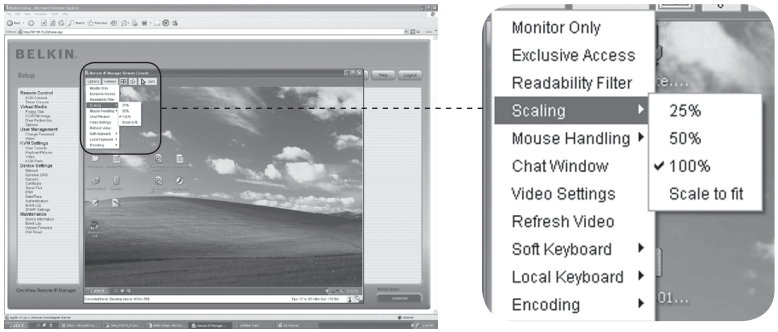
- **Monitor Only**
  Toggles the “Monitor Only” filter on or off. If the filter is switched on, no Remote Console interaction is possible, but monitoring is possible.

- **Exclusive Access**
  With appropriate permission, you can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until you disable the exclusive access or log off.

P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:33:09 AM

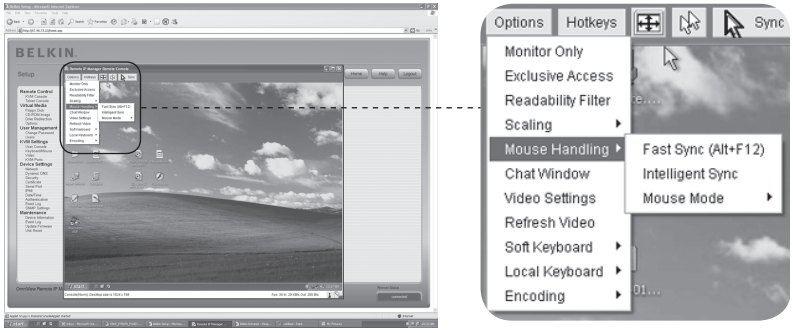
- **Scaling**

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



- **Mouse Handling**

  The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer as explained in the “Mouse, Keyboard, and Video Configuration” section.



- **Fast Sync**

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

- **Intelligent Sync**

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

  Warning: This method takes more time than fast sync and requires a correctly adjusted picture. To set up the picture, you may use either the auto-adjustment function or the manual correction in the Video Settings panel.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:33:10 AM

- **Local Cursor**

  Offers a list of different cursor shapes from which to choose 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 (JVM)—versions 1.2 and higher offer the full list.

- **Video Settings**

  Opens a panel for changing the RIPM video settings. The RIPM features two different dialogs that influence the video settings.

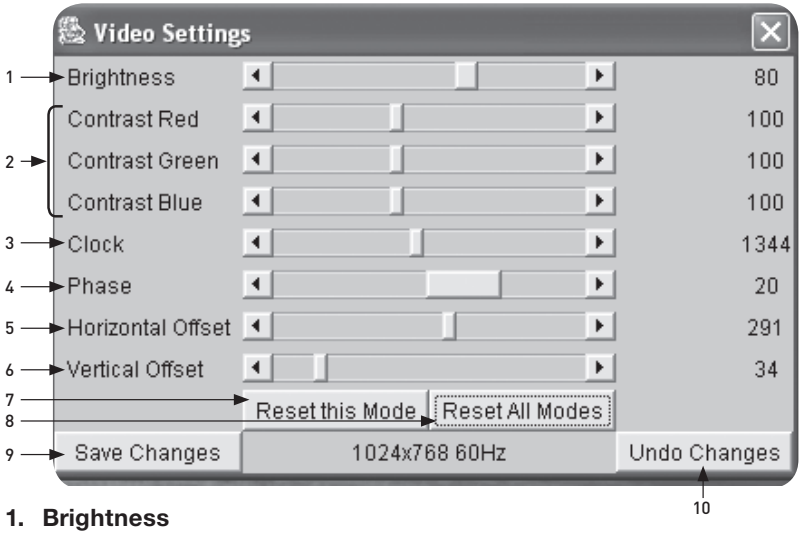
- **Video Settings through the HTML Front End**

  Select this option to enable the local video port. This option determines whether the local video output of the RIPM is active and passing through the incoming signal from the host system.

  The “Noise Filter” option defines how the RIPM reacts to small changes in the video-input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video-input signal). The default setting should be suitable for most situations.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:33:11 AM

Video Settings through the Remote Console



1. **Brightness**
   Controls the brightness of the picture.
2. **Contrast**
   Controls the contrast sharpness of the picture.
3. **Clock**
   Defines the horizontal frequency for a video line and depends on the video mode. Different video-card types may require different values here. The default settings in conjunction with the auto-adjustment procedure should be adequate for all common configurations. To achieve a better picture quality, you may try to change this setting together with the sampling phase.
4. **Phase**
   Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.
5. **Horizontal Offset**
   Allows you to use the left and right buttons to move the picture in a horizontal direction while this option is selected.
6. **Vertical Offset**
   Allows you to use the left and right buttons to move the picture in a vertical direction while this option is selected.
7. **Reset this Mode**
   Resets this specific mode's settings to the factory-made defaults.
8. **Reset all Modes**
   Resets all settings to the factory-made defaults.
9. **Save Changes**
   Saves changes permanently.
10. **Undo Changes**
    Restores last settings.

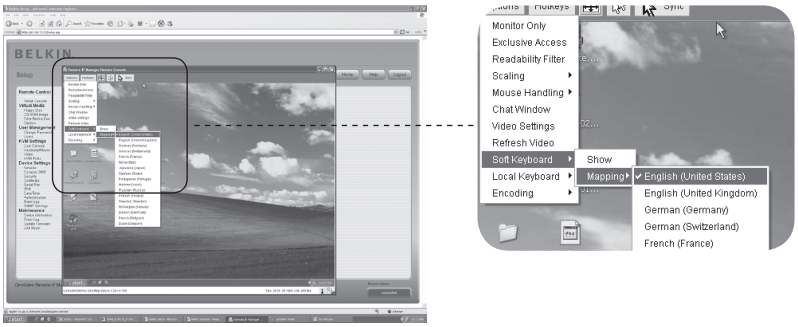
P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:33:11 AM

Mapping Sequence

Soft Keyboard
Opens up the menu for the soft keyboard.

Show
Pops up the soft keyboard. The soft keyboard is necessary in the event that your host system runs a completely different language and country mapping than your administration machine.

Mapping
Used for choosing the appropriate language and country mapping of the soft keyboard.



P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:33:11 AM

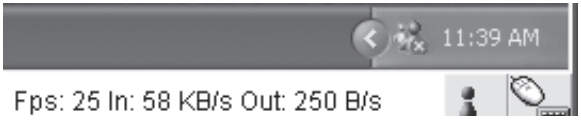
Local Keyboard
Used to change the language mapping of your browser machine running the Remote Console applet. Normally, the applet automatically determines the correct value. However, depending on your particular JVM and your browser settings, this is not always possible. A typical example is a German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

Hot Keys
Opens a list of predefined hot keys. Choose one entry and the command will be sent to the host system. You can add a confirmation dialog that will be displayed before the selected command is sent to the remote host. Select “OK” to perform the command on the remote host.

P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:33:12 AM

The status line shows both the Remote Console and the connection state. The size of the remote screen is displayed on the left. The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption; “SSL” indicates a secure connection using SSL.

Both the incoming (“In:”) and the outgoing (“Out:”) network traffic are displayed in kilobytes per second. If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.



The next button displays the Remote Console Access settings.

One or more users are connected to the Remote Console of the RIPM.

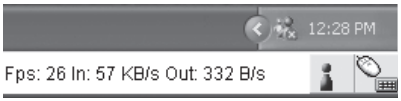
Exclusive access is set for you. Any other user may not access the remote host via the Remote Console unless you disable this option.

P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:33:12 AM

A remote user has exclusive access. You may not access the remote host via the Remote Console unless the other user disables this option.

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

The “Monitor Only” option disabled.



The “Monitor Only” option is enabled.

For more information about Monitor Only and Exclusive Access settings, see the “Remote Console Control Bar” section on page 23 of this User Manual.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:33:13 AM

Resetting the Remote IP Manager to Factory Settings

To reset the RIPM and change the network settings back to the factory defaults:

1. Make a serial connection for initial configuration (HyperTerminal)

Bits per second:	115200
Data bits:	8
Parity:	none
Stop bits:	1
Flow control:	hardware or none

2. Press the reset button, located between the power DC jack and the network jack. Release the reset button and immediately press the ESC key in the serial terminal program (HyperTerminal) several times until the prompt "=>" appears.

   Note: If the prompt does not come up within the first three seconds after releasing the reset button, repeat Steps 1 and 2. The RIPM will detect the ESC key only during the first three seconds of the boot process.

3. When prompted, type "defaults" and press the enter key. The RIPM will then boot and reset back to the factory settings.
4. Power down your server (the computer to which the RIPM is locally connected).
5. Unplug the power supply from the RIPM as well as the "CPU/KVM switch" port cables and the network cable.
6. Reconnect the cables and power up your server.

Now you can reconfigure the RIPM to your network settings through a HyperTerminal connection, or by using the setup software.

Logout of the Remote IP Manager

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

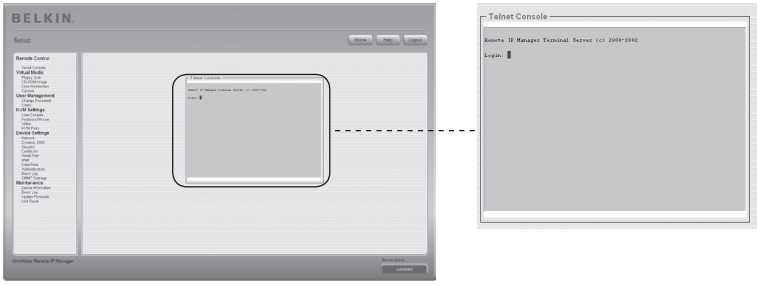
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:33:13 AM

KVM Console

Remote Console Preview

To open the KVM console, click on the menu entry on the left or on the console picture on the right. To refresh the picture, click the “Refresh” button.

Telnet Console



The RIPM firmware features a Telnet gateway that enables a user to connect to the RIPM via a standard Telnet client. To connect to the RIPM via Telnet protocol, you may use a terminal program such as xterm, TeraTerm, or PuTTY. As an alternative, you may also enter the Telnet command on the command line or use the “Run” dialog from the Windows Start menu. As an example, you may type the following sequence:

Telnet: 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:33:14 AM

Replace the IP address with the one that was assigned to the RIPM during installation. You will then be prompted for the username and password information in order to log in to the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means the user management of the Telnet interface is entirely controlled with the appropriate functions of the web interface. Once you have successfully logged in to the RIPM, a command line will be presented and you can enter the appropriate management commands. In general, the Telnet interface supports two operation modes: the command-line mode and the terminal mode. The command-line mode is used to control or display some parameters. In terminal mode, the pass-through access to serial port 1 is activated (if the serial settings were made correctly). To access the RIPM via serial interface, a null modem cable is required. All inputs are redirected to the device on serial port 1, and its answers are displayed on the Telnet interface.

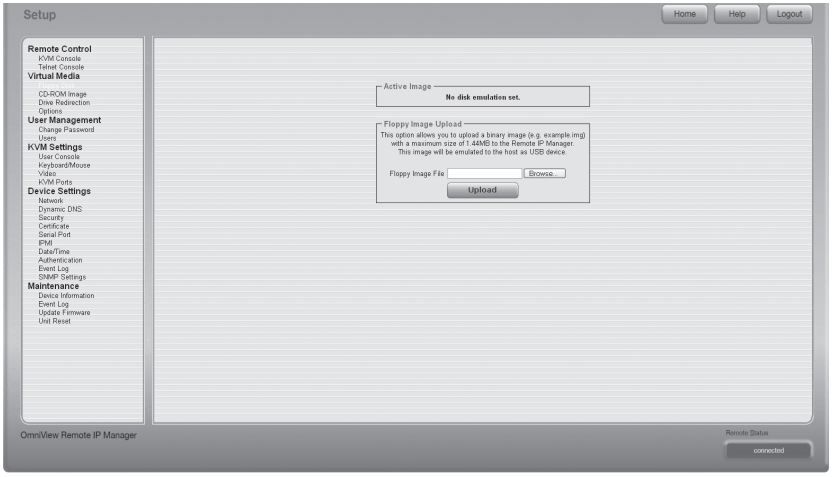
The following list shows the command syntax and usage.

Help	Displays the list of possible commands.
cls	Clears the screen.
quit	Exits the current session and disconnects from the client.
version	Displays the release information.
terminal	Starts the terminal pass-through mode for serial port 1. The key sequence “esc exit” switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for pass-through access.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:33:14 AM

Floppy Disk



This feature is for uploading and transferring image files. This option allows you to upload a binary image (example.img) with a maximum size of 1.44MB to the RIPM. This image will be emulated to the host as a USB device. All other formats need to be transferred using the drive-redirection feature. To use a larger image, mount this image using a Windows Share.

Upload a Floppy Image

Step 1: Click “Browse” to specify the file to be transferred.

Step 2: Click “Upload” to upload the file to the RIPM. You will receive a message confirming that the file has been successfully uploaded to the RIPM.

Step 3: Click on “KVM Console” in the Remote Console section of the RIPM interface to access the desktop of the remote computer.

Step 4: Double-click on the My Computer icon to open its folder.

Step 5: A second entry for the floppy drive will be listed in My Computer. This entry is called “3-1⁄2 Floppy (B)”. You can access the files you have transferred here.

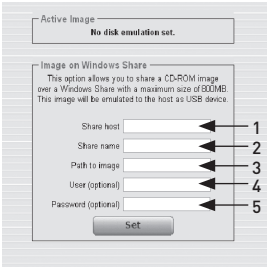
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:33:15 AM

CD-ROM Image

Use Image on Windows Share (SAMBA).

To include an image from a Windows Share, select “CD-ROM” from the submenu.

You must provide the following information in order to mount the selected image properly:



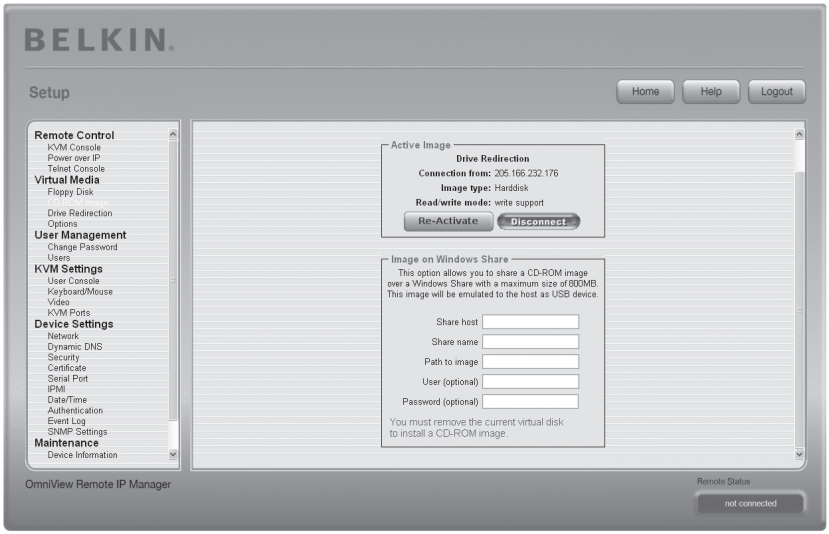
1. **Share Host**
   The server name or its IP address. (This IP address is obtained by running the drive-redirection software—explained below.)
2. **Share Name**
   The name of the share folder to be used.
3. **Path to Image**
   The path of the image file on the share.
4. **User (Optional)**
   If necessary, specify the username for the share. If unspecified and a guest account is activated, this guest-account information will be used as your login.
5. **Password (Optional)**
   If requested to supply a password, specify the password for the given username.

P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:33:15 AM

Upload a CD-ROM Image

Step 1: Open and run the drive-redirection software.

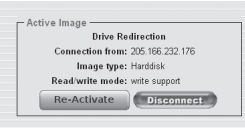
Step 2: When the drive-redirection software has connected, leave this window open and go to the CD-ROM image in the Virtual Media section of the RIPM interface.



Note: The IP address listed under “Connection From” is the IP address that is used as the share host address. To verify that the IP address assigned by the drive-redirection software is correct, connect the serial cable between the RIPM and the computer and open a hyperterminal session. Log in as “ping” and type the IP address exactly as it is in the “Share host” field. You should receive the output “<IP> is alive!”

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:33:15 AM

Step 3: Click “Re-Activate” in the Active Image section.



Step 4: Enter the IP Address provided by the drive re-direction software into the “Share Host “ field.

Step 5: Enter the “Share name” and the “Path to Image.”

Step 6: To upload the file, click the “Set” button. The file will be displayed as a USB device on the remote computer.

The specified image file should be accessible from the RIPM. The information above must be given from the point of view of the RIPM. It is important to specify correct IP addresses and device names. Otherwise, the RIPM may not be able to access the referenced image file properly and will leave the given file un-mounted (displays an error message instead). Belkin recommends that you use the correct values and repeat this step, if necessary.

The specified share must be configured correctly. Therefore, administrative permissions are required. As an ordinary user, you may not have these permissions. You should either log in as a system administrator or ask your system administrator for help to complete this task.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:33:15 AM

Drive Redirection

The drive-redirection feature provides another way to use a virtual disc drive on the remote computer. You can work with a drive on your local computer from the remote machine by sharing the drive over a TCP network connection. Storage devices including floppy and hard discs*, CD-ROMs, and removable media, such as USB sticks, can be redirected. You can even configure your remote machine to be able to write data to a local disc.

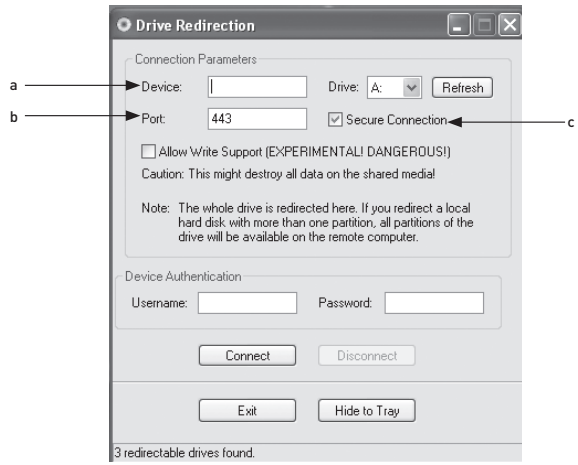
***Note:** Belkin does not recommend enabling write support when redirecting hard disks and is not responsible for data lost or corrupted during this process.

Please exercise caution when using this feature. Drive redirection works on a level that is far below the operating system, so that neither the local nor the remote operating system can detect that a drive is being redirected at a given time. This can create inconsistent data when one of the operating systems (on either the local machine or the remote host) writes data to the device. With write support enabled, the remote computer can damage data and the file system on the redirected device. If, on the other hand, the local operating system writes data to the redirected device, the drive cache on the remote host's operating system could contain older data, confusing the remote host's operating system. We therefore recommend using drive redirection, especially the write-support function, with great care.

Note: To be able to use the drive-redirection feature, you must install the drive-redirection software, which was included with this product, on the computer you are using to access the RIPM remotely.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:33:16 AM

1. **Open the drive-redirection application.**



2. **Specify the parameters of the network connection.**
   - **a. Device**
     This is the IP address of the RIPM to which you would like to connect.
   - **b. Port**
     This is the network port. By default, the RIPM uses the remote console port (#443). You may change this value if you have changed the remote console port in your RIPM's network settings.
   - **c. Secure Connection**
     Enable this box to establish a secure connection via SSL. This maximizes security; however, it might reduce connection speed.
3. **Select the drive you would like to redirect.** All available devices (drive letters) are shown. Please note that the RIPM shares the whole drive, not just one partition, with the remote computer. If you have a hard disc with more than one partition, all drive letters that belong to it will be redirected. Use the "Refresh" button to regenerate the list of drive letters, especially for a USB stick.
4. **Write Support**

   Warning: Use this feature with caution. Write support allows the remote computer to write to your local drive. If both the remote and the local systems try to write data to the same device simultaneously, **the file system on the drive will be destroyed.** Please use this feature only when you are completely confident that you can to do so safely.

   Note: Belkin does not recommend enabling write support when redirecting hard disks and is not responsible for data lost or corrupted during this process.
5. **Authenticate the device.** To use drive redirection, you must authenticate on the RIPM using a valid username and password. You will require permission to change the virtual disc configuration.

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:33:16 AM

6. **Establish drive redirection by pressing the "Connect" button once.** If all the settings are correct, the status bar displays that the connection has been established, the "Connect" button is disabled, and the "Disconnect" button is enabled. In the event of an error, the status line shows the error message.

   The drive-redirection software tries to lock the local drive before it is redirected. This prevents the local operating system from accessing the drive as long as it is redirected. The attempt will fail if a file on the drive is currently open. In the case of a locking failure, you will be prompted to confirm that you wish to establish the connection. However, remember that if write support is enabled, drive redirection could damage a drive that is not locked.
7. Use the "Disconnect" button to stop a drive redirection after the process has started.
8. Click "Exit" to shut down the drive-redirection program. If a drive-redirection connection is active, the connection will close before the application terminates.
9. Use the "Hide to Tray" button to minimize the application without terminating it completely. An active connection will remain until you close the application. You can access the software by double-clicking on its tray icon. The tray icon also indicates whether or not a connection is established. Right-click on it to access a submenu.

Options

Disable Drive Redirection
This switches off drive redirection.

Force Read-Only Connections
This switches off write support for drive redirection.

Click "Apply" to submit your changes.

P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:33:16 AM

Creating an Image

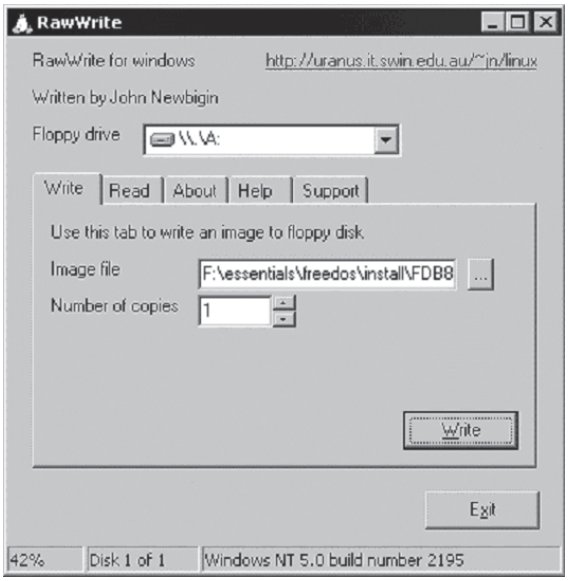
Floppy Images

UNIX® and UNIX-Like Operating Systems (OS)

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a floppy image file, copy the contents of a floppy to a file. You can use the following command: dd [if=/dev/fd0] [of=/tmp/floppy.image]. In this case, “dd” reads the entire disc from the device “/dev/fd0” and saves the output in the specified output file “/tmp/floppy.image”. Adjust both parameters exactly to your needs (input device, etc.).

MS Windows

You can use the tool “RawWrite for Windows”.



Select the “Read” tab from the menu. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the “Copy” button to initiate the image-creation process. For related tools, please see the home page of the “fdos project” **(http://www.fdos.org).**

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:33:16 AM

CD-ROM/ISO 9660 Images

UNIX and UNIX-Like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, Linux). To create a CD-ROM image, copy the contents of the CD-ROM to a file. You can use the following command:

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

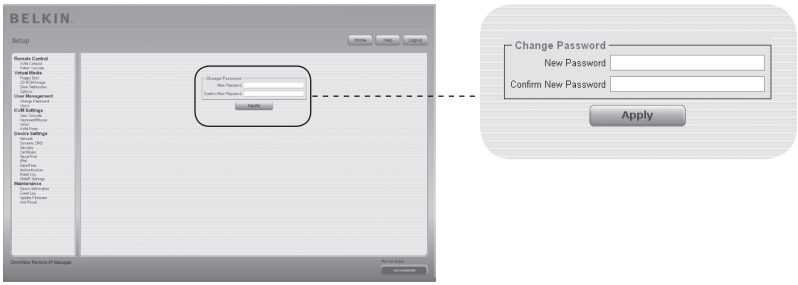
In this case, “dd” reads the entire disc from the device “/dev/cdrom” and saves the output in the specified output file “/tmp/cdrom.image”. Adjust both parameters exactly to your needs (input device, etc.).

MS Windows

To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single ISO image file on your hard disk. For example, with “Nero,” you choose “Copy and Backup”, and navigate to the “Copy Disc” section. Select the CD-ROM or DVD drive from which you would like to create an ISO image. Specify the file name of the ISO image and save the CD-ROM content in that file.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:33:16 AM

Change Password

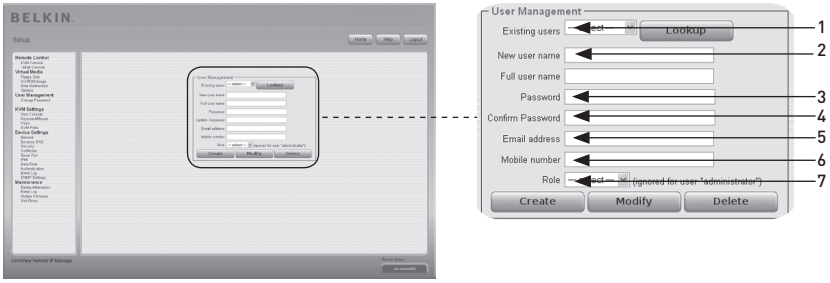


In order to change your password, enter the new password in the upper entry field. Retype the password in the field below.

Click “Apply” to submit your changes.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:33:17 AM

Users



User Management

The RIPM comes with a pre-configured user account for the administrator that has fixed permissions. This user has all possible rights to configure the device and to use all functions the RIPM offers. Upon delivery, the account for the user “administrator” has the password “belkin”. Make sure to change the password immediately after you have installed and accessed your RIPM for the first time. A full list of available options follows. This list can only be seen by the administrator.

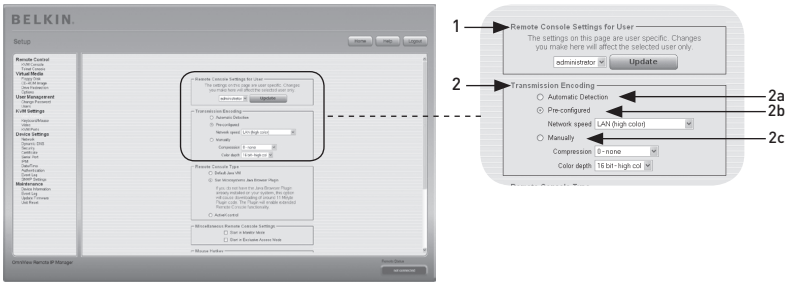
1. **Existing Users**
   Select an existing user for modification. Once a user has been selected, click the “lookup” button to see the user information.
2. **New Username**
   The new username for the selected account.
3. **Password**
   The password for the login name. It must be at least four characters long.
4. **Confirm Password**
   Confirmation of the password above.
5. **Email Address**
   This is optional.
6. **Mobile Number**
   This is also optional.
7. **Role**
   In addition to being an administrator or an ordinary user, each user can be a member of a group (named a “role”). Choose the desired role from the selection box.
   To create a new user, press the “Create” button. The “Modify” button changes the displayed user settings. To delete a user, press the “Delete” button.

   Note: The RIPM is equipped with a host-independent processor and memory unit, both of which have a limitation in terms of processing instructions and memory space. To guarantee an acceptable response
   time, Belkin recommends that you do NOT exceed a total of 25 users connected to the RIPM at the same time. The memory space that is available on the RIPM depends on the configuration and usage of the RIPM (log file entries, etc.).

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:33:17 AM

User Console

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



1. **Remote Console Settings for User**

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

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

2. **Transmission Encoding**

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

   2a. Automatic Detection

   Encoding and compression level are determined automatically from the available bandwidth and current content of the video image.

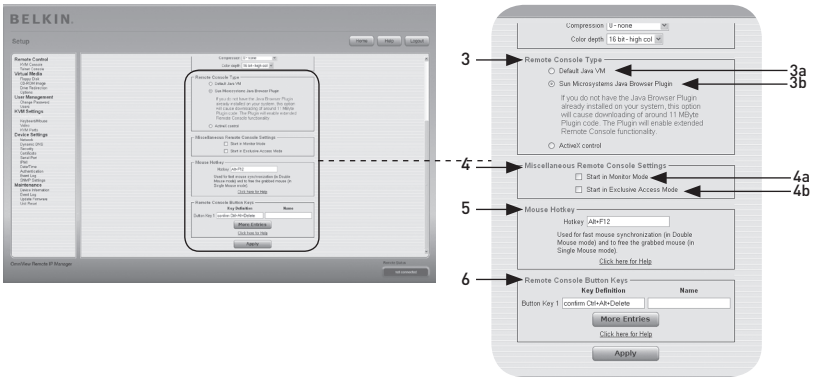
   2b. Pre-Configured Settings

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

   2c. Manual Configuration

   This allows you to adjust compression rate and color depth individually. Depending on the selected compression rate, the data stream between the RIPM 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 RIPM simultaneously. The standard color depth is 16-bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore, compression level 0 (no compression) uses only 16-bit color depth. At lower bandwidths, only 4-bit (16 colors) and 2-bit (four gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4-bit color depth. One-bit color depth (black/white) should be used only for extremely slow network connections.

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:33:18 AM



3. Remote Console Type
Specifies which Remote Console Viewer to use.

3a. Default Java Virtual Machine (JVM)
This function uses the default JVM of your web browser, either the Microsoft JVM for Internet Explorer or the Sun JVM.

3b. Sun Microsystems Java Browser Plug-In
This plug-in instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not yet installed on your system, it may be downloaded and installed automatically. However, in order to make the installation possible, you must answer the appropriate dialog prompts with “yes”. The download volume is approximately 11Mbps. The advantage of downloading Sun’s JVM is that it provides 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 it.

4. Miscellaneous Remote Console Settings

4a. Start in Monitor Mode
This setting lets you select the initial value for the monitor mode. By default, the monitor mode is disabled. If you switch it on, the Remote Console window starts in read-only mode.

4b. Start in Exclusive-Access Mode
This enables the exclusive-access mode at Remote Console startup. Using this mode forces the Remote Consoles of all other users to close. No other users will be able to open the Remote Console simultaneously again until you either disable this feature or log off.

5. Mouse Hot Key
The mouse hot key lets you specify a hot-key combination either to start the mouse-synchronization process (by entering the combination on the Remote Console) or to leave the single-mouse mode.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:33:19 AM

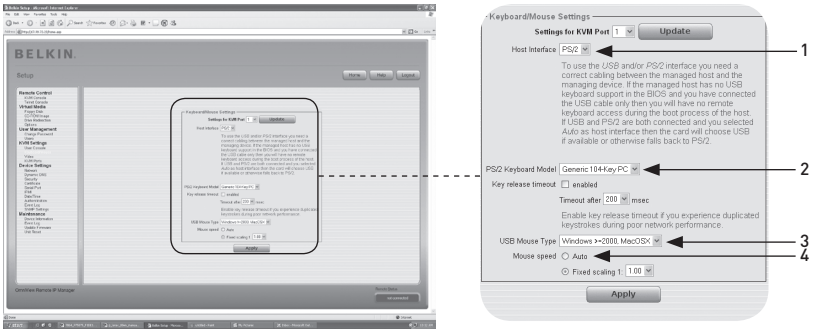
6. **Remote Console Button Keys**
   The button keys allow simulating keystrokes on the remote system that cannot be generated locally. This might be necessary if there is a key missing or if the local operating system of the Remote Console is unconditionally catching a keystroke. Typical examples are “Control+Alt+Delete” on Windows and DOS, which are always caught, or the key sequence “Control+Backspace” on Linux, which can be used for terminating the X server. In order to define a new button key, or to adjust an existing one, refer to the rules that describe the setting for a key. In general, the syntax for a key is as follows:

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

   A term in brackets is optional. The star at the end means that you must add further keys as often as required for your case. The term “confirm” adds a confirmation dialogue that is displayed before the keystrokes can be sent to the remote host. The “keycode” is the key to be sent. Multiple key codes can be concatenated with a plus, a minus, or a “<” 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 such a case, all pressed keys will be released in reversed sequence. So, the minus sign builds single, separate key presses and key releases. The “<” sign releases the last key only. The star inserts a pause with a duration of 100 milliseconds. As an example, the key combination of Ctrl, Alt, and F2 is represented by the sequence “Ctrl+Alt+F2”.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:33:19 AM

Keyboard/Mouse



1. **Host Interface**
   The Host Interface enables the interface to which the mouse is connected. You can choose “Auto” for automatic detection, “USB” for a USB mouse, or “PS/2” for a PS/2 mouse.

   Note: To use the USB and/or PS/2 interface, you need to connect the correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable, you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you select “Auto” as Host Interface, USB will be selected on boot up if available. If USB is not available, “PS/2” will be selected

   To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

   - the host BIOS must have USB keyboard support
   - the USB cable must be connected or selected in the “Host Interface” option

2. **PS/2 Keyboard Model**
   This lets you choose a keyboard layout from among “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extended by three additional Windows keys, “Generic 106-Key PC” for a Japanese keyboard, and “Apple Macintosh” for the Macintosh® computer keyboard. If a keyboard time-out is required, select the appropriate option and set the desired time value in the input field below.

3. **USB Mouse Type**
   This enables the USB mouse type. Choose an appropriate option from the selection box. For a detailed description of the mouse type and recommended options for the different operating systems, please see the “Recommended Mouse Settings” section on page 21 of this User Manual.*

*This feature only works with Windows OS.

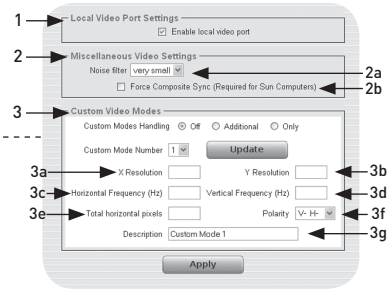
P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:33:19 AM

4. **Mouse Speed**
   - **Auto Mouse Speed**
     Use this option if the mouse settings on the host use an additional acceleration setting. The RIPM detects the acceleration and speed of the mouse during the mouse-sync process.
   - **Fixed Mouse Speed**
     Use this option for a direct translation of mouse movements between the local and the remote pointer. You may also set a fixed scaling that determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option works only when the mouse settings on the host are linear, i.e., when there is no mouse acceleration involved.

   To set the options, click the “Apply” button.

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:33:20 AM

Video



To set the options (see below), click the “Apply” button.

1. **Local Video Port Settings**

   Enable Local Video Port
   This option monitors the local video output of the RIPM, and indicates whether it is active and passing through the incoming signal from the host system.

2. **Miscellaneous Video Settings**

   2a. Noise Filter
   This feature defines how the RIPM reacts to small changes in the video-input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the
   video-input signal).

   2b. Force Composite Sync (Required for Sun Computers)
   To support signal transmission from a Sun machine, enable this option. If this function is not enabled, the picture of the Remote Console will not be visible.

3. **Custom Video Modes**
   The maximum number of custom video resolutions is four.

   The “Custom Modes Handling” option lets you disable custom modes (“Off”), or set standard or exclusive video resolutions (“Only”). A final option (“Additional”) allows you to force a special video mode for the RIPM. To change the parameters for custom video mode, choose the appropriate number from the selection box and press the “Update” button. You will be required to provide some additional information so that the video mode can be correctly recognized:

   Warning: The “Host Monitor Settings” option is for advanced users only. Using it incorrectly can damage video-transmission performance. Please be sure that you understand the feature thoroughly before attempting to adjust the Host Monitor Settings.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:33:20 AM

3a. X Resolution
This refers to the visible number of horizontal pixels.

3b. Y Resolution
This refers to the visible number of vertical pixels.

3c. Horizontal Frequency (Hz)
This refers to the horizontal (line) frequency in hertz.

3d. Vertical Frequency (Hz)
This refers to the vertical (refresh) frequency in hertz.

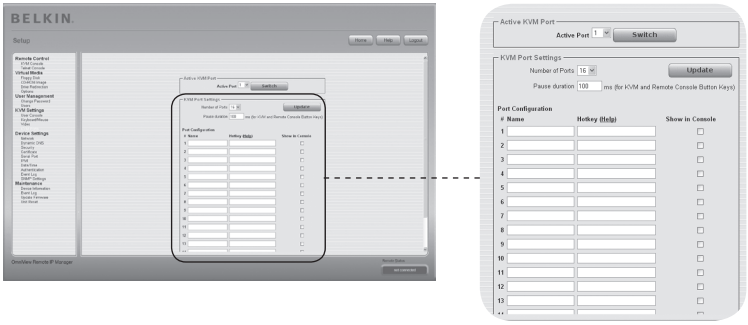
3e. Total horizontal pixels
This refers to the total number of pixels per line, including the non-visible and blanking area.

3f. Polarity
This refers to the positive or negative characteristic of the synchronization signals. V indicates vertical polarity; H indicates horizontal polarity.

3g. Description
Here you can provide a mode name, which is displayed in the Remote Console if custom mode is activated.

KVM Ports

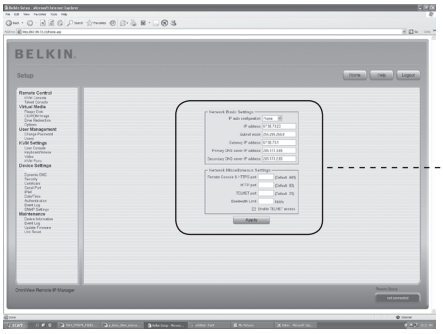
It is possible to select the number of ports used by the connected KVM switch, and you may assign each port a name. In order to provide KVM-port switching through the RIPM, key combinations have to be defined for the ports.

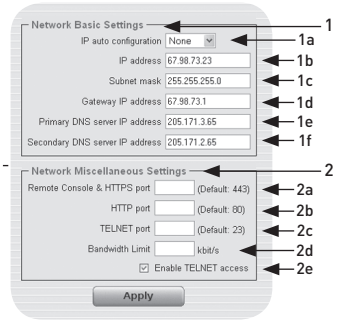


P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:33:21 AM

Network

The “Network Settings” panel (shown below) allows you to change network-related parameters, as explained below. Once applied, the new network settings take effect immediately.





Warning: Changing the network settings of the RIPM could result in a loss of network connection. If you change the settings remotely, be sure that all the values are correct so that you do not lose access to the RIPM.

1. **Basic Network Settings**

   1a. IP Auto Configuration
   With this option, you can define the location from which the RIPM takes its network settings—either a DHCP or BOOTP server. For DHCP, select “DHCP”; for BOOTP, select “bootp”. If you choose “none”, IP auto configuration is disabled.

   1b. The IP address is assigned by your network administrator.

   1c. The term **“Subnet Mask”** refers to the net mask of the local network, which is used to determine the subnet to which an IP address belongs.

   1d. Gateway IP Address
   If the RIPM must be accessible from networks other than the local one, set this IP address to the local network router’s IP address.

   1e. Primary DNS Server IP Address
   This is the IP address of the primary Domain Name Server (DNS) in dot notation. You can leave this option blank; however, if you do, the RIPM will not be able to perform name resolution.

   1f. Secondary DNS Server IP Address
   This term refers to the IP address of the secondary DNS in dot notation. It will be used in the event that the Primary DNS Server cannot be contacted.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:33:21 AM

2. Network Miscellaneous Settings

2a. Remote Console and HTTPS Port
This is the port number at which the RIPM's Remote Console server and HTTPS server are listening. If left empty, the default value will be used.

2b. HTTP Port
This is the port number at which the RIPM's HTTP server is listening. If left empty, the default value will be used.

2c. Telnet Port
This refers to the port number at which the RIPM's Telnet server is listening. If left empty, the default value will be used.

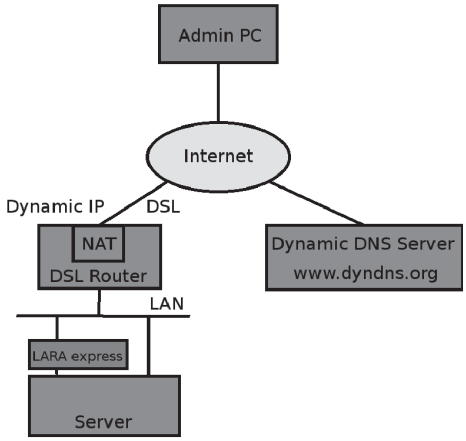
2d. Bandwidth Limit
This option refers to the maximum network traffic generated through the RIPM Ethernet device (value in Kbps).

2e. Enable Telnet Access
Set this option to allow users to access the RIPM using the Telnet gateway (see the "Telnet Console" section on page 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:33:21 AM

Dynamic DNS

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario:



Dynamic DNS Scenario

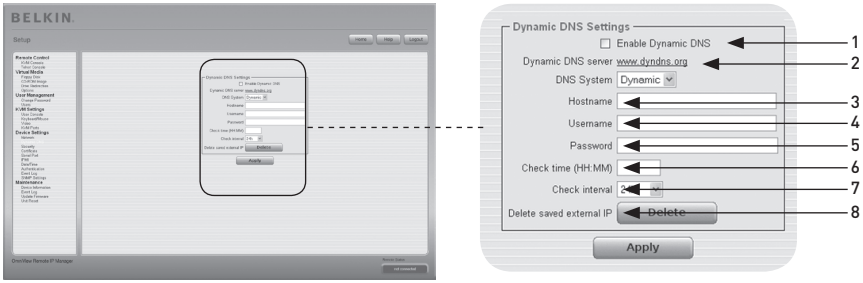
You can reach the RIPM via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the RIPM connects to a special dynamic DNS in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to the NIC. The administrator must register a RIPM to use the service with the dynamic DNS and assign a certain host name to it. A username and password will be assigned during the registration process. This account information together with the host name is needed in order to determine the IP address of the registered RIPM.

You must perform the following steps in order to enable dynamic DNS:

- Make sure that the LAN interface of the RIPM is properly configured.
- Enter the dynamic-DNS-settings-configuration dialog as shown on page 55.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:33:22 AM

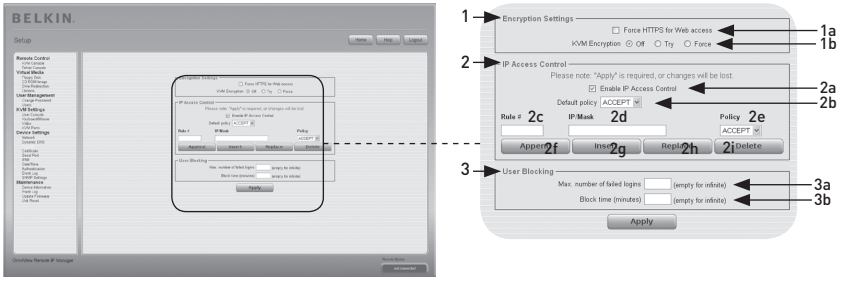
Dynamic DNS Settiings



1. **Enable Dynamic DNS**
   This enables the Dynamic DNS service. This requires a configured DNS server IP address.
2. **Dynamic DNS Server**
   The RIPM registers itself in regular intervals at this location. At the time of this publication, the dynamic DNS is a fixed setting since only dyndns.org is currently supported.
3. **Host Name**
   RIPM is the host name provided by the dynamic DNS. Use the whole name, including the domain, i.e., “testserver.dyndns.org” (or “RIPM.dyndns.org”), and not just the actual host name.
4. **Username**
   During your manual registration with the dynamic DNS, you must have registered this username.
   Note: Spaces are not allowed within the username.
5. **Password**
   During your manual registration with the dynamic DNS, you must have designated this password.
6. **Check Time**
   The RIPM card registers itself in the dynamic DNS at “Check Time”.
7. **Check Interval**
   This is the interval for reporting to the dynamic DNS by the RIPM.
   Note: The RIPM has its own independent real-time clock. Be careful to ensure that the time setting of the RIPM is correct.
8. Use the helpful option **“Delete saved external IP”** if you would like to update your externally saved IP address. To delete the saved address, press the “Delete” button.

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:33:22 AM

Security



1. Encryption Settings

1a. Force HTTPS

If this option is enabled, access to the Web front end is possible using a HTTPS connection only. The RIPM will not "listen" through the HTTP port for incoming connections. In the event that you want to create your own SSL certificate that can be used to identify the RIPM, please refer to the "Certificate" section on page 58.

1b. KVM Encryption

This option controls the encryption of the Remote Frame Buffer (RFB) protocol. The Remote Console uses RFB to transmit the screen data to the administrator machine, and keyboard/mouse data back to the host. If set to "Off", no encryption is used. If set to "Try", the applet attempts to make an encrypted connection. If the connection cannot be established, an unencrypted connection is used instead. If set to "Force", the applet attempts to make an encrypted connection. If the connection fails, the system generates an error report.

2. IP-Access Control

This section explains the settings related to IP-access control. It is used to limit access to a number of distinguished clients. These clients will be identified by the IP addresses from which they are trying to build connections.

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

2a. Enable IP-Access Control

Enables access control based on IP source addresses.

2b. Default Policy

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

Warning: If you set this to "DROP" and you have no "ACCEPT" rules configured, access to the Web front end over LAN is impossible. To re-enable access, you can change the security settings via modem or by temporarily disabling IP-access control with the initial configuration procedure.

2c. Rule Number

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

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:33:23 AM

2d. IP/Mask
Specifies the IP address or IP-address range for which the rule applies. In the following examples, the number concatenated to an IP address with a " / " represents the number of valid bits of the given IP address that will be used.

192.168.1.22/32 matches the IP address 192.168.1.22

192.168.1.0/24 matches all IP packets with source addresses from 192.168.1.0 to 192.168.1.255

0.0.0.0/0 matches any IP packet

2e. Policy
The policy determines what to do with matching packets. They can be either accepted or dropped.

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

2f. Appending a Rule
Enter the IP/mask and set the policy. Finally, press the "Append" button.

2g. Inserting a Rule
Enter the rule number and the IP/mask. Set the policy. Finally, press the "Insert" button

2h. Replacing a Rule
Enter the rule number and the IP/mask. Set the policy. Finally, press the "Replace" button.

2i. Deleting a Rule
Enter the rule number and press the "Delete" button.

3. User Blocking
The user-blocking mechanism allows the administrator to disable the login of a certain user if his or her password was entered incorrectly a specific number of times. The duration of the blocking is also configurable.

3a. Maximum Number of Failed Logins
Enter the maximum number of failed login attempts after which a user should be blocked. Leave this field empty to disable the user-blocking feature.

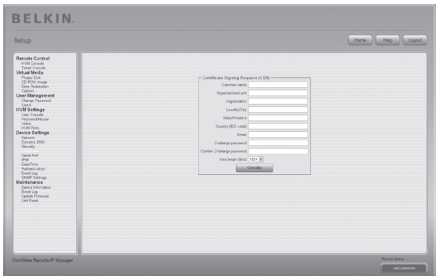
3b. Block Time
The number of minutes the user is blocked after he or she has exceeded the maximum number of failed login attempts. Leave this field empty to block this user until he or she is manually unblocked.

Unblocking Users
There are two possibilities to unblock a blocked user:

- A parent user may go to the user-management settings (see the "User Management" section) and press the "Unblock" button for the user.
- An administrator may use the serial console for the initial configuration and log in as the user "unblock". The RIPM will ask for the administrator password and present a list of blocked users who may be unblocked.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:33:23 AM

Certificate



Certificate Settings

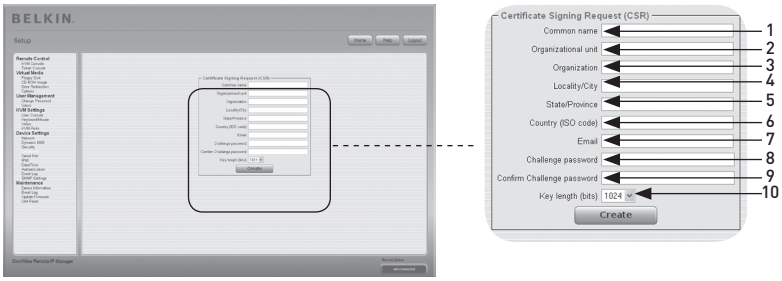
The RIPM uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment, the RIPM must expose its identity to a client using a cryptographic certificate. Upon delivery, this certificate and the underlying secret key will be the same for all RIPMs ever produced and will not match the network configuration that will be applied to the RIPM by its user. The certificate's underlying secret key is also used for securing the SSL handshake. It is possible to generate and install a new base64 x.509 certificate that is unique for a particular RIPM. In order to do that, the RIPM 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 CA verifies that you are who you claim to be and signs and issues to you an SSL certificate. To create and install an SSL certificate for the RIPM, do the following:

- Create an SSL CSR using the panel shown in the figure below. You need to fill out a number of fields, each of which is explained below. Once this is done, click on the "Create" button; this will initiate the CSR generation. The CSR can be downloaded to your administration machine with the "Download CSR" button.
- Send the saved CSR to a CA for certification. You will get the new certificate from the CA.
- Upload the certificate to the RIPM using the "Create" button.

After you have completed these three steps, the RIPM will have its own certificate that will identify the card to its clients.

Warning: If you destroy the CSR on the RIPM, there is no way to get it back. Should you delete it by mistake, repeat the three steps described above.

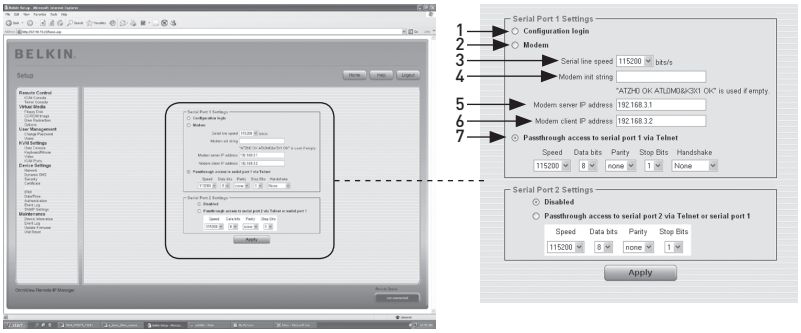
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:33:24 AM



1. **Common Name**
   This is the network name of the RIPM 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 RIPM with a web browser but without the prefix "http://". If the RIPM is accessed using HTTPS and the name given here and the actual network name are different, the browser will pop up a security warning.
2. **Organizational Unit**
   This field specifies to which department within an organization the RIPM belongs.
3. **Organization**
   The name of the organization to which the RIPM belongs.
4. **Locality/City**
   The city in which the organization is located.
5. **State/Province**
   The state or province in which the organization is located.
6. **Country (ISO Code)**
   The country in which the organization is located (a 2-letter ISO code, e.g., US for the United States).
7. **Challenge Password**
   Some certification authorities require a challenge password to authorize later changes on the certificate (e.g., revocation of the certificate). The minimum length of this password is four characters.
8. **Confirm Challenge Password**
   Requires you to reenter the challenge password.
9. **Email**
   This refers to the email address of a contact person who is responsible for the RIPM and its security.
10. **Key Length**
    This is the length of the generated key in bits. In most cases, 1,024 bits are sufficient. Longer keys may result in slower RIPM response time during connection establishment.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:33:24 AM

Serial Port



The RIPM Serial Settings allow you to specify which device is connected to the serial port and how to use it. To access the serial interface, a null modem cable is required.

1. **Configuration or Console Login**
   Do not use the serial port for any special function; use it only for the initial configuration.
2. **Modem**
   The RIPM offers remote access using a telephone line in addition to standard access over a built-in Ethernet adapter. The modem needs to be connected to the serial interface of the RIPM. Connecting to the RIPM using a telephone line means nothing other than building up a dedicated point-to-point connection from your console computer to the RIPM. In other words, the RIPM acts as an Internet Service Provider (ISP) into which you can dial. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the RIPM, make sure to configure your console computer accordingly. For instance, on Windows-based operating systems, you can configure a dial-up network connection that defaults to the correct settings (like PPP). The Modem Settings panel allows you to configure the remote access to the RIPM using a modem. The meaning of each parameter will be described below. The modem settings are part of the Serial Settings panel.
3. **Serial-Line Speed**
   The speed with which the RIPM is communicating with the modem. Most modems available today will support the default value of 115.200bps. If you are using an old modem and discovering problems, try to lower this speed.
4. **Modem Init String**
   The initialization string used by the RIPM to initialize the modem. The default value will work with all standard modems directly connected to a telephone line. If you have a special modem, or if your modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by using a new string. Refer to the section in your modem's manual about AT command syntax.

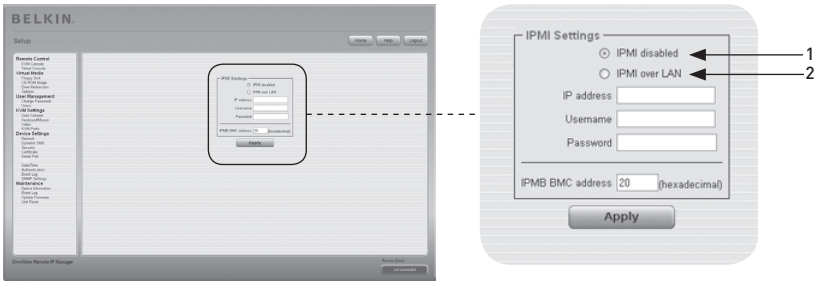
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:33:25 AM

5. **Modem Server IP Address**
   This IP address will be assigned to the RIPM itself during the PPP handshake. Since it is a point-to-point IP connection, virtually any IP address may be assigned, but you must make sure that it does not interfere with the IP settings of the RIPM and your console computer. The default value will work in most cases.
6. **Modem Client IP Address**
   This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection, virtually any IP address may be assigned, but you must make sure that the assigned IP is not interfering with the IP settings of the RIPM and your console computer. The default value will work in most cases.
7. **Pass-Through Access to Serial Port via Telnet**
   Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet console or a standard Telnet client to connect to the RIPM. For more information about the Telnet interface, refer to the “Telnet Console” section.

   Note: Check www.belkin.com for a list of compatible modems.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:33:25 AM

Intelligent Platform Management Interface (IPMI)



The RIPM IPMI facilities provide an additional way to power the system on or off or to perform a hard reset. Furthermore, these facilities allow you to view an event log of the host system and the status of some system sensors (e.g., temperature). If your host system supports IPMI, you can access it in one of the following ways:

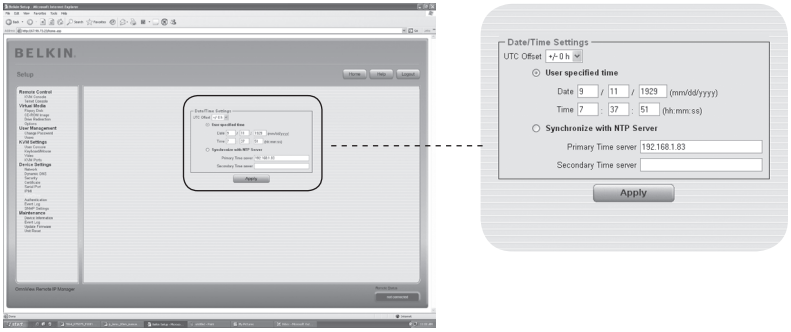
- IPMI over LAN (IPMI v1.5 is required)
- IPMI Settings

The figure above shows the RIPM IPMI settings panel. Its options will be explained below.

1. **IPMI Disabled**
   Disables IPMI on the RIPM. This means that Status via IPMI and Event Log via IPMI are not available; the power on/off and reset functions do not use IPMI rather than the ATX (Advanced Technology Extended), and the reset cable is connected from the RIPM to the motherboard.
2. **IPMI over LAN**
   You can also connect the IPMI over a LAN connection. The prerequisite for this access type is a host system with IPMI v1.5 and a network adapter with a side-band connection to the baseboard management controller (BMC) (mostly on board). In the IPMI settings, you must enter the IP address of this host system and the correct password for the LAN connection. You can also access other IPMI systems by entering their respective IP addresses.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:33:25 AM

Date and Time

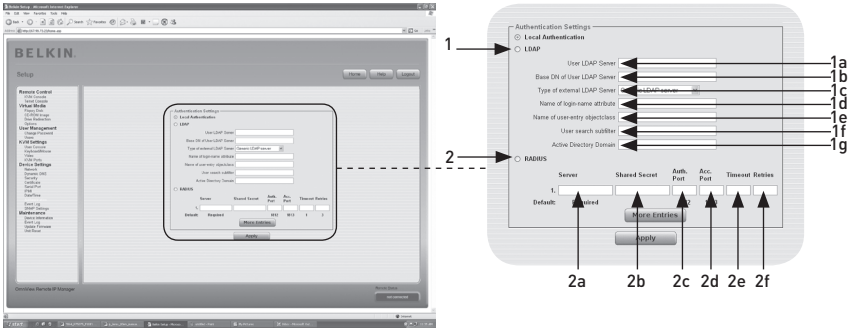


This link refers to a page where the internal real-time clock of the RIPM can be set up. You can adjust the clock manually or use a Network Time Protocol (NTP) time server. Without a time server, your time setting will not be persistent, so you must adjust it each time the RIPM loses power for more than a few minutes. To avoid this, you can use an NTP time server, which sets up the internal clock automatically to the current Coordinated Universal Time (CUT). Because NTP server time is always CUT, there is a setting that allows you to set up a static offset to get your local time.

Warning: There is currently no automatic way to adjust to daylight saving time. You must set up the CUT offset twice a year according to the local rules of your country.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:33:26 AM

Authentication



The RIPM lets you either use a local authentication or keep the information in a central Lightweight Directory Access Protocol (LDAP) or in a Remote Authentication Dial-In User Service (RADIUS) server. For LDAP or RADIUS, you must specify some information in the Authentication Settings panel. For more information regarding the LDAP and RADIUS settings, see below.

1. **LDAP**

   1a. User LDAP Server
   Enter the name or IP address of the LDAP server containing all the user entries. If you choose a name instead of an IP address, you need to configure a DNS server in the network settings.

   1b. Base DN of User LDAP Server
   Specify the distinguished name (DN) where the directory tree starts in the user LDAP server.

   1c. Type of External LDAP Server
   Set the type of the external LDAP server. This is necessary because some server types require special handling. Additionally, the default values for the LDAP scheme are set appropriately. You can choose between a Generic LDAP Server, a Novell Directory Service, and a Microsoft Active Directory. If you have neither a Novell Directory Service nor a Microsoft Active Directory, then choose a Generic LDAP Server and edit the LDAP scheme (see below).

   1d. 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.

   1e. 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.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:33:27 AM

1f. User Search Sub-Filter
Here you can refine the search for users that should be known to the RIPM.

1g. 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.

2. Remote Authentication Dial In User Service (RADIUS)
RADIUS 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 free RADIUS, open-RADIUS, or RADIUS on UNIX systems. The RADIUS protocol is well specified and tested. We can give a recommendation for all products listed above, especially for the free RADIUS implementation.

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

To access a remote device using the RADIUS protocol, you must log in. You will be asked to specify your username and password. The RADIUS server will read your input data (Authentication), and the RIPM will look 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 like the Remote Console. If there is no activity for half an hour, your connection to the RIPM will be interrupted and closed.

2a. Server
Enter either the IP address or the host name of the RADIUS server to be connected. If you are using the host name, DNS must be configured and enabled.

2b. Shared Secret
A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. The RIPM serves as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (i.e., to verify 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 and may contain both lowercase and uppercase letters (A–Z, a–z), numerals (0–9), and other symbols (characters not defined as letters or numerals), such as exclamation points (“ ! ”) or asterisks (“ * ”).

2c. Authentication Port
The port the RADIUS server listens to for authentication requests. The default value is #1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:33:27 AM

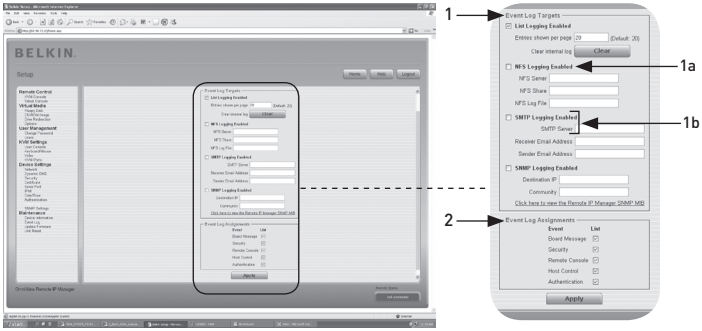
2d. Accounting Port
The port the RADIUS server listens to for accounting requests. The default value is #1813.

2e. Timeout
Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the request. If the request job is not completed within this interval of time, it is canceled. The default value is one second.

2f. Retries
Sets the number of retries if a request could not be completed. The default value is three times.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:33:27 AM

Event Log



Important events like a login failure or a firmware update are logged to a selection of logging destinations (see Figure 6-33). Each event belongs to an event group, which can be activated separately. The common way to log events is to use the internal log list of the RIPM. To show the log list, click on “Event Log” on the Maintenance page. In Event Log Settings, you can choose how many log entries are shown on each page. You can also clear the log file.

1. **Event Log Targets**
   To log events, you may use the internal log list of the RIPM. To show the log list, click on “Event Log” on the “Maintenance” page. Since the RIPM’s system memory is used to save all the information, the maximum number of log-list entries is restricted to 1,000 events. Every entry that exceeds this limit overrides the oldest one.

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

   1a. Network File System (NFS) Logging Enabled
   Define a NFS server to which directories and static links must be exported; all logging data will then be written to a file in that location. To write logging data from multiple RIPM devices to only one NFS share, you must define a file name that is unique for each device. When you change the NFS settings and press the “Apply” button, the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an
   error message.

   Note: In contrast to the internal log file on the RIPM, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so that it grows continuously. You may need to delete it or move away events logged within the file from time to time.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:33:27 AM

1b. SNMP Settings

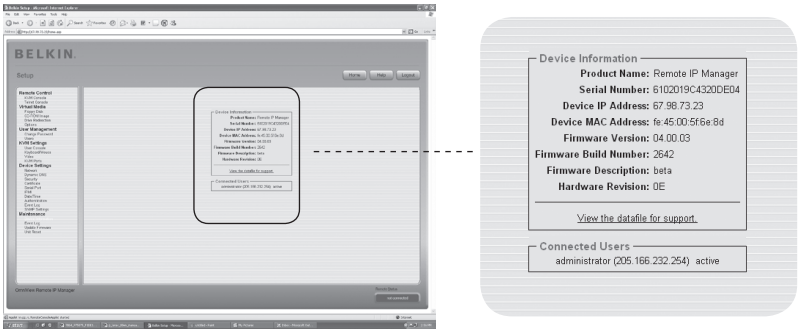
Simple Mail Transfer Protocol (SMTP) Logging Enabled
With this option, the RIPM is able to send email to an address entered into the email-address text field in Event Log Settings. These mails contain the same description strings as the internal log file, and the mail subject is filled with the event group of the occurred log event. In order to use this log destination, you must specify an SMTP server that is both reachable from the RIPM and needs no authentication (<serverip>:<port>).

SNMP Logging Enabled
If this is activated, the RIPM sends an SNMP trap to a specified IP address every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate field. Most of the event traps contain only one descriptive string that contains all information about the log event. Authentication and host power have their own standard trap, which they automatically create and which consists of several fields detailing information about the event. To receive this SNMP trap, use any SNMP trap listener.

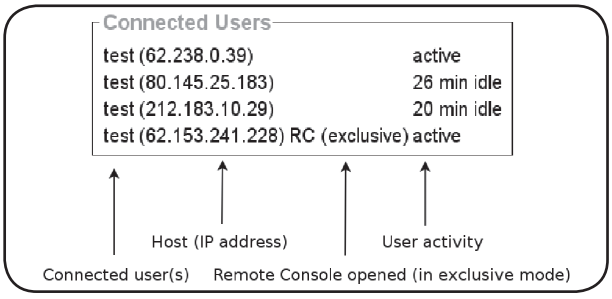
2. Event Log Assignments
You may choose which actions of the RIPM will be saved in the log file. Check the desired box(es) and click “Apply” to confirm your selection.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:33:27 AM

Device Information



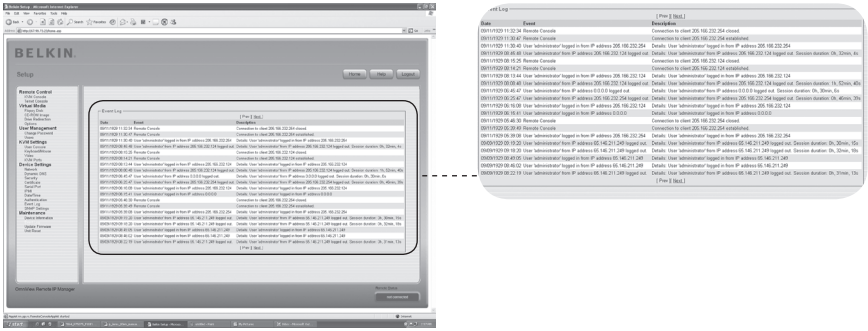
This section contains a summary of information about this RIPM and its current firmware and allows you to reset the RIPM. The data file for support allows you to download the RIPM data file with specific support information. This is an eXtensible Markup Language (XML) file with customized support information, e.g., the serial number.



The figure above displays RIPM activity. From left to right, the display shows the connected user(s), the host user's IP address, and the RIPM's activity status. "RC" means that the Remote Console is open. If the Remote Console is opened in "exclusive mode," the term "(exclusive mode)" is added. For more information about this option, see the "Remote Console Control Bar" section on page 23 of this User Manual. To display the user activity, the last column contains either the term "active" to indicate an active user or "20 min idle" to indicate a user who has been inactive for a certain amount of time.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:33:28 AM

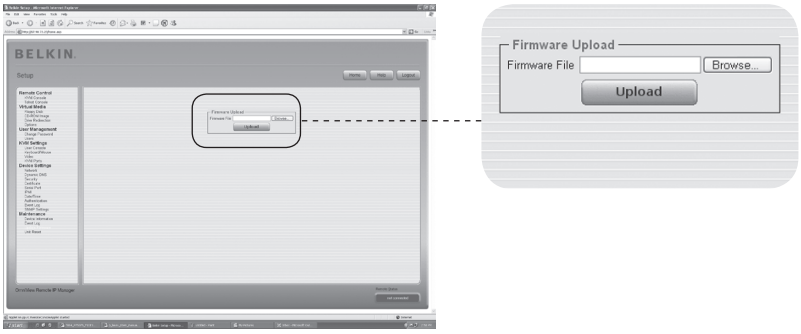
Event Log



The “Event Log” list includes the events that are kept by the RIPM, extended by the event date, a short event description, and an IP address indicating the origin of the event request. You may use the text buttons “Prev” and “Next” to browse the data.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:33:29 AM

Update Firmware



The RIPM is a complete standalone computer; it runs on software known as firmware, which is written onto its read-only memory (ROM). The RIPM's firmware can be updated remotely to install new or improved functionality or special features. A new firmware update is a binary file that must be downloaded from the Belkin website. If the firmware file is compressed (i.e., if the file suffix is .zip), you must unzip it before you can proceed. In the Windows operating system, you can use WinZip (located on the Web at http://www.winzip.com/) to decompress your firmware updates.

Note: To update the RIPM's firmware, you must save the new, uncompressed firmware file on the system that you connect to the RIPM.

Updating the firmware is a three-stage process:

1. Upload the new firmware file onto the RIPM. To do so, select the file on your local system using the "Browse" button on the "Upload Firmware" panel. Next, click "Upload" to transfer the previously selected file from your local file system onto the RIPM. Once the firmware file is uploaded, the RIPM will automatically verify its validity and confirm that no transmission errors have occurred. If an error does occur, the "Upload Firmware" function will be aborted and the current firmware will remain intact.

2. If the upload succeeds (as is likely to be the case), the "Update Firmware" panel will appear. The panel will display the version number of the firmware that is currently running and the version number of the uploaded firmware. Click "Update" to replace the old version with the new.

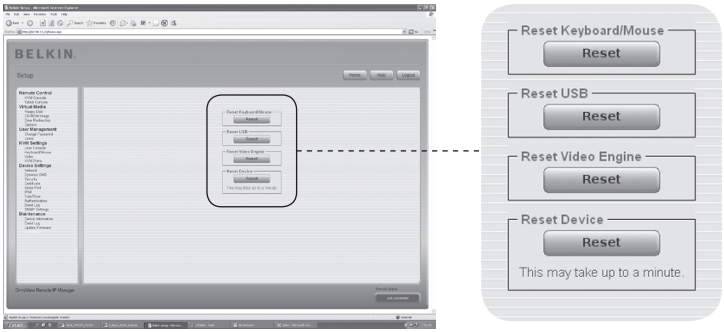
   Warning: This process is irreversible and usually takes several minutes. Please be sure that the RIPM's power supply will not be interrupted during the update process; a power disruption could cause the RIPM to become unstable.

3. After the firmware has been updated, the RIPM will reset automatically. After about one minute, you will be redirected to the login page to log in once again.

   Warning: The 3-stage firmware-update process and complete consistency check make updating the firmware virtually mistake-proof. However, only experienced staff members or administrators should perform a firmware update. It is critical that the power supply to the RIPM NOT be interrupted during the update process.

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:33:29 AM

Unit Reset



This section describes methods used to reset specific parts of the device. This involves the keyboard and mouse, the video display of the computer attached to the RIPM, and the RIPM itself. To activate newly updated firmware, you must reset the RIPM. This process automatically closes all current connections to the administration console and to the RIPM, and takes only about 30 seconds. Resetting sub-devices (e.g., the video engine) takes only a few seconds and does not result in closing connections. To reset a specific RIPM, click on the "Reset" button as shown in the image above.

Note: Only the administrator is allowed to reset the RIPM.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:33:30 AM

The remote mouse does not work or is not synchronous.

First, check the VGA connection. Both the RIPM and the local monitor must support the same video resolution. Make sure that your mouse settings match your mouse model, i.e., PS/2 or USB. Also, the mouse model must be set on both the RIPM and the host (the computer connected to the RIPM) operating system. In some circumstances, the mouse synchronization process can produce errors. Please refer to the “Mouse, Keyboard, and Video Configuration” section in Chapter 3 for further explanation.

The video quality is bad and/or grainy.

Use the menu entry “Reset” to set the RIPM to its default values. Then, click the “Auto-Adjust” button to select an appropriate video output. Check that the video cables are securely connected.

Login on the RIPM fails.

Verify both your user login and your password. The default username is “administrator”, and the default password is “belkin”. Make sure that your web browser is configured to accept cookies.

The RIPM’s Remote Console window does not open.

Verify that Java has been loaded. A firewall may prevent access to the Remote Console. The TCP ports #80 (for HTTP) and #443 (for both HTTPS and RFB) must be open (the server providing the firewall must accept incoming TCP connections on these ports).

The Remote Console is unable to connect and displays a time-out error.

Verify your hardware and network setup. If there is a proxy server between the RIPM and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the RIPM and the client. In addition, check the settings of the RIPM and choose a different server port for RFB transfer. If you use a firewall, check the appropriate port for accepting connections. You may restrict these connections to the IP addresses used by the RIPM and your client.

No connection can be established to the RIPM.

Inspect your hardware. Is the RIPM attached to a power supply? Verify your network configuration (IP address, router). Send a “ping” request to the RIPM to find out whether the RIPM is reachable via network.

Special key combinations (e.g., ALT+F2, ALT+F3) are intercepted by the console system and not transmitted to the host.

Define a so-called “button key”. This can be done in the Remote Console settings (see the “Remote Console Control Bar” section on page 23.

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:33:30 AM

The RIPM web pages are not displayed correctly.

Check your browser's cache settings. Make sure the cache settings are NOT set to "never check for newer pages". Under that setting, the RIPM pages could be loaded from your browser cache and not from the RIPM, which may be causing the problem.

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. Please consult the OS manual for additional information.

Every time I reopen the Remote Console dialog box, the mouse pointers are no longer synchronous.

Disable the setting "Automatically move mouse pointer to the default button of dialog boxes" in the mouse settings of your operating system.

The Remote Console remains black.

Check whether the RIPM is USB-powered only. If there is not enough power via USB, the Remote Console opens but remains black. Verify the RIPM settings on page 26 of this User Manual. Check that the video cables are securely connected.

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 RIPM. Refer to the "Remote Console Control Bar" section on page 23 of this User Manual.

I forgot my password. How can I reset the RIPM to factory defaults?

You can use the serial interface. For a detailed description, see the "Resetting the Remote IP Manager to Factory Settings" section on page 31 of this User Manual.

Please check www.belkin.com for additional troubleshooting and a list of hardware that is compatible with the RIPM.

Note: If any of these solutions do not remedy the situation, please call technical support at 1-800-2BELKIN.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:33:30 AM

FCC Statement

Declaration of Conformity with FCC Rules for Electromagnetic Compatibility

We, Belkin Corporation, of 501 West Walnut Street, Compton, CA 90220, declare under our sole responsibility that the product:

F1DE101H

to which this declaration relates:
Complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Declaration of Conformity
We, Belkin Corporation, declare under our sole responsibility that the product F1DE101H, to which this declaration relates, is in conformity with Emissions Standard EN55022 and with Immunity Standard EN55024, LVP EN61000-3-2, and EN61000-3-3.

ICES
This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme á la norme NMB-003 du Canada.

Belkin Corporation Limited 2-Year Product Warranty

What this warranty covers.
Belkin Corporation warrants to the original purchaser of this Belkin product that the product shall be free of defects in design, assembly, material, or workmanship.

What the period of coverage is.
Belkin Corporation warrants the Belkin product for two years.

What will we do to correct problems?
Product Warranty.
Belkin will repair or replace, at its option, any defective product free of charge (except for shipping charges for the product).

What is not covered by this warranty?
All above warranties are null and void if the Belkin product is not provided to Belkin Corporation for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin Corporation determines that the Belkin product has been improperly installed, altered in any way, or tampered with. The Belkin Product Warranty does not protect against acts of God (other than lightning) such as flood, earthquake, war, vandalism, theft, normal-use wear and tear, erosion, depletion, obsolescence, abuse, damage due to low voltage disturbances (i.e. brownouts or sags), non-authorized program, or system equipment modification or alteration.

How to get service.
To get service for your Belkin product you must take the following steps:

1. Contact Belkin Corporation at 501 W. Walnut St., Compton CA 90220, Attn: Customer Service, or call (800)-223-5546, within 15 days of the Occurrence. Be prepared to provide the following information:
   a. The part number of the Belkin product.
   b. Where you purchased the product.
   c. When you purchased the product.
   d. Copy of original receipt.
2. Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:33:30 AM

Belkin Corporation reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin Corporation for inspection shall be borne solely by the purchaser. If Belkin determines, in its sole discretion, that it is impractical to ship the damaged equipment to Belkin Corporation, Belkin may designate, in its sole discretion, an equipment repair facility to inspect and estimate the cost to repair such equipment. The cost, if any, of shipping the equipment to and from such repair facility and of such estimate shall be borne solely by the purchaser. Damaged equipment must remain available for inspection until the claim is finalized. Whenever claims are settled, Belkin Corporation reserves the right to be subrogated under any existing insurance policies the purchaser may have.

How state law relates to the warranty.
THIS WARRANTY CONTAINS THE SOLE WARRANTY OF BELKIN CORPORATION, THERE ARE NO OTHER WARRANTIES, EXPRESSED OR, EXCEPT AS REQUIRED BY LAW, IMPLIED, INCLUDING THE IMPLIED WARRANTY OR CONDITION OF QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND SUCH IMPLIED WARRANTIES, IF ANY, ARE LIMITED IN DURATION TO THE TERM OF THIS WARRANTY.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

IN NO EVENT SHALL BELKIN CORPORATION BE LIABLE FOR INCIDENTAL, SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL OR MULTIPLE DAMAGES SUCH AS, BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS ARISING OUT OF THE SALE OR USE OF ANY BELKIN PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This warranty gives you specific legal rights, and you may also have other rights, which may vary from state to state. Some states do not allow the exclusion or limitation of incidental, consequential, or other damages, so the above limitations may not apply to you.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:33:30 AM

BELKIN®

OmniView® Remote IP Manager

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, The Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spain
+34 9 16 25 80 00
+34 9 02 02 00 34 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, France
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH
Hanebergstrasse 2
80637 Munich, Germany
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

© 2006 Belkin Corporation. All rights reserved. All trade names are registered trademarks of respective manufacturers listed.
Mac OS and Macintosh are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

P75075ea

BELKIN®

Console IP de prise en main à distance OmniView®

Con-
trôlez

Commandez votre ordinateur ou votre switch KVM au moyen d'un navigateur Web – où que vous soyez

EN
FR
DE
NL
ES
IT

Manuel de l'utilisateur

F1DE101Hea

Table des matières

Table des matières

1-1 Introduction et contenu de l'emballage

Félicitations et merci d'avoir fait l'achat de la Console IP de prise en main à distance OmniView Belkin (la CIPD). Permettant aux entreprises d'ajouter la technologie KVM-sur-IP en toute simplicité à leur configuration de serveurs et KVM existantes, la CIPD réduit de façon significative les temps morts et les coûts. Les administrateurs peuvent procéder au dépannage du système rapidement grâce à un accès à distance, de partout et en tout temps.

la CIPD s'intègre aisément à votre réseau local (LAN) déjà en place, peu importe sa taille. Ce manuel de l'utilisateur contient toutes les informations nécessaires à l'installation et l'utilisation de la CIPD, ainsi qu'un guide de dépannage dans l'éventualité peu probable d'un problème. Merci de votre confiance. Nous sommes certains que vous allez vite constater pourquoi plus d'un million d'OmniView de Belkin sont utilisés dans le monde.

Console IP de prise en main à distance OmniView®

Kits de Câbles PS/2

Câble VGA

Câble inverseur DB9

câble mini-USB

Bloc d'alimentation 5 VCC, 2 A

Dispositif de montage dans une baie et vis

CD d'installation du logiciel

Manuel de l'utilisateur

Guide d'installation rapide

Carte d'enregistrement

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:33:34 AM

- **Accès à distance**
  la CIPD permet un accès à distance à votre configuration KVM et les serveurs connectés. Il permet également un accès distant à un ordinateur ou un serveur seul.

- **Utilisateurs numériques**
  la CIPD permet à un utilisateur numérique d'accéder aux switchs KVM et aux serveurs et de les contrôler. Il permet en outre à 25 utilisateurs supplémentaires de voir une image numérique afin de collaborer au dépannage.

- **Basé sur navigateur Web**
  L'interface de la CIPD est basée sur navigateur Web. Tout ordinateur peut y accéder, du moment qu'il est connecté à un réseau LAN, WAN ou à l'Internet au moyen d'une connexion TCP/IP standard. Aucun logiciel supplémentaire n'est requis.

- **Interface conviviale**
  L'interface conviviale vous permet régler ou modifier les fonctions de la CIPD rapidement et facilement via un navigateur Web, sans avoir à installer un logiciel supplémentaire sur votre ordinateur.

- **Accès au BIOS**
  la CIPD vous permet d'accéder au BIOS (basic input/output system) de vos serveurs afin d'apporter des modifications ou procéder à des redémarrages.

- **Prise en charge de périphérique série**
  la CIPD prend en charge un périphérique série, tel qu'une unité de distribution de l'alimentation (PDU), afin de procéder, à distance, à des redémarrages à froid de vos serveurs.

- **Sécurité renforcée**
  la CIPD offre un chiffrement SSL sur 256 bits et une protection par mot de passe multi-serveurs pour empêcher l'accès non autorisé à vos serveurs.

- **Virtual Media***
  Avec la prise en charge Virtual Media, vous pouvez transférer des images et des fichiers entre les ordinateurs locaux et distants, charger un logiciel à distance, appliquer des rustines pour applications ou systèmes d'exploitation et procéder à un test diagnostique à partir d'un CD.

  *Disponible sur les ordinateurs sous Windows® uniquement.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:33:34 AM

- **Gestion des comptes**
  la CIPD permet à l'administrateur de créer plusieurs comptes utilisateurs et de contrôler l'accès aux serveurs.
- **Journal des événements**
  Le Journal des événements renferme toute l'activité des utilisateurs de la CIPD.
- **Notification par e-mail**
  la CIPD permet à l'administrateur de surveiller l'activité des utilisateurs par l'envoi de notifications de connexion, de connexions invalides et de déconnexions.
- **Prise en charge multi-plateformes.**
  la CIPD est compatible avec les switchs KVM ou serveurs avec connexions pour console PS/2 ou USB.
- **Résolution vidéo**
  Grâce à une bande passante de 117 MHz, la CIPD accepte des résolutions vidéo pouvant aller jusqu'à 1600 x 1200 @ 75 Hz.
- **Possibilité de montage dans une baie 0U**
  la CIPD est assez compact pour se placer sur votre bureau ou être monté à l'arrière de votre baie de serveur pour une installation 0U.
- **Mises à jour du micrologiciel**
  La mise à niveau par mémoire Flash vous permet d'obtenir les mises à jour du micrologiciel les plus récentes pour votre CIPD. Ces mises à jour garantissent la compatibilité de la CIPD avec les tout derniers périphériques et matériels. En outre, elles sont gratuites pour toute la durée de vie de la CIPD. Visitez www.belkin.com pour des informations sur les mises à jour et de l'assistance.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:33:34 AM

Configuration requise

- Console IP de prise en main à distance OmniView (inclus)
- Kit de câbles PS/2 (inclus)
- Câble VGA (inclus)
- Câble mini-USB (inclus)
- Bloc d'alimentation 5 VCC, 2 A (inclus)
- Clavier, moniteur et souris
- Connexion au réseau à l'aide d'un port Ethernet 10/100Base-T (RJ45)
- Câble CAT5
- Dispositif de montage dans une baie avec vis (fourni avec l'option d'installation dans une baie)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:33:34 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x et versions ultérieures;
UNIX®; Mac OS® X v10.0 et versions ultérieures (avecKVM);
Sun™ Solaris™ 8.x et versions ultérieures (avec adaptateur Sun – Référence Belkin F1DE083)

Navigateurs pris en charge

- Microsoft® Internet Explorer 6.0 ou version ultérieure
- Netscape® Navigator® 7.0 ou version ultérieure

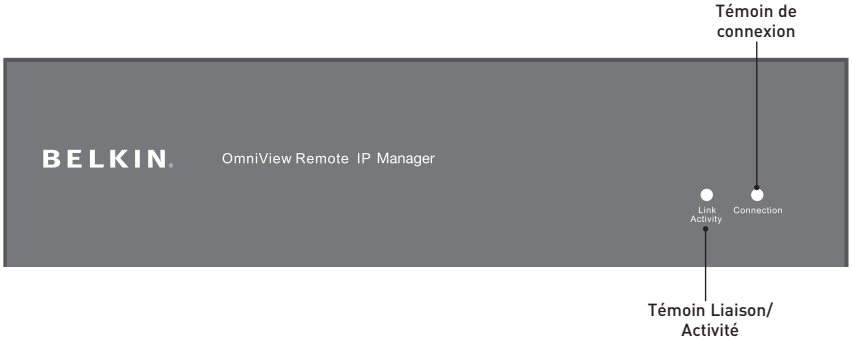
P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:33:34 AM

Référence :	F1DE101H
Alimentation :	5 VCC, 2 A
Nombre de serveurs pris en charge :	1 local, 1 numérique (1 utilisateur simultané)
Émulation de clavier :	PS/2 et USB
Émulation de souris :	PS/2 et USB
Moniteurs pris en charge :	CRT et LCD (avec prise en charge VGA)
Résolutions prises en charge :	Jusqu'à 1600 x 1200 @ 75 Hz
Bande passante distante maximale :	5 Mo
Entrée clavier :	miniDIN6 (PS/2)
Entrée souris :	miniDIN6 (PS/2)
Port du moniteur :	HDDB15 femelle (VGA)
Port USB du CPU :	mini USB
Connexion réseau :	RJ45
Chiffrement :	SSL 256 bits, 128 bits, AES, DES, 3DES
Authentification :	LDAP (via client LDAP local), RADIUS, AD
Protocoles pris en charge :	SNMP v1, IPv4
Port série :	DB9
Témoins :	2
Boîtier :	métal
Dimensions :	171 x 44 x 114 mm
Poids :	0,75 kg
Température de fonctionnement :	0 °C – 48,89 °C
Température de stockage :	-20 °C – 60 °C
Humidité :	5 % à 80 %
Garantie :	2 ans

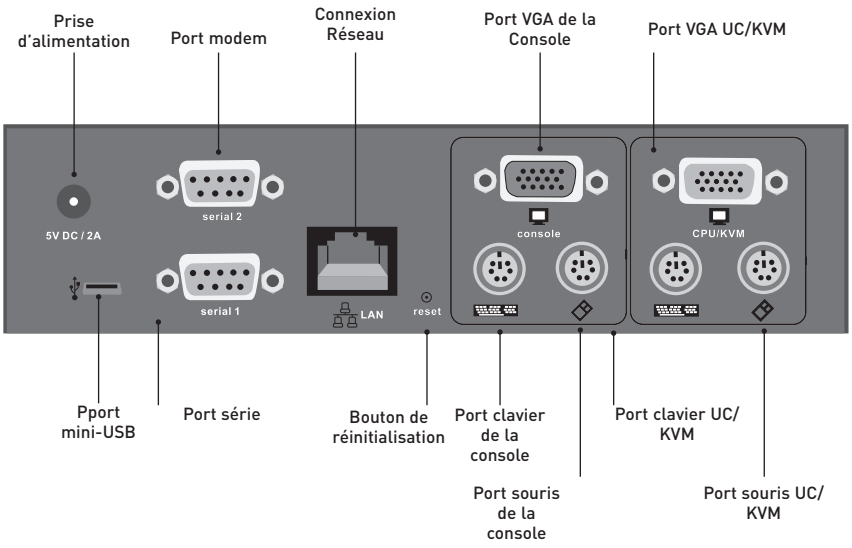
Remarque : Ces spécifications sont sujettes à modification sans préavis.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:33:34 AM

Devant de l'unité

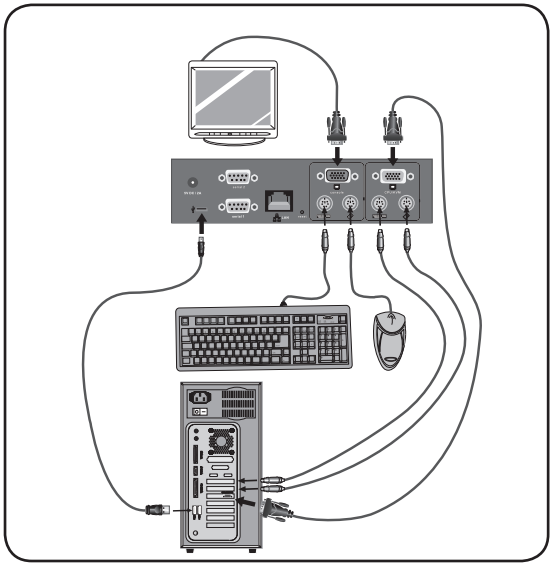


Arrière de l'unité

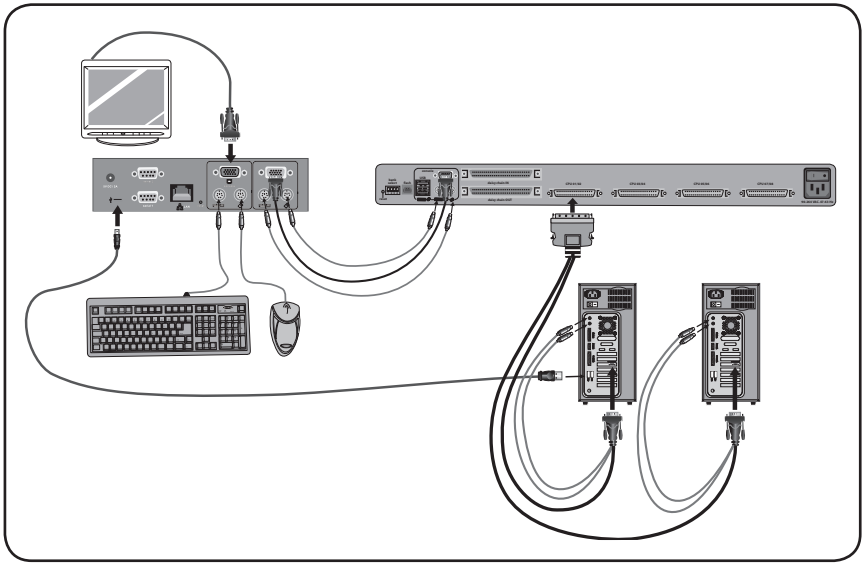


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:33:35 AM

Configuration CIPD standard avec un ordinateur



Configuration CIPD standard avec un switch KVM



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:33:38 AM

Étape 1 | Installation de la CIPD dans une baie de serveur

la CIPD est livré avec des fixations de montage qui conviennent à l'installation dans une baie 19 pouces.

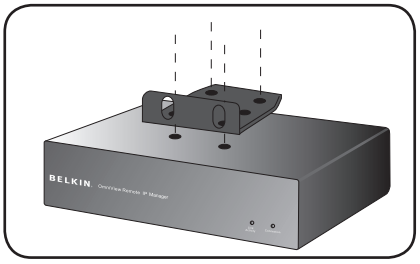


Fig. 1

1.1 Fixez le dispositif sur le haut ou le bas de la CIPD avec les vis fournies.

1.2 Montez la CIPD dans la baie. Voir **Illustr.. 1.**

Remarque : Les vis de fixation pour la baie ne sont pas fournies. Veuillez utiliser les vis spécifiées par le fabricant de votre baie.

Avertissement : Avant de brancher quoi que ce soit à la CIPD ou aux ordinateurs, assurez-vous qu'ils sont bien tous hors tension. Belkin Corporation n'est pas responsable des dommages causés dans le cas où vous ne le feriez pas.

Étape 2 | Branchement de votre console à la CIPD

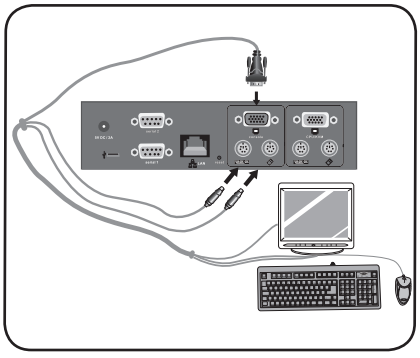


Fig. 2

2.1 Branchez votre clavier et votre souris aux ports pour clavier et souris « Console » de la CIPD.

2.2 Branchez votre moniteur au port VGA « Console » de la CIPD. Voir **Illustr. 2.**

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:33:42 AM

Étape 3 | Option 1 : Branchement de la CIPD au switch KVM (système hôte)

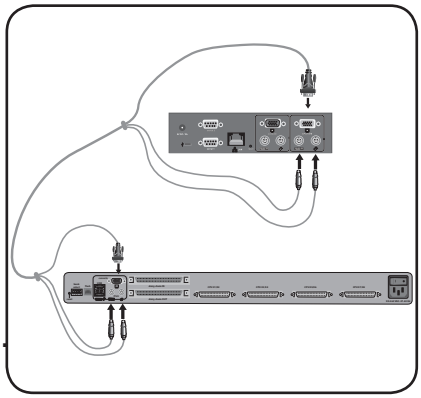


Fig. 3

3.1 Éteignez le switch KVM.

3.2 À l'aide du câble PS/2 et VGA fourni, branchez une extrémité aux ports moniteur, clavier et souris « CPU/KVM switch » de la CIPD. Voir **Illustr. 3.**

3.3 Branchez l'autre extrémité aux ports moniteur, clavier et souris de votre switch KVM.

Étape 3 | Option 2 : Branchement de la CIPD à un ordinateur (système hôte)

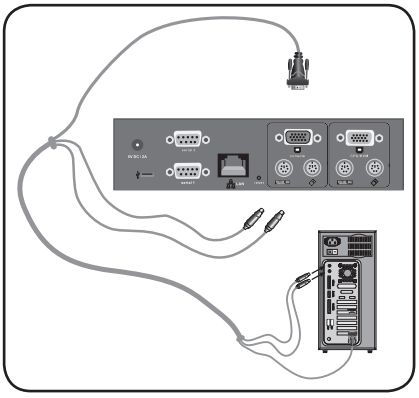


Fig. 4

3.1 Éteignez l'ordinateur.

3.2 À l'aide du kit de câbles PS/2 et VGA fourni, branchez une extrémité aux ports moniteur, clavier et souris « CPU/KVM switch » de la CIPD.
Voir **Illustr. 4.**

3.3 Branchez l'autre extrémité aux ports moniteur, clavier et souris de votre ordinateur.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:33:44 AM

Étape 4 | Branchement du câble mini-USB pour la prise en charge Virtual Media

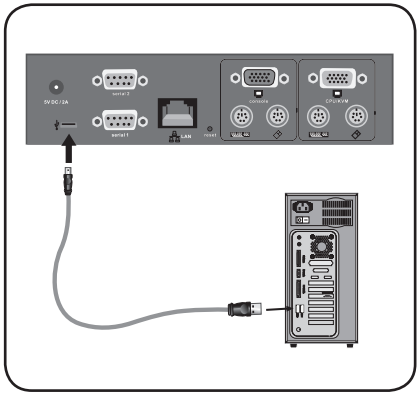


Fig. 5

4.1 Éteignez l'ordinateur.

4.2 À l'aide du câble mini USB fourni, branchez une extrémité au port mini USB de la CIPD et l'autre extrémité à un port USB disponible de votre ordinateur. Voir **Illustr. 5.**

Remarque : Vous pouvez brancher à la CIPD un ordinateur sous Windows OS pour la prise en charge Virtual Media. Il n'est pas nécessaire que l'ordinateur ne soit le système hôte.

Remarque : Si votre ordinateur n'est PAS sous Windows, l'étape ci-dessous n'est pas nécessaire.

Etape 5 | Mise sous tension de la CIPD

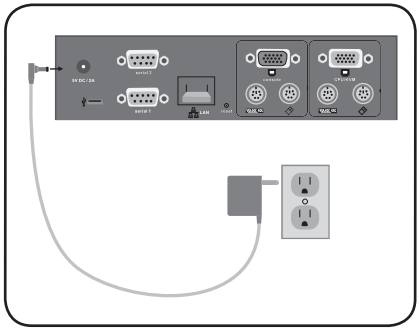


Fig 6

5.1 Branchez le bloc d'alimentation fourni sur une prise secteur libre.

5.2 Raccordez la fiche cylindrique à la prise d'alimentation de la CIPD. Voir **Illustr. 6.**

5.3 Allumez le switch KVM ou l'ordinateur.

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:33:46 AM

Il y a deux façons de mettre en route et de configurer la CIPD. Vous pouvez vous servir du logiciel de configuration compris sur le CD, ou vous pouvez brancher un câble d'interface série à la CIPD et utiliser un logiciel de terminal (par exemple, HyperTerminal®).

Remarque : Belkin vous recommande l'utilisation du logiciel de configuration fourni.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:33:47 AM

Logiciel de configuration

Le logiciel compris sur le CD fourni vous aide à la configuration de la CIPD avec les paramètres de votre réseau, afin que vous puissiez y accéder à distance.

1. Connectez la CIPD à votre ordinateur via votre réseau local. Lancez l'outil de configuration sur CD-ROM à partir de l'ordinateur où la CIPD est installé.
2. Suivez les instructions de l'assistant pour la configuration de la CIPD. Vous aurez besoin de l'adresse IP, du masque de sous-réseau et des paramètres de passerelle qui seront assignés à la CIPD. Vous devrez probablement obtenir ces informations auprès de l'administrateur réseau. Lorsque la configuration est terminée, vous recevrez une notification vous avertissant du « succès » de celle-ci. La configuration de la CIPD est terminée et vous pouvez maintenant y accéder.
3. Ce CD-ROM contient également le logiciel nécessaire au transfert de fichiers entre les ordinateurs locaux et distants. Pour en savoir plus, consultez la section « Virtual Media » de ce manuel de l'utilisateur.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:33:47 AM

Pour configurer la CIPD via une interface série, vous aurez besoin d'un câble inverseur (fourni). Branchez une extrémité du câble inverseur au port « Serial 01 » de la CIPD et l'autre extrémité au port série de l'ordinateur. L'interface série doit être réglée avec les paramètres ci-dessous :

Paramètre	**Valeur**
Bits/seconde	115200
Bits de données	8
Parité	non
Bits d'arrêt	1
Contrôle du flux	aucun

Servez-vous d'un logiciel de terminal (par exemple, HyperTerminal) pour vous connecter à la CIPD. Réinitialisez la CIPD et appuyez immédiatement sur la touche « ESC ». Vous verrez une invite de commande « => ». Entrez la commande « config » et appuyez sur la touche « ENTRÉE ». Vous serez invité à régler la configuration automatique de l'IP, l'adresse IP, le masque de réseau et la passerelle par défaut. Le fait d'appuyer sur « ENTRÉE » sans saisir de valeurs ne modifie pas les paramètres. La passerelle doit être réglée à « 0.0.0.0 » (aucune) ou toute autre valeur correspondant à l'adresse IP de la passerelle. Après la confirmation, la CIPD effectue une réinitialisation avec les nouvelles valeurs saisies précédemment.

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:33:47 AM

Interface Web

Il est possible d'accéder à la CIPD au moyen d'un navigateur Web standard prenant en charge le Java™. Vous pouvez utiliser le protocole HTTP ou une connexion chiffrée via l'HTTPS. Saisissez l'adresse IP configurée de la CIPD dans votre navigateur Web. Les paramètres de connexion initiaux sont :

Paramètre	Valeur
Connexion	administrator
Mot de passe	belkin

Il est fortement recommandé de modifier ces identifiants. Vous pouvez le faire à la page « User Management [Gestion des utilisateurs] ».

Telnet

Il est possible d'utiliser un client Telnet standard pour accéder à un périphérique quelconque connecté à l'un des ports série de la CIPD via un mode terminal.

L'interface principale de la CIPD est une interface HTTP. Pour utiliser la fenêtre console distante du système hôte géré, le navigateur doit être équipé de Java Runtime Environment, version 1.1 ou ultérieure. Si le navigateur n'offre aucune prise en charge Java (comme pour les périphériques de poche), vous pouvez tout de même gérer votre système hôte à l'aide des formulaires administratifs affichés par le navigateur.

Pour une connexion non sécurisée à la CIPD, utilisez l'un des navigateurs suivants :

- Microsoft Internet Explorer version 5.0 ou ultérieure sous Windows 2000 et XP
- Netscape Navigator 7.0 sous Windows 2000 et XP

Pour pouvoir accéder au système hôte distant en vous servant d'une connexion sécurisée chiffrée, vous devez utiliser un navigateur prenant en charge le protocole HTTPS. Une sécurité renforcée n'est garantie que par l'utilisation d'une clé de 128 bits.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:33:47 AM

3-1 Ouverture d'une session sur la Console IP de prise en main à distance

Ouvrez votre navigateur Internet. Saisissez l'adresse de votre CIPD que vous avez configurée lors du processus d'installation. Pour ce faire, utilisez une adresse IP ou un nom d'hôte et un nom de domaine, advenant le fait que vous avez donné un nom à votre CIPD dans le serveur de noms de domaines (DNS).

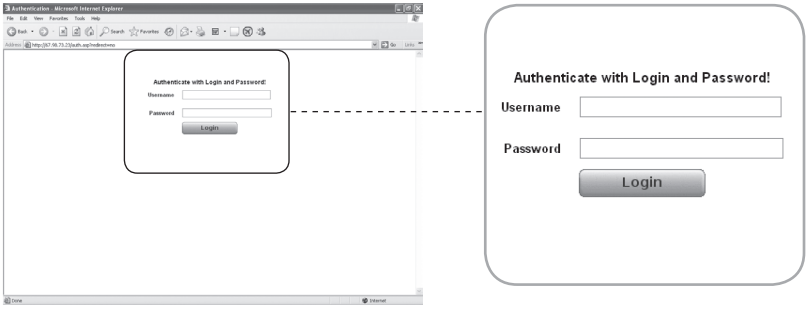
Par exemple, saisissez l'adresse suivante dans la barre d'adresse de votre navigateur pour établir une connexion non sécurisée :

http://192.168.1.22/

Pour établir une connexion sécurisée, saisissez :

http://192.168.1.22/

Ceci vous amènera à la page de connexion de la CIPD, tel que montré ci-dessous :



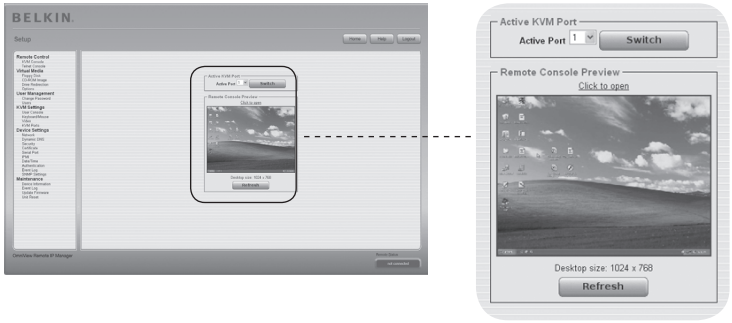
la CIPD est équipé d'un administrateur-utilisateur intégré qui a le droit d'administrer la CIPD :

Paramètre	Valeur
Connexion	administrator
Mot de passe	belkin

Remarque : Votre navigateur Web doit être en mesure d'accepter des cookies. Sinon, la connexion est impossible.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:33:47 AM

« Remote Access [Accès distant] » correspond à l'écran, au clavier et à la souris redirigés du système hôte distant que la CIPD contrôle. Le navigateur Web utilisé pour l'accès à la CIPD doit être équipé de Java Runtime Environment version 1.1 ou ultérieure. Cependant, il est fortement recommandé d'installer Sun JVM (Java Virtual Machine) 1.4. La Console distante se comporte exactement comme si vous étiez devant l'écran de votre système distant. Vous pouvez vous servir du clavier et de la souris comme d'habitude. Ouvrez la Console distante en sélectionnant l'image de prévisualisation sur le site principal de l'interface HTML.



Voici quelques unes des options disponibles dans le menu :

Bouton d'ajustement automatique

Si la vidéo affichée est de mauvaise qualité ou déformée d'une façon ou d'une autre, appuyez sur ce bouton et attendez quelques secondes. la CIPD effectue les ajustements nécessaires pour obtenir un affichage de meilleure qualité.

Synchroniser la souris

Choisissez cette option pour synchroniser le curseur de la souris local avec celui de la souris distante. Ceci peut s'avérer particulièrement nécessaire avec l'utilisation de paramètres d'accélération de la souris sur le système hôte.

Paramètres vidéo du Menu des options.

Ceci ouvre une nouvelle fenêtre contenant des éléments permettant de contrôler les paramètres vidéo de la CIPD. Vous pouvez modifier certaines valeurs liées à la luminosité et au contraste de l'image affichée et ainsi améliorer la qualité vidéo. Il est également possible de rétablir les paramètres par défaut de tous les modes vidéo ou uniquement de celui en cours.

Remarque : Lors du premier démarrage, si le curseur n'est pas synchronisé avec le curseur de la souris distante, appuyez sur le bouton d'ajustement automatique « Auto-Adjust » une fois.

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:33:48 AM

Entre la CIPD et l'hôte se trouve deux interfaces disponibles pour la transmission des données du clavier et de la souris. USB et PS/2 (disponibles séparément). Le fonctionnement correct de la souris distante dépend de plusieurs paramètres. Ceux-ci sont expliqués plus en détail plus loin dans ce manuel.

Interface USB de la Console IP de prise en main à distance

Pour utiliser l'interface USB, vous devez utiliser le câblage approprié entre l'hôte géré et le périphérique de gestion. Par exemple, si le BIOS de l'hôte géré ne prend pas en charge le clavier USB et vous n'avez branché que le câble USB, vous n'aurez aucun accès au clavier à distance pendant le processus de démarrage de l'hôte. Veuillez vous référer à la section « Clavier/souris » en page 48.

Paramètres du clavier de la Console IP de prise en main à distance

Les paramètres du type de clavier hôte de la CIPD doivent être valides afin que le clavier distant fonctionne de façon appropriée. Vérifiez les paramètres dans l'interface de la CIPD. Veuillez vous référer à la section « Clavier/souris » en page 48.

Paramètres de la souris distante

Un problème courant des dispositifs KVM est la synchronisation entre les curseurs de la souris locale et de la souris distante. la CIPD apporte une solution à ce problème grâce à un algorithme de synchronisation intelligent. Trois modes souris sont disponibles sur la CIPD.

- **Vitesse de souris automatique**

Le mode Vitesse de souris automatique tente de détecter automatiquement les paramètres de vitesse et d'accélération du système hôte. Référez-vous à la section ci-dessous pour des explications détaillées.

- **Vitesse de souris fixe**

  Ce mode traduit les mouvements de la souris de la Console distante de sorte qu'un mouvement d'un pixel équivaut à un mouvement de pixel sur le système distant. Ce paramètre peut être ajusté avec la mise à l'échelle. Veuillez prendre note que ceci ne fonctionne que lorsque la fonction d'accélération de la souris du système distant est désactivée.

- **Modes Souris simple/double**

  Ce mode est expliqué dans la section « Modes Souris simple/double » en page 20.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:33:48 AM

Synchronisation automatique de la vitesse de la souris

Le Mode de synchronisation automatique de la vitesse de la souris détecte la vitesse de la souris lors de la synchronisation. Lorsque la souris ne se déplace pas correctement, il existe deux façon de re-synchroniser la souris locale et la souris distante.

- **Fast Sync (Synchronisation rapide)**
  Ce type de synchronisation est utilisé pour corriger un décalage temporaire, mais fixe. Choisissez cette option à partir du menu Options de la console distante. Si celui-ci a été défini, vous pouvez également exécuter le raccourci clavier correspondant à la synchronisation de la souris (voir en page 23 à la section « Barre de contrôle de la console distante ».

- **Intelligent Sync (synchronisation intelligente)**
  Si la synchronisation rapide ne fonctionne pas ou si les paramètres de la souris ont été modifiés sur le système hôte, utilisez la synchronisation intelligente. Cette méthode ajuste le paramètre du mouvement réel du pointeur de la souris, de sorte que le pointeur s'affiche à l'endroit approprié à l'écran. Cette méthode demande plus de temps que la synchronisation rapide. Vous pouvez l'obtenir en choisissant l'élément approprié dans le menu des options de la Console distante. La synchronisation intelligente nécessite une image correctement ajustée. Utilisez la fonction d'ajustement automatique ou la correction manuelle de la boîte de dialogue « Video Settings [Paramètres vidéo] » pour configurer l'image. La forme du pointeur influence la capacité de détection du pointeur. Belkin vous recommande l'utilisation d'un pointeur d'une forme simple et courante. Dans la plupart des cas, la détection et la synchronisation d'un pointeur animé échoue. En général, les pointeurs dont la forme change pendant le processus de détection sont pratiquement impossibles à visualiser sur l'image vidéo transférée. L'utilisation d'un pointeur avec une forme simple garantit la simplicité du processus de détection et une synchronisation efficace.

  Le bouton « Mouse [Souris] » de la console distante peut se comporter différemment, selon l'état actuel de la synchronisation de la souris. De façon générale, le fait d'appuyer sur ce bouton exécute une synchronisation rapide, excepté lorsque le mode vidéo a été modifié récemment. Veuillez également vous référer à la section « Barre de contrôle de la console distante ».

Lors du premier démarrage, si le curseur n'est pas synchronisé avec le curseur de la souris distante, appuyez sur le bouton d'ajustement automatique « Auto-Adjust » une fois.

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:33:48 AM

Paramètres système de la souris hôte

Le système d'exploitation hôte possède plusieurs paramètres pour le pilote de la souris.

Bien que la CIPD est compatible avec les souris accélérées et est en mesure de synchroniser les pointeurs de la souris locale et de la souris distante, les limites suivantes peuvent empêcher le bon déroulement de la synchronisation :

- **Pilote de souris spécial**
  Certains pilotes de souris influencent le processus de synchronisation, ce qui conduit à une désynchronisation des pointeurs. Si cela se produit, assurez-vous que vous n'utilisez pas de pilote de souris spécial propre à un fabricant sur votre système hôte.

- **Paramètres de souris sous Windows 2003 Server/XP**
  Windows XP possède un paramètre servant à améliorer l'accélération de la souris : ce paramètre doit être désactivé.

- **Active Desktop**
  Si la fonction « Active Desktop » de Microsoft Windows est activée, n'utilisez pas un fond d'écran uni. Utilisez plutôt une image ou un papier peint. Vous pouvez également désactiver la fonction Active Desktop.

  Déplacez le pointeur de la souris au coin supérieur gauche de l'écran de l'appliquette et faites quelques déplacements aller-retour. Ceci aura pour effet de re-synchroniser la souris. Si la re-synchronisation échoue, désactivez la fonction d'accélération de la souris et répétez l'opération.

- **Modes Souris simple/double**
  L'information ci-dessous concerne le mode double souris, où les pointeurs de la souris locale et de la souris distante sont visibles et doivent être synchronisés. la CIPD possède un autre mode, le mode souris simple, où seulement le pointeur de la souris distante est visible. Activez ce mode sous Console distante (voir la section « Barre de contrôle de la console distante » en page 23) et cliquez sur la fenêtre. Le pointeur de la souris local est masqué et le pointeur de la souris distante peut être contrôlé directement. Pour quitter ce mode, vous devez définir un raccourci clavier dans la fenêtre des paramètres de la console distante. Appuyez sur cette séquence de touches pour faire apparaître le pointeur local.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:33:48 AM

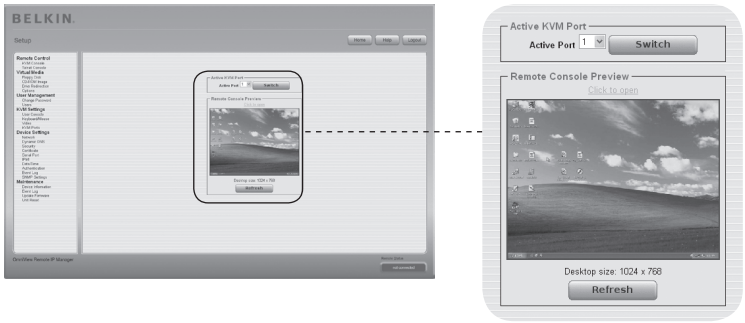
Paramètres recommandés pour la souris

Windows 2000, 2003, XP (toutes les versions)	De façon générale, Belkin recommande l'utilisation d'une souris USB. Choisissez l'USB sans synchronisation de la souris.
Mac OS X	Belkin recommande l'utilisation du mode souris simple.
Sun Solaris	Réglez les paramètres de la souris à « 1:1, no acceleration » via « xset m 1 » ou à l'aide du CDE Control Panel. Vous pouvez également utiliser le mode souris simple.
Linux	Choisissez d'abord l'option « Other Operating Systems [Autres systèmes d'exploitation] » dans la boîte de sélection du type de souris. Ensuite, choisissez l'option « Auto Mouse Speed [vitesse de souris automatique] ». Ceci concerne les souris USB et les souris PS/2.

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:33:48 AM

Navigation

Après vous être connecté à la CIPD, la page principale de celui-ci apparaît. Cette page contient trois sections, chacune comprenant des informations spécifiques. Les boutons du haut vous permettent de naviguer dans l'interface (voir le Tableau pour de plus amples informations). Le cadre inférieur gauche contient une barre de navigation, qui vous permet de passer d'une section à l'autre de la CIPD. Les informations relatives à la tâche, qui dépendent de la section choisie précédemment, s'affiche dans le cadre de droite.



Remarque : S'il n'y a pas d'activité pendant 30 minutes, la CIPD se déconnecte automatiquement. Si vous cliquez sur l'un des liens, vous serez amené à l'écran de connexion.

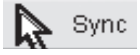
P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:33:49 AM

La partie supérieure de la fenêtre de la console distante comprend une barre de contrôle. Au moyen des éléments qu'elle contient, vous pouvez connaître l'état de la console distante et régler les paramètres de la console distante. Une description de chaque commande suit.

- **Bouton d'ajustement automatique**

Si la vidéo affichée est de mauvaise qualité ou déformée d'une façon ou d'une autre, appuyez sur ce bouton et attendez quelques secondes. la CIPD effectue les ajustements nécessaires pour obtenir un affichage de meilleure qualité.

- **Synchroniser la souris**



Choisissez cette option pour synchroniser le curseur de la souris locale avec celui de la souris distante. Ceci peut s'avérer particulièrement important avec l'utilisation de paramètres d'accélération de la souris sur le système hôte. De façon générale, il n'est pas nécessaire de modifier les paramètres de la souris.

- **Modes Souris simple/double**

Choisissez ce mode pour passer du mode souris simple (où seul le pointeur de la souris distante est visible) au mode double souris (où les pointeurs de la souris locale et de la souris distante sont visibles et doivent être synchronisés). Le mode souris simple n'est disponible que sous Sun JVM 1.4 ou version ultérieure.

- **Options**

Pour ouvrir le menu des options, cliquez sur le bouton « Options ».

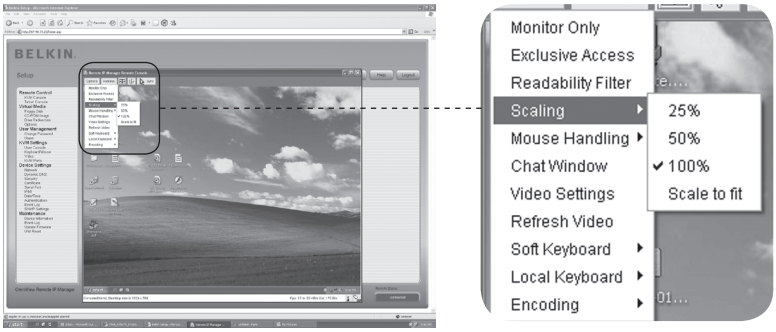
Une courte description des options suit :

- **Monitor Only (Surveillance seulement)**
  Active ou désactive le filtre « Monitor Only [Surveillance seulement] ». Si le filtre est activé, aucune interaction n'est possible avec la console distante. Cependant, la surveillance est possible.

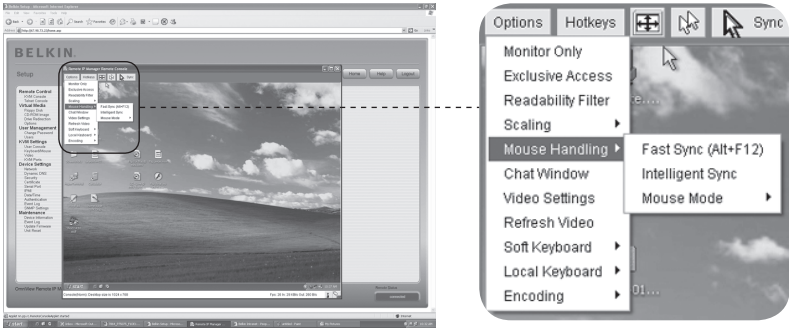
- **Exclusive Access (Accès exclusif)**
  Avec les permissions appropriées, vous pouvez forcer la fermeture de toutes les consoles distantes des autres utilisateurs. Personne ne peut ouvrir la console distante de nouveau tant que vous ne désactivez pas l'accès exclusif ou tant que vous ne vous déconnectez pas.

P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:33:49 AM

- **Scaling (Mise à l'échelle)**
  Permet de réduire l'échelle de la console distante. Vous pouvez continuer à utiliser la souris et le clavier, mais l'algorithme de mise à l'échelle ne conservera pas tous les détails de l'affichage.



- **Mouse Handling (Gestion de la souris)**
  Le sous-menu de gestion de la souris propose deux options de synchronisation des pointeurs des souris locale et distante, tel qu'expliqué à la section « Configuration du clavier, de la souris et du moniteur ».



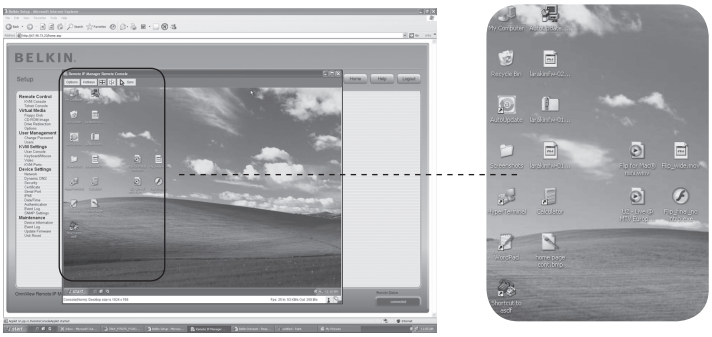
- **Fast Sync (Synchronisation rapide)**
  Ce type de synchronisation est utilisé pour corriger un décalage temporaire, mais fixe.

- **Intelligent Sync (Synchronisation intelligente)**
  Utilisez cette option si la synchronisation ne fonctionne pas ou si les paramètres de la souris ont été modifiés sur le système hôte.

  Avertissement : Cette méthode prend plus de temps que la synchronisation rapide et requiert une image correctement ajustée. Utilisez la fonction d'ajustement automatique ou la correction manuelle de la boîte de dialogue « Video Settings [Paramètres vidéo] » pour configurer l'image.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:33:50 AM

- **Local Cursor (Curseur local)**
  Offre une liste de formes de curseurs pouvant être utilisés avec le pointeur de la souris locale. La forme sélectionnée sera gardée en mémoire pour l'utilisateur actuel et sera activée la prochaine fois que cet utilisateur ouvre la console distante. Le nombre de formes disponibles dépend de Java Virtual Machine (JVM) ; les versions 1.2 et ultérieures offrent la liste complète.



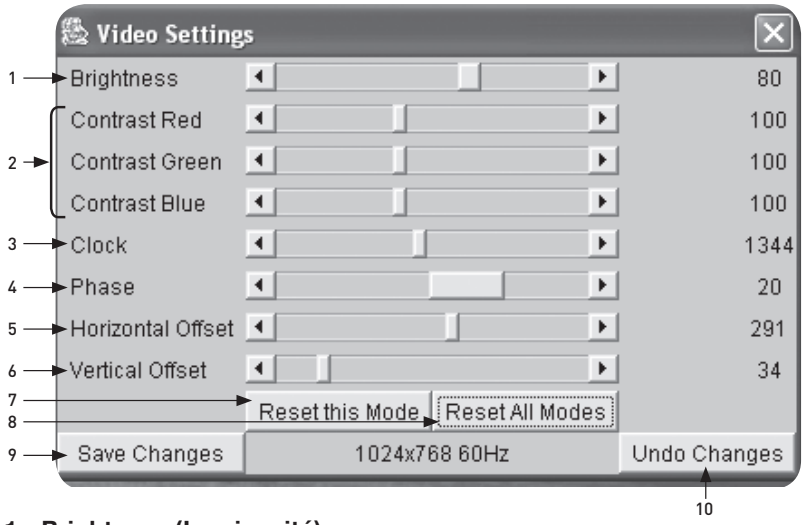
- **Video Settings (Paramètres vidéo)**
  Ouvre une boîte de dialogue qui permet de modifier les paramètres vidéo de la CIPD. la CIPD comprend deux dialogues pouvant agir sur les paramètres vidéo.

- **Paramètres vidéo via l'interface HTML**
  Sélectionnez cette option pour activer le port vidéo local. Cette option détermine si la sortie vidéo locale de la CIPD est active et est transmise par le signal entrant du système hôte.

  L'option « Noise Filter [Filtre de bruit] » définit la réaction de la CIPD aux petits changements dans le signal vidéo en entrée. Un filtre large nécessite un trafic réseau moins dense et permet un affichage vidéo plus rapide, mais les petits changements à différents endroits de l'affichage peuvent ne pas être reconnus immédiatement. Un filtre étroit affiche tous les changements instantanément mais entraîne un trafic réseau constant et très dense, peu importe si le contenu affiché ne varie pas beaucoup (selon la qualité du signal vidéo en entrée). Le paramètre par défaut convient à la plupart des situations.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:33:50 AM

Paramètres vidéo via la console distante



1. **Brightness (Luminosité)**
   Modifie la luminosité de l'image.
2. **Contrast (Contraste)**
   Modifie la netteté du contraste de l'image.
3. **Clock (horloge)**
   Définit la fréquence horizontale d'une ligne vidéo et dépend du mode vidéo. Les valeurs peuvent varier selon la carte vidéo. Les paramètres par défaut, ainsi que la procédure d'ajustement automatique conviennent pour la plupart des configurations. Pour obtenir une image de meilleur qualité, modifiez ce paramètre ainsi que le paramètre de phase d'échantillonnage.
4. **Phase**
   Définit la phase pour l'échantillonnage vidéo, qui sert au contrôle de la qualité de l'affichage, de concert avec le paramètre d'horloge d'échantillonnage.
5. **Horizontal Offset (Décalage horizontal)**
   Si vous choisissez cette option, servez-vous des boutons gauche et droite pour déplacer l'image horizontalement.
6. **Vertical Offset (Décalage vertical)**
   Si vous choisissez cette option, servez-vous des boutons gauche et droite pour déplacer l'image verticalement.
7. **Reset this Mode (Réinitialiser ce mode)**
   Permet de rétablir les valeurs par défaut des paramètres propres au mode.
8. **Reset all Modes (Réinitialiser tous les modes)**
   Permet de rétablir les valeurs par défaut de tous les paramètres.
9. **Save Changes (Enregistrer les modifications)**
   Permet d'enregistrer définitivement les modifications.
10. **Undo Changes (Annuler les modifications)**
    Rétablit les derniers paramètres.

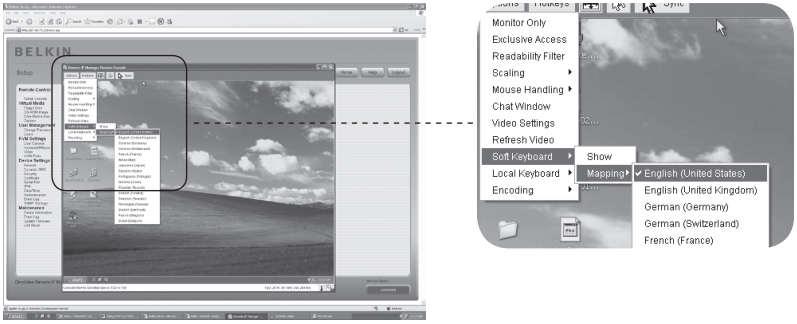
P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:33:51 AM

Mapping Sequence (séquence d'affectation)

Soft Keyboard (clavier logiciel)
Ouvre le menu du clavier logiciel.

Show (Montrer)
Fait apparaître le clavier logiciel. Le clavier logiciel est nécessaire si le système hôte fonctionne avec des paramètres de langue et de pays différents de votre machine servant à l'administration.

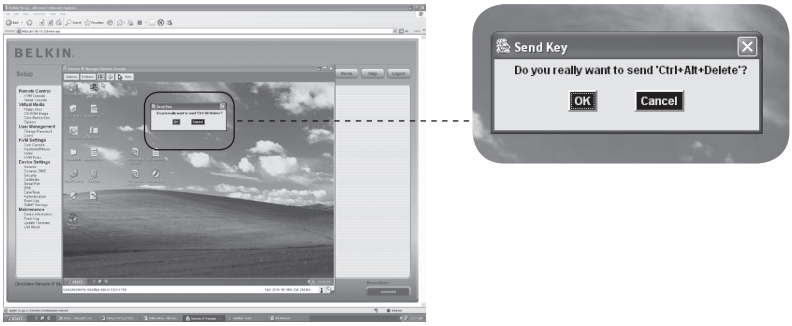
Mapping (Affectation)
Sert à choisir la configuration appropriée (langue et pays) pour le clavier logiciel.



P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:33:51 AM

Local Keyboard (Clavier local)
Sert à modifier la configuration (langue) de l'ordinateur sur lequel l'appliquette de la console distante est en cours d'exécution. De façon générale, l'appliquette détermine automatiquement la valeur appropriée. Cependant, selon votre JVM et vos paramètres de navigateur, ceci n'est pas toujours possible. Un exemple classique est l'utilisation d'un système allemand avec un clavier selon la configuration US-English. Dans ce cas, vous devez ajuster manuellement le paramètre de clavier local avec la langue appropriée.

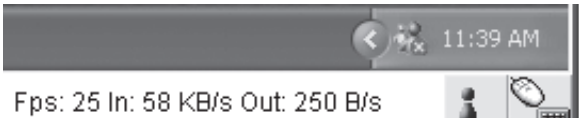
Hot Keys (Raccourcis)
Ouvre une liste de raccourcis clavier pré-déterminés. Choisissez une entrée et la commande sera envoyée au système hôte. Vous pouvez ajouter un dialogue de confirmation, qui s'affichera avant que la commande sélectionnée ne soit envoyée à l'hôte distant. Sélectionnez « OK »pour exécuter la commande sur l'hôte distant.



P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:33:52 AM

La ligne d'état montre l'état de la console distante et de la connexion. La taille de l'écran distant est affichée à gauche. La valeur entre parenthèses indique la connexion à la console distante. « Norm » indique une connexion standard sans chiffrement ; « SSL » indique une connexion sécurisée avec protocole SSL.

Le trafic réseau entrant (« In ») et sortant (« Out ») s'affiche en kilooctets par seconde. Si le encodage avec compression est activé, une valeur entre parenthèses montre le débit de transfert comprimé.



Le bouton suivant affiche les paramètres d'accès à la console distante.

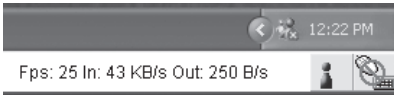
Un ou plusieurs utilisateurs peuvent se connecter à la console distante de la CIPD.

Vous avez l'accès exclusif. Tout autre utilisateur ne peut accéder à l'hôte distant via la console distante tant que vous n'avez pas désactivé cette option.

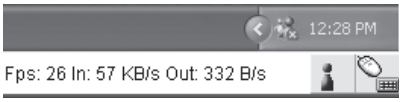
P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:33:52 AM

Un utilisateur distant possède l'accès exclusif. Vous ne pouvez accéder à l'hôte distant via la console distante tant que l'autre utilisateur n'a pas désactivé cette option.

Le bouton tout à droite affiche l'état des paramètres de « surveillance seulement » (Monitor Only)..



L'option de surveillance seulement est désactivée.



L'option de surveillance seulement est activée.

Pour en savoir plus sur les paramètres de surveillance seulement et d'accès exclusif, voir la section « Barre de contrôle de la console distante » en page 23 de ce manuel de l'utilisateur.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:33:53 AM

Rétablissement des paramètres d'origine de la Console IP de prise en main à distance

Pour réinitialiser la CIPD et rétablir les paramètres réseau d'origine :

1. Établissez une connexion série pour la configuration initiale (HyperTerminal)

Bits par seconde :	115200
Bits de données :	8
Parité :	aucun
Bits d'arrêt :	1
Contrôle du flux :	matériel ou aucun

2. Appuyez sur le bouton de réinitialisation, situé entre la prise CC et la prise réseau. Relâchez le bouton de réinitialisation et appuyez immédiatement sur la touche ÉCHAPP du programme de terminal série (HyperTerminal) à plusieurs reprises, jusqu'à ce que l'invite « => » apparaisse.

   Remarque : Si l'invite n'apparaît pas dans les trois secondes suivant le relâchement du bouton de réinitialisation, répétez les étapes 1 et 2. la CIPD ne détectera la touche ÉCHAPP que pendant les trois premières secondes du processus de démarrage.
3. Lorsque vous y êtes invité, tapez « defaults » et appuyez sur la touche Entrée. la CIPD démarre et retrouve les paramètres d'origine.
4. Éteignez votre serveur (l'ordinateur auquel la CIPD est connecté localement).
5. Débranchez le bloc d'alimentation de la CIPD, ainsi que les câbles au port « CPU/KVM switch » et le câble réseau.
6. Rebranchez les câbles et mettez votre serveur sous tension.

Vous pouvez maintenant reconfigurer la CIPD avec vos paramètres réseau via une connexion HyperTerminal ou à l'aide du logiciel de configuration.

Fermeture d'une session sur la Console IP de prise en main à distance

Ce lien vous permet de déconnecter l'utilisateur en cours et d'afficher un nouvel écran de connexion. Veuillez noter qu'une déconnexion automatique survient lorsqu'il n'y a pas d'activité pendant 30 minutes.

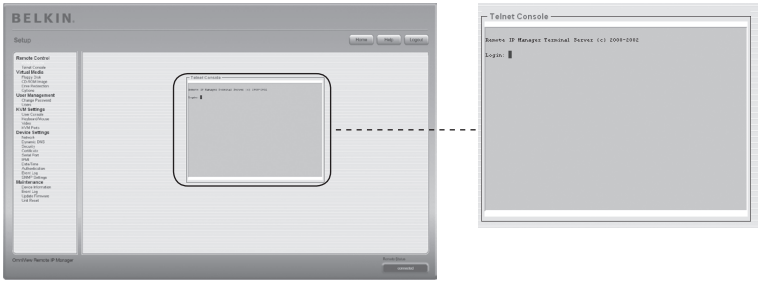
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:33:53 AM

Console KVM

Prévisualisation de la console distante

Pour ouvrir la console KVM, cliquez sur l'entrée du menu à gauche ou sur l'image de la console à droite. Pour actualiser l'image, cliquez sur le bouton « Refresh [Actualiser] ».

Console Telnet



Le micrologiciel de la CIPD comprend une passerelle Telnet, qui permet à un utilisateur de connecter à la CIPD au moyen d'un client Telnet standard. Pour vous connecter à la CIPD via le protocole Telnet, vous pouvez utiliser un programme de terminal comme xterm, TeraTerm ou PuTTY. Vous pouvez également entrer la commande Telnet sur la ligne de commande ou vous servir du dialogue « Exécuter »à partir du menu Démarrer. Par exemple, vous pouvez taper la séquence suivante :

Telnet : 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:33:54 AM

Remplacez l'adresse IP par celle que vous avez attribuée à la CIPD au cours de l'installation. Vous serez ensuite invité à entrer le nom d'utilisateur et le mot de passe pour établir une connexion avec l'unité. Ces identifiants sont les mêmes que ceux qui sont nécessaires pour la connexion à l'interface Web. Cela veut dire que la gestion de l'interface Telnet par l'utilisateur est assurée par les fonctions appropriées de l'interface Web. Après vous être connecté à la CIPD, une ligne de commande s'affiche. Vous pouvez y entrer les commandes de gestion appropriées. De façon générale, l'interface Telnet prend en charge deux modes de fonctionnement : le mode ligne de commande et le mode terminal. Le mode ligne de commande sert au contrôle ou à l'affichage de certains paramètres. En mode terminal, l'accès d'intercommunication au port série 1 est activé (si les paramètres série sont réglés adéquatement). Pour configurer la CIPD via une interface série, vous aurez besoin d'un câble inverseur. Toutes les saisies sont redirigées vers l'unité au port série 1 et ses réponses s'affichent sur l'interface Telnet.

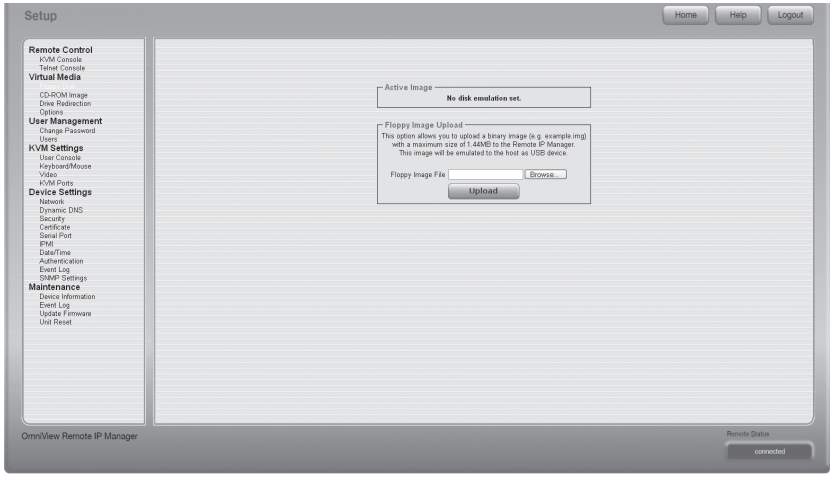
La liste suivante montre la syntaxe des commandes et leur utilisation.

Help	Afficher la liste des commandes possibles.
cls	Effacer l'écran.
quit	Quitter la section en cours et se déconnecter du client.
version	Afficher des informations sur la version
terminal	Lancer le mode terminal d'intercommunication pour le port série 1. La séquence « esc exit » a pour effet de passer en mode commande. La commande possède également un paramètre optionnel (1 ou 2), servant à sélectionner le port série pour l'intercommunication.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:33:54 AM

Floppy Disk (disquette)



Cette fonction permet de télécharger et de transférer des fichiers image. Cette option vous permet de télécharger en amont une image binaire (par exemple, .img) d'une taille maximum de 1,44 Mo, vers la CIPD. Cette image sera émulée sur l'hôte en tant que périphérique USB. Tous les autres formats doivent être transférés au moyen de la fonction de redirection de lecteur. Pour une image plus grande, téléchargez cette image au moyen de Partage Windows.

Télécharger l'image d'une disquette

Étape 1 : Cliquez « Browse [Parcourir] » pour sélectionner le fichier à être transféré.

Étape 2 : Cliquez « Upload [Télécharger] » pour télécharger le fichier vers la CIPD Vous recevrez un message confirmant que le fichier a été téléchargé vers la CIPD avec succès.

Étape 3 : Cliquez sur « KVM Console [Console KVM] » dans la section de la console distante sur l'interface de la CIPD afin d'accéder au bureau de l'ordinateur distant.

Étape 4 : Cliquez deux fois sur l'icône Poste de travail pour ouvrir ce dossier.

Étape 5 : Vous verrez une seconde entrée pour le lecteur de disquettes sous Poste de travail. Cette entrée est appelée « 3-1⁄2 Floppy (B) ». Vous pouvez accéder aux fichiers transférés ici.

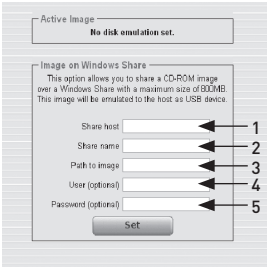
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:33:55 AM

Image d'un CD-ROM

Servez-vous de la fonction Image de Partage Windows (SAMBA).

Pour inclure une image d'un Partage Windows, sélectionnez « CD-ROM » à partir du sous-menu.

Vous devez fournir les informations suivantes afin de télécharger l'image sélectionnée :



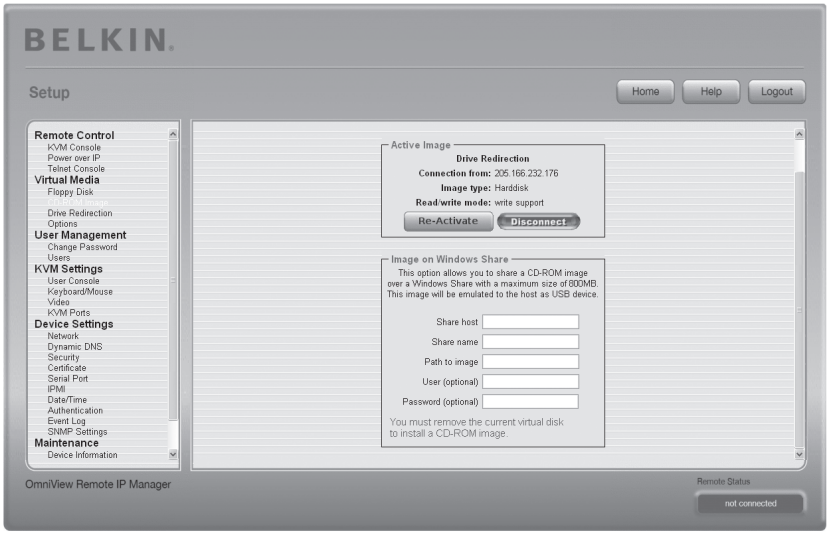
1. **Share Host**
   Le nom du serveur ou son adresse IP. (Cette adresse IP s'obtient en exécutant le logiciel de redirection de lecteur – voir ci-dessous.)
2. **Share Name**
   Le nom du dossier de partage.
3. **Path to Image**
   Le chemin d'accès vers le fichier sur la ressource partagée.
4. **User (facultatif)**
   Si nécessaire, indiquez le nom d'utilisateur pour la ressource partagée. Si ce nom n'est pas spécifié et qu'un compte visiteur est activé, les identifiants de ce compte visiteur servira à votre connexion.
5. **Password (facultatif)**
   Si vous devez entrer un mot de passe, entrez le mot de passe correspondant au nom d'utilisateur donné.

P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:33:55 AM

Télécharger l'image d'un CD-ROM

Étape 1 : Ouvrez et exécutez le logiciel de redirection de lecteur.

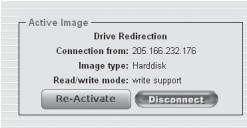
Étape 2 : Lorsque le logiciel de redirection de lecteur s'est connecté, laissez la fenêtre ouverte et allez à l'image du CD-ROM dans la section Virtual Media de l'interface de la CIPD.



Remarque : L'adresse IP sous « Connection From » est l'adresse IP qui sert d'adresse hôte de la ressource partagée. Pour vérifier la validité de l'adresse IP attribuée par le logiciel de redirection de lecteur, branchez le câble série entre la CIPD et l'ordinateur, puis ouvrez une session HyperTerminal. Connectez-vous avec « ping »et entrez l'adresse IP exactement comme elle apparaît dans le champ « Share host ». Vous devriez recevoir la réponse « <IP> is alive! ».

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:33:55 AM

Étape 3 : Cliquez « Re-Activate [re-activer] » dans la section Active Image.



Étape 4 : Entrez l'adresse IP fournie par le logiciel de redirection de lecteur dans le champ « Share Host ».

Étape 5 : Entrez le « Share name » et le « Path to Image ».

Étape 6 : Pour télécharger le fichier, cliquez sur le bouton « Set ». Le fichier sera affiché en tant que périphérique USB sur l'ordinateur distant.

Le fichier image spécifié doit être maintenant accessible à partir de la CIPD. L'information ci-dessus doit être donnée du point de vue de la CIPD. Il est très important de spécifier les bonnes adresses IP et les bons noms de périphériques. Sinon, la CIPD peut ne pas pouvoir accéder au fichier image référencé et ne procédera pas à l'ajout du fichier (il affichera un message d'erreur). Belkin vous recommande l'utilisation de valeurs correctes. Répétez cette étape si nécessaire.

La ressource partagée spécifiée doit être correctement configurée. Pour ce faire, des permissions de type administrateur sont requises. En tant qu'utilisateur régulier, il se peut que vous ne possédiez pas ces permissions. Vous devez soit vous connecter en tant qu'administrateur du système ou demander à l'administrateur de votre système d'exécuter cette tâche.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:33:55 AM

Redirection de lecteur

La fonction de redirection de lecteur offre une autre façon d'utiliser un lecteur de disque virtuel sur l'ordinateur distant. Vous pouvez travailler avec un lecteur sur votre ordinateur local à partir de la machine distante en partageant le lecteur sur une connexion réseau TCP. Les périphériques de stockage tels que les disques durs, lecteurs de disquettes, lecteurs de CD-ROM, ainsi que les média amovibles tels que les clés USB peuvent être redirigés. Vous pouvez même configurer votre machine distante pour permettre l'écriture de données sur un disque local.

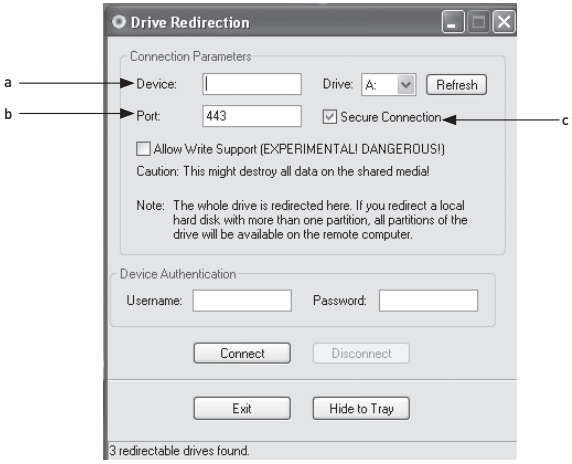
***Remarque :** Belkin ne recommande pas l'utilisation de la fonction d'écriture lors de la redirection de disques durs et ne peut être tenu responsable des pertes de données et des données corrompues survenant pendant ce processus.

Veuillez vous servir de cette fonction avec prudence. La redirection de lecteur fonctionne à un niveau bien inférieur au système d'exploitation, de sorte que les systèmes d'exploitation local et distant ne peuvent détecter la redirection d'un lecteur à un moment donné. Ceci peut entraîner une corruption des données lorsque l'un des systèmes d'exploitation (sur la machine locale ou l'hôte distant) écrit des données sur le périphérique. Si la fonction d'écriture est activée, l'ordinateur distant peut endommager les données et le système de fichiers du périphérique redirigé. Par contre, si le système d'exploitation local écrit des données sur le périphérique redirigé, la cache du lecteur du système d'exploitation de l'hôte distant peut contenir des données plus anciennes, ce qui confond le système d'exploitation de l'hôte distant. C'est pourquoi nous vous recommandons d'user de prudence lors de la redirection de lecteur, en particulier lors de l'utilisation de la fonction d'écriture.

Remarque : Pour utiliser la fonction de redirection de lecteur, vous devez installer le logiciel de redirection de lecteur (fourni avec ce produit) sur l'ordinateur à partir duquel vous accédez à la CIPD à distance.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:33:56 AM

1. **Ouvrez l'application de redirection de lecteur.**



2. **Spécifiez les paramètres de la connexion au réseau.**
   - **a. Device (unité)**
     Il s'agit de l'adresse IP de la CIPD auquel vous voulez vous connecter.
   - **b. Port**
     Il s'agit du port réseau. Par défaut, la CIPD utilise le port de console distante (n° 443). Vous pouvez modifier cette valeur si vous avez modifié le port de console distante dans les paramètres réseau de votre CIPD.
   - **c. Secure Connection (connexion sécurisée)**
     Cochez cette option pour établir une connexion sécurisée via SSL. Ceci a pour effet de maximiser la sécurité. Toutefois, la vitesse de connexion peut être réduite.
3. **Sélectionnez le lecteur que vous voulez rediriger.** Tous les périphériques disponibles (lettres de lecteurs) sont montrés. Veuillez prendre note que la CIPD ne partage pas le lecteur en entier avec l'ordinateur distant, mais uniquement une partition. Si vous possédez un disque dur avec plus d'une partition, toutes les lettres qui appartiennent à ce disque seront redirigées. Servez-vous du bouton « Refresh [Actualiser] » pour actualiser la liste des lettres de lecteurs. Ceci est particulièrement important pour une clé USB
4. **Prise en charge de l'écriture**

   Avertissement : Usez de prudence de l'utilisation de cette fonction. La fonction d'écriture permet à l'ordinateur distant d'écrire des données sur votre lecteur local. Si le système local et le système distant tentent d'écrire des données sur le même périphérique simultanément, **le système de fichiers du lecteur sera détruit.** Veuillez n'utiliser cette fonction que lorsque vous êtes certain que vous pouvez le faire en toute sécurité pour vos données.

   Remarque : Belkin ne recommande pas l'utilisation de la fonction d'écriture lors de la redirection de disques durs et ne peut être tenu responsable des pertes de données et des données corrompues survenant pendant ce processus.
5. **Authentifiez le périphérique.** Pour utiliser la fonction de redirection de lecteur, vous devez procéder à l'authentification sur la CIPD avec un nom d'utilisateur et un mot de passe valides. Vous devez posséder la permission vous permettant de modifier la configuration du disque virtuel.

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:33:56 AM

6. **Procédez à la redirection du lecteur en appuyant une fois sur le bouton « Connect ».**
   Si tous les paramètres sont corrects, la barre d'état affiche que la connexion a été établie : le bouton « Connect » est désactivé et le bouton « Disconnect » est activé. Si une erreur survient, la ligne d'état montre un message d'erreur.

   Le logiciel de redirection de lecteur tente de verrouiller le lecteur local avant qu'il ne soit redirigé. Ceci empêche le système d'exploitation local d'accéder au lecteur tant et aussi longtemps que celui-ci est redirigé. Cette tentative échoue si un fichier du lecteur est ouvert. Si le verrouillage échoue, vous serez invité à confirmer l'établissement de la connexion. Cependant, rappelez-vous que si la fonction d'écriture est activée, la redirection de lecteur peut endommager un lecteur non verrouillé.
7. Servez-vous du bouton « Disconnect » pour mettre fin à la redirection d'un lecteur.
8. Cliquez sur « Exit » pour fermer le programme de redirection de lecteur. Si une connexion de redirection est active, la connexion est fermée avant la fermeture de l'application.
9. Utilisez le bouton « Hide to Tray [minimiser] » pour minimiser l'application sans toutefois la fermer. Une connexion en cours demeure active tant que vous ne fermez pas l'application. Vous pouvez accéder au logiciel en cliquant deux fois sur l'icône dans la barre de tâches. L'icône indique également la présence ou l'absence d'une connexion. Cliquez avec le bouton droit de la souris pour faire apparaître un sous-menu.

Options

Disable Drive Redirection (désactiver la redirection de lecteur)
Ceci désactive la redirection de lecteur.

Force Read-Only Connections (forcer des connexions en lecture seule)
Cet désactive la fonction d'écriture de la redirecteur de lecteur.

Cliquez sur « Apply [Appliquer] » pour enregistrer vos modifications.

P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:33:56 AM

Créer une image

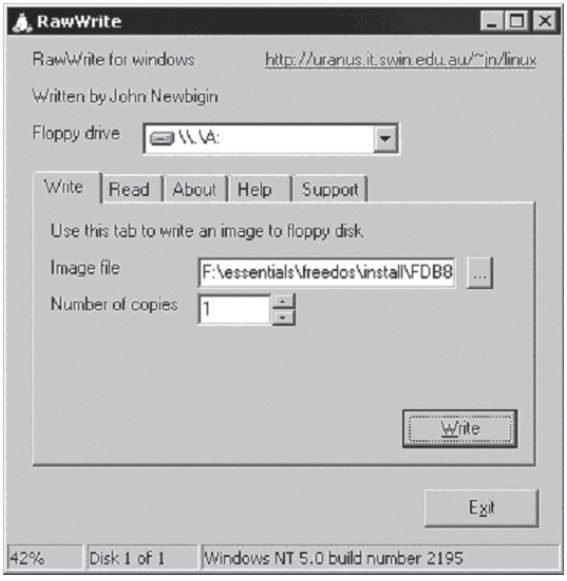
Image d'une disquette

UNIX® et systèmes d'exploitation de type UNIX

Pour créer un fichier image, utilisez « dd ». Il s'agit d'un des utilitaires d'origine UNIX et est livré avec tout système d'exploitation de type UNIX (UNIX, Sun Solaris, Linux). Pour créer un fichier image d'une disquette, copiez le contenu de la disquette dans un fichier. Vous pouvez utiliser la commande suivante : dd [if=/dev/fd0] [of=/tmp/floppy.image]. Ici, « dd » lit le disque du périphérique « /dev/fd0 » et enregistre le résultat dans le fichier spécifié « /tmp/floppy.image ». Réglez les paramètres selon vos besoins spécifiques (périphérique de saisie, etc.)

MS Windows

Vous pouvez utiliser l'outil « RawWrite for Windows ».



Sélectionnez l'onglet « Read » à partir de ce menu. Entrez (ou choisissez) le nom du fichier dans lequel vous désirez copier le contenu de la disquette. Cliquez sur le bouton « Copy » pour commencer le processus de création de l'image. Pour des outils de même type, visistez le site du « fdos project » à **(http://www.fdos.org).**

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:33:56 AM

Images CD-ROM/ISO 9660

UNIX et systèmes d'exploitation de type UNIX

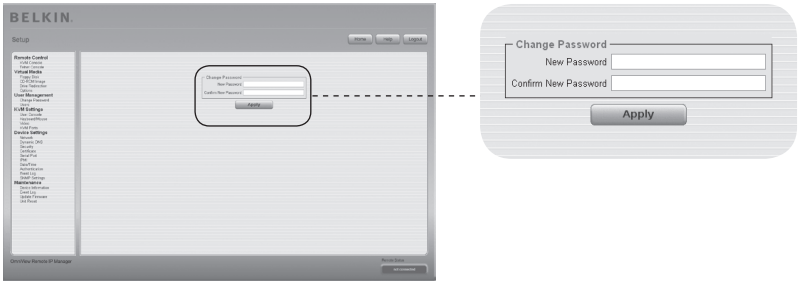
Pour créer un fichier image, utilisez « dd ». Il s'agit d'un des utilitaires d'origine
UNIX et est livré avec tout système d'exploitation de type UNIX (UNIX, Sun Solaris, Linux). Pour créer une image d'un CD-ROM, copiez le contenu du CD-ROM dans un fichier. Vous pouvez utiliser la commande suivante :
dd [if=/dev/cdrom] [of=/tmp/cdrom.image].
Ici, « dd » lit le disque du périphérique « /dev/cdrom » et enregistre le résultat dans le fichier spécifié « /tmp/cdrom.image ». Réglez les paramètres selon vos besoins spécifiques (périphérique de saisie, etc.)

MS Windows

Pour créer le fichier image, servez-vous de votre outil de création d'image de CD favori. Copier le contenu du disque en un seul fichier image ISO sur votre disque dur. Par exemple, avec « Nero », choisissez « Copy and Backup » et allez à la section « Copy Disc ». Sélectionnez le lecteur de CD-ROM ou de DVD dont vous désirez créer une image ISO. Sépcifiez le nom du fichier de l'image ISO et enregistrer le contenu du CD-ROM dans ce fichier.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:33:57 AM

Changer de mot de passe

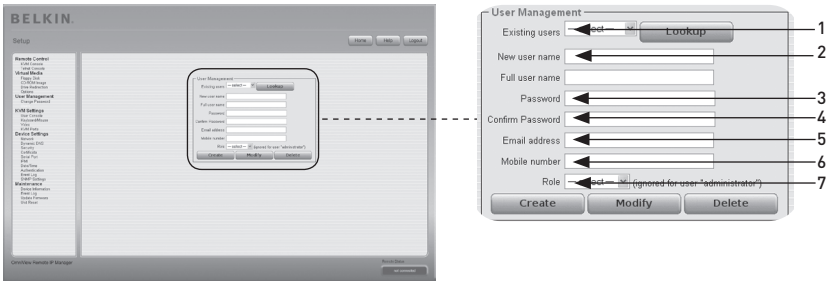


Pour modifier le mot de passe, entrez le nouveau mot de passe dans le champ de saisie du haut. Saisissez de nouveau le mot de passe dans le champ du dessous.

Cliquez sur « Apply [Appliquer] » pour enregistrer vos modifications.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:33:57 AM

Utilisateurs



Gestion des utilisateurs

la CIPD comprend un compte utilisateur pré-configuré pour l'administrateur, avec des permissions fixes. L'utilisateur possède tous les droits pour la configuration de l'unité et l'utilisation de toutes les fonctions de la CIPD. Par défaut, le nom d'utilisateur est « administrator » et le mot de passe « belkin ». N'oubliez pas de changer le mot de passe immédiatement après avoir installé la CIPD et y avoir accédé pour la première fois. Une liste complète des options disponibles suit. Cette liste ne peut être vue que par l'administrateur.

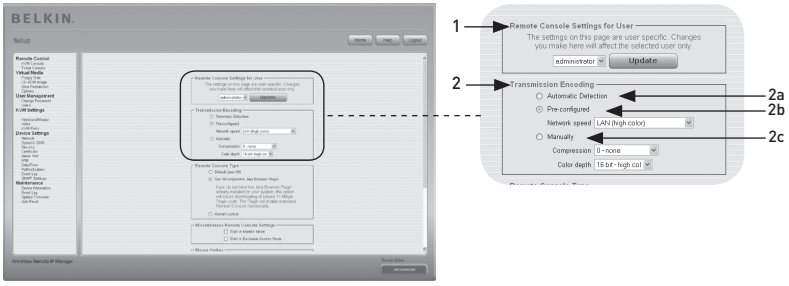
1. **Existing Users (utilisateurs existants)**
   Sélectionnez un utilisateur existant pour modification. Une fois sélectionné, cliquez sur le bouton « Lookup [Rechercher] » afin d'afficher des informations sur cet utilisateur.
2. **New Username (nouveau nom d'utilisateur)**
   Le nouveau nom d'utilisateur pour le compte sélectionné.
3. **Password (mot de passe)**
   Le mot de passe pour le nom d'utilisateur. Il doit comporter au moins quatre caractères.
4. **Confirm Password (confirmer le mot de passe)**
   Confirmation du mot de passe ci-dessus.
5. **Email Addres (adresse e-mail)**
   Facultatif.
6. **Mobile Number (numéro de portable)**
   Facultatif.
7. **Role (rôle)**
   En plus d'être un administrateur ou un utilisateur régulier, chaque utilisateur peut être membre d'un groupe (un « rôle »). Choisissez le rôle désiré à partir de la boîte de sélection. Pour créer un nouvel utilisateur, appuyez sur le bouton « Create [Créer] ». Le bouton « Modify [Modifier] » permet de changer les paramètres de l'utilisateur affiché. Pour supprimer un utilisateur, appuyez sur le bouton « Delete [Supprimer] ».

   Remarque : la CIPD possède un processeur et une unité mémoire indépendants de l'hôte, avec une limite quant au traitement des instructions et l'espace mémoire. Pour garantir un temps de réponse acceptable,
   Belkin recommande de NE PAS dépasser un total de 25 utilisateur connectés simultanément à la CIPD. L'espace mémoire disponible sur la CIPD dépend de la configuration et de l'usage de la CIPD (entrées dans le journal, etc.).

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:33:58 AM

User Console (console de l'utilisateur)

Les paramètres suivants se rapportent à l'utilisateur. Ceci veut dire que l'administrateur peut régler ces paramètres pour chaque utilisateur. La modification des paramètres pour un utilisateur n'affecte pas les paramètres des autres utilisateurs.



1. **Remote Console Settings for User (paramètres de console distante pour l'utilisateur)**
   Cette boîte de sélection affiche l'identifiant de l'utilisateur dont les valeurs sont affichées et pour qui les modifications seront prises en compte. Sélectionnez l'utilisateur désiré dans la boîte de sélection et appuyez sur le bouton « Update [Mise à jour] ». Ceci fera afficher les paramètres utilisateur indiqués ci-dessous.

   Remarque : Vous ne pouvez modifier les paramètres des autres utilisateurs que si vous possédez les droits d'accès requis pour cette tâche. Un utilisateur ordinaire ne peut le faire sans les permissions requises pour modifier les paramètres de tout autre utilisateur.

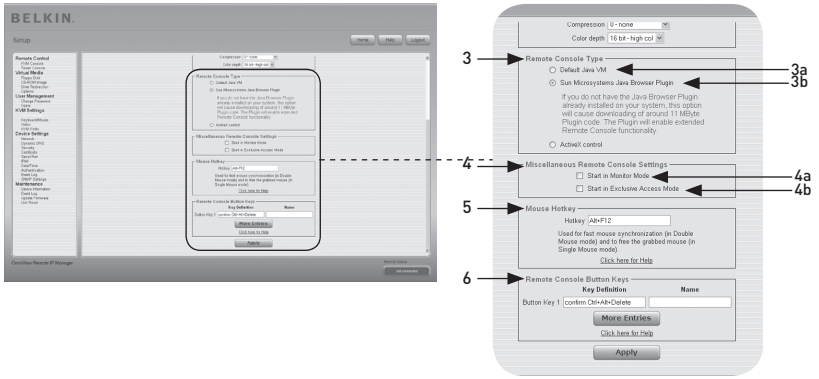
2. **Transmission Encoding (encodage de transmission)**
   Le paramètre d'« Encodage de transmission » vous permet de modifier l'algorithme d'encodage d'image qui transmet les données vidéo à l'écran de la console distante. Il vous permet d'optimiser la vitesse de l'écran distant selon le nombre d'utilisateurs simultanés et de la bande passante de la ligne de connexion (modem, RNIS, ADSL, LAN, etc.).

   2a. Automatic Detection (détection automatique)
   L'encodage et le niveau de compression sont déterminés automatiquement à partir de la bande passante disponible et le contenu actuel de l'image vidéo.

   2b. Pre-Configured Settings (paramètres préconfigurés)
   Les paramètres pré-configurés offrent le meilleur résultat en raison de l'ajustement optimal de la compression et de la profondeur d'échantillonnage pour le débit réseau indiqué.

   2c. Manual Configuration (configuration manuelle)
   Ceci vous permet d'ajuster le débit de compression et la profondeur d'échantillonnage individuellement. Selon le débit de compression sélectionné, le flux de données entre la CIPD et la console distante seront compressés afin de préserver la bande passante. Puisque les débits de compression élevés sont chronophages, ils ne doivent pas être utilisés lorsque plusieurs utilisateurs accèdent à la CIPD simultanément. La profondeur d'échantillonnage par défaut est 16 bits (65 536 couleurs). Les autres profondeurs d'échantillonnage sont réservés aux connexions réseau plus lentes, afin de permettre une transmission des données plus rapide. Ainsi, le niveau de compression 0 (aucune compression) utilise une profondeur d'échantillonnage de 16 bits. Pour les bandes passantes réduites, le 4 bits (16 couleurs) et le 2 bits (quatre échelles de gris) sont recommandés pour les interfaces standard. Les images de type photo présentent de meilleurs résultats avec une profondeur d'échantillonnage de 4 bits. La profondeur de 1 bit (noir/blanc) ne devrait être utilisé que pour les connexions réseau extrêmement lentes.

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:33:59 AM



3. **Remote Console Type (type de console distante)**
   Indique quel visionneur de console distante sera utilisé.

   3a. Default Java Virtual Machine (machine virtuelle Java (JVM) par défaut)
   Cette fonction utilise la JVM par défaut de votre navigateur Web, soit la JVM de Microsoft pour Internet Explorer ou la JVM Sun.

   3b. Sun Microsystems Java Browser Plug-In (plugin navigateur Java de Sun Microsystems)
   Ce plugin donne la consigne au navigateur Web de votre système administrateur d'utiliser la JVM de Sun Microsystems. La JVM du navigateur est utilisée pour exécuter le code de la fenêtre Console distante puisque cette dernière est, en fait, une appliquette Java. Si vous cochez cette case pour la première fois sur votre système d'administration et que le plugin Java approprié n'est pas encore installé sur votre système, il sera automatiquement téléchargé et installé. Toutefois, pour que l'installation soit possible, vous devez répondre « Oui » aux fenêtres de dialogue appropriées. Le volume à télécharger est d'environ 11 Mo. Il est avantageux de télécharger la JVM Sun puisqu'elle offre une JVM stable et identique sur des plateformes différentes. Le logiciel de la Console distante est optimisé pour cette version de la JVM et offre plus de fonctionnalités lorsqu'elle est utilisée.

4. **Miscellaneous Remote Console Settings (paramètres divers de la Console distante)**

   4a. Start in Monitor Mode (démarrer en mode Moniteur)
   Ce paramètre vous permet de sélectionner la valeur initiale pour le mode moniteur. Par défaut, le mode moniteur est désactivé. Si vous l'activez, la fenêtre de la console distante s'affiche en mode lecture seule au démarrage.

   4b. Start in Exclusive-Access Mode (démarrer en mode d'Accès exclusif)
   Ceci active le mode d'accès exclusif au démarrage de la console distante. Ce paramètre force la fermeture de la console distante pour tous les autres utilisateurs. Aucun autre utilisateur ne pourra ouvrir la console distante en même temps, à moins que vous ne désactiviez la fonction ou que vous vous déconnectiez.

5. **Mouse Hot Key (raccourci-clavier souris)**
   Le raccourci-clavier souris vous permet de déterminer une combinaison de touches au clavier pour démarrer le processus de synchronisation de la souris (en entrant la combinaison sur la console distante) ou pour le mode à une souris.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:34:00 AM

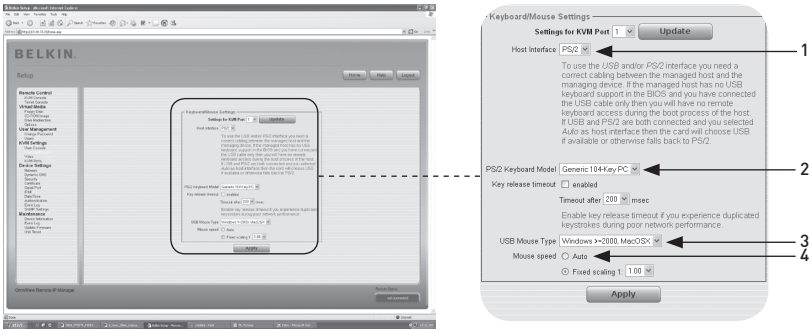
6. **Remote Console Button Keys (clavier à touches de la console distante)**
   Le clavier à touches simule les frappes ne pouvant être générées localement, sur le système distant. Cela peut être nécessaire s'il manque une touche ou si le système d'exploitation local de la console distante saisit toutes les frappes, sans conditions. Par exemple, « CTRL + ALT + SUPPR » sous Windows et DOS, sont toujours saisies, ou la séquence de touches « CTRL + EFFACEMENT » sous Linux, qui sert pour terminer le serveur X. Pour définir un nouveau clavier à touches pour en modifier un, suivez les règles qui décrivent la définition d'une touche. De façon générale, la syntaxe d'une touche va comme suit :

   [confirm] <code touche>[+|-|<[*]<code touche>]*

   Un terme entre parenthèses est facultatif. L'astérisque à la fin indique que vous devez ajouter d'autres touches au besoin, selon le cas. Le terme « confirm » ajoute un dialogue de confirmation qui s'affiche avant que les frappes puissent être envoyées à l'hôte distant. Le « code touche » est la touche à être envoyée. Vous pouvez concaténer plusieurs codes de touches avec un signe « + » ou un signe « - », ou encore un signe « < ». Le signe « + » permet de réaliser des associations de touches. Il sera nécessaire d'appuyer sur toutes les touches jusqu'à ce que vous parveniez à un signe « - » ou à la fin de la combinaison. Dans ce cas, toutes les touches sur lesquelles vous avez appuyé devront être relâchées dans l'ordre inverse. Le signe « - » permet donc de créer une demande d'appui sur une touche distincte et de la relâcher. Le signe « < » ne relâche que la dernière touche. L'astérisque insère une pause d'une durée de 100 millisecondes. Par exemple, la combinaison de touches CTRL, ALT et F2 est représentée par la séquence CTRL+ALT+F2.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:34:00 AM

Clavier/souris



1. **Host Interface (interface hôte)**
   L'Interface hôte permet l'interface de la souris là où celle-ci est branchée. Vous pouvez choisir « Auto » pour une détection automatique, « USB » pour une souris USB ou « PS/2 » pour une souris PS/2.

   Remarque : Pour utiliser l'interface USB ou PS/2, vous devez brancher le câblage approprié entre l'hôte géré et le périphérique de gestion. Si le BIOS de l'hôte géré ne prend pas en charge le clavier USB et vous n'avez branché que le câble USB, vous n'aurez aucun accès au clavier distant pendant le processus de démarrage de l'hôte. Si un clavier est branché au port USB et au port PS/2 et que le paramètre « Auto » est sélectionné, l'USB sera privilégié au démarrage si disponible. Si l'USB n'est pas disponible, le PS/2 sera sélectionné.

   Pour accéder au clavier USB distant pendant le processus de démarrage de l'hôte, les conditions suivantes doivent être remplies :

   - le BIOS de l'hôte doive prendre en charge les claviers USB
   - le câble USB doit être branché ou sélectionné dans l'option « Interface hôte ».

2. **PS/2 Keyboard Model (modèle clavier PS/2)**
   Ceci vous permet de choisir une disposition de clavier, tel que « Generic 101-Key PC » pour une disposition standard, « Generic 104-Key PC » pour une disposition standard avec trois touches Windows supplémentaires, « Generic 106-Key PC » pour un clavier japonais et « Apple Macintosh » pour le clavier Macintosh®. Si une temporisation du clavier est requise, sélectionnez l'option appropriée et déterminez la valeur de temporisation dans le champ de saisie.

3. **USB Mouse Type (souris de type USB)**
   Ceci active la souris de type USB. Choisissez l'option appropriée dans la boîte de sélection. Pour une description détaillée du type de souris et les options recommandées pour divers systèmes d'exploitation, veuillez consulter la section « Paramètres de souris recommandés » en page 21 du manuel de l'utilisateur.

*Cette fonction ne fonctionne que sous les systèmes d'exploitation Windows.

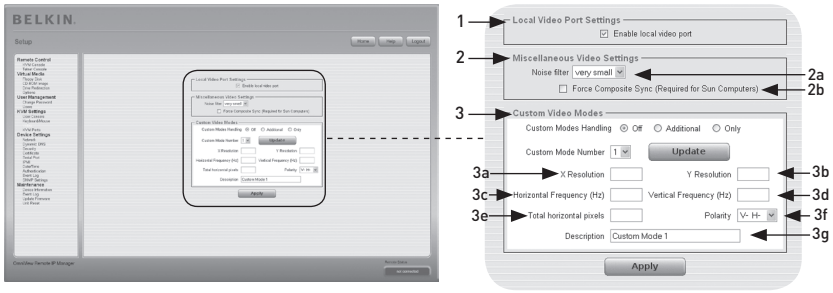
P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:34:01 AM

4. **Mouse Speed (vitesse de la souris)**
   - **Auto Mouse Speed (vitesse de souris automatique)**
     Utilisez cette option si les paramètres souris de l'hôte mettent déjà en œuvre un paramètre d'accélération. la CIPD détecte l'accélération et la vitesse de la souris pendant le processus de synchronisation de la souris.
   - **Fixed Mouse Speed (vitesse de souris fixe)**
     Utilisez cette option pour une traduction directe des mouvements de la souris entre le pointeur local et le pointeur distant. Vous pouvez également déterminer une mise à l'échelle fixe, qui indique le déplacement du pointeur de la souris distante, lorsque le pointeur de la souris locale est déplacé d'un pixel. Cette option ne fonctionne que lorsque les paramètres de la souris sur l'hôte sont linéaires, c'est-à-dire lorsqu'il n'y a aucune accélération de la souris.

   Pour enregistrer les options, « Apply [Appliquer] ».

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:34:01 AM

Vidéo



Pour enregistrer les options (voir ci-dessous), « Apply [Appliquer] ».

1. **Local Video Port Settings (paramètres du port vidéo local)**

   Enable Local Video Port (activer le port vidéo local
   Cette option surveille la sortie vidéo locale de la CIPD et indique si elle est active et transite via le signal en entrée venant du système hôte.

2. **Miscellaneous Video Settings (paramètres vidéo divers)**

   2a. Noise Filter (filtre de bruit)
   Cette fonction définit la réaction de la CIPD aux petits changements dans le signal vidéo en entrée. Un filtre large nécessite un trafic réseau moins dense et permet un affichage vidéo plus rapide, mais les petits changements à différents endroits de l'affichage peuvent ne pas être reconnus immédiatement. Un filtre étroit affiche tous les changements instantanément mais entraîne un trafic réseau constant et très dense, peu importe si le contenu affiché ne varie pas beaucoup (selon la qualité du signal vidéo en entrée).

   2b. Force Composite Sync (forcer la synchronisation composite – requis avec les ordinateurs Sun)
   Pour la prise en charge de la transmission du signal d'une machine Sun, activez cette option.
   Si cette fonction n'est pas activée, l'image de la console distante ne sera pas visible.

3. **Custom Video Modes (modes vidéo personnalisés)**
   Le nombre maximum de résolutions vidéo personnalisées est quatre.

   L'option « Gestion des modes personnalisés » vous permet de désactiver les modes personnalisés (« Off »), ou déterminer des résolutions standard ou exclusives (« Only »). Une dernière option (« Additional ») vous permet de forcer un mode vidéo spécifique pour la CIPD. Pour modifier les paramètres du mode vidéo personnalisé, choisissez le chiffre approprié dans la boîte de sélection et appuyez sur le bouton « Update [Mise à jour] ». Vous devrez entrer des informations supplémentaires de sorte que le mode vidéo puisse être reconnu correctement :

   Avertissement: L'option « Host Monitor Settings [Paramètres moniteur de l'hôte] » est réservé aux utilisateurs aguerris. Une utilisation incorrecte peut diminuer les performances de transmission vidéo. Assurez-vous de comprendre la fonction de A à Z avant de modifier les paramètres moniteur de l'hôte.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:34:01 AM

3a. X Resolution (résolution X)
Réfère au nombre de pixels horizontaux visibles.

3b. Y Resolution (résolution Y)
Réfère au nombre de pixels verticaux visibles.

3c. Horizontal Frequency (fréquence horizontale) (Hz)
Réfère à la fréquence horizontale (ligne) en hertz.

3d. Vertical Frequency (fréquence verticale) (Hz)
Réfère à la fréquence verticale (rafraîchissement) en hertz.

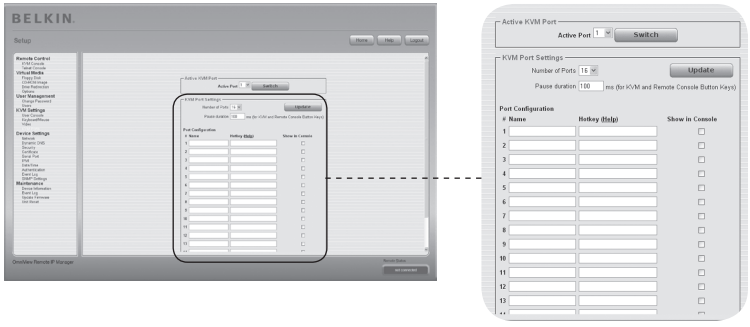
3e. Total horizontal pixels (pixels horizontaux totaux)
Réfère aux nombre total de pixels par ligne, y compris les zones invisibles et d'occultation.

3f. Polarity (polarité)
Réfère à la polarité positive ou négative des signaux de synchronisation. V indique une polarité verticale, H indique une polarité horizontale.

3g. Description
Entrez ici un nom pour ce mode, qui s'affiche dans la console distante si un mode personnalisé est activé.

Ports KVM

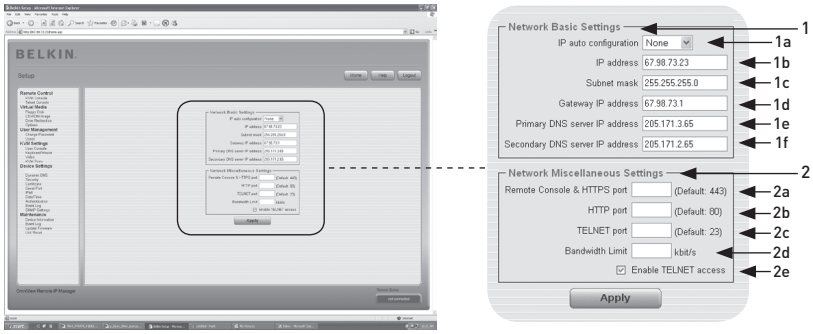
Il est possible de choisir le nombre de ports utilisés par le switch KVM connecté. Vous pouvez même leur attribuer des noms. Pour pouvoir effectuer une permutation des ports KVM via la CIPD, vous devez définir des associations de touches pour les ports.



P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:34:02 AM

Network (réseau)

La fenêtre « Network Settings [Paramètres réseau] » (ci-dessous) vous permet de modifier les paramètres réseau, tel qu'expliqué ci-dessous. Une fois appliqués, les nouveaux paramètres réseau sont pris en compte immédiatement.



Avertissement : Modifier les paramètres réseau de la CIPD peut entraîner la perte de la connexion réseau. Si vous modifiez les paramètres à distance, assurez-vous que toutes les valeurs sont correctes de manière à pouvoir continuer à accéder à la CIPD.

1. **Paramètres réseau de base**
   - **1a. IP Auto Configuration (configuration automatique de l'IP)**
     Sert à définir l'emplacement où la CIPD puise ses paramètres réseau, comme un serveur DHCP ou BOOTP. Pour le DHCP, sélectionnez « DHCP » ; pour le BOOTP sélectionnez « BOOTP ». Si vous choisissez « none [aucun] », la configuration automatique de l'IP est désactivée.
   - **1b. L'adresse IP** est attribuée par votre administrateur réseau.
   - **1c.** Le terme **« Subnet Mask [Masque de sous-réseau] »** réfère au masque réseau du réseau local, qui sert à déterminer le sous-réseau auquel une adresse IP appartient.
   - **1d. Gateway IP Address (adresse IP de passerelle)**
     Si l'on doit pouvoir accéder à la CIPD à partir de réseaux autres que le réseau local, définissez cette adresse IP avec l'adresse IP du routeur du réseau local.
   - **1e. Primary DNS Server IP Address (adresse IP du serveur DNS principal)**
     Il s'agit de l'adresse IP du serveur de noms de domaines (DNS) principal en notation pointée. Vous pouvez laisser cette option vide. Cependant, la CIPD ne pourra pas effectuer une résolution du nom.
   - **1f. Secondary DNS Server IP Address (adresse IP du serveur DNS secondaire)**
     Réfère à l'adresse IP du serveur DNS secondaire en notation pointée. Elle servira si le serveur DNS principal ne peut être contacté.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:34:03 AM

2. **Paramètres réseau divers**

   2a. Remote Console and HTTPS Port (console distante et port HTTPS)
   Il s'agit du numéro de port « écouté » par le serveur de la console distante de la CIPD et le serveur HTTPS. S'il est vide, la valeur par défaut est employée.

   2b. HTTP Port (port HTTP)
   Il s'agit du numéro de port « écouté » par le serveur HTTP de la CIPD. S'il est vide, la valeur par défaut est employée.

   2c. HTTP Telnet (port HTTP)
   Il s'agit du numéro de port « écouté » par le serveur Telnet de la CIPD. S'il est vide, la valeur par défaut est employée.

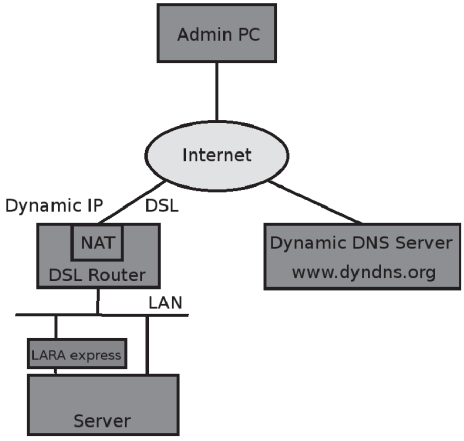
   2d. Bandwidth Limit (limite de la bande passante)
   Réfère au trafic réseau maximum généré par le dispositif Ethernet de la CIPD (en Kbps).

   2e. Enable Telnet Access (activer l'accès Telnet)
   Permet aux utilisateurs d'accéder à la CIPD au moyen de la passerelle Telnet (voir « Console Telnet » en page 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:34:03 AM

DNS Dynamique

Un service Dynamic DNS libre (dyndns.org) peut être utilisé dans le cas suivant :



Cas Dynamic DNS

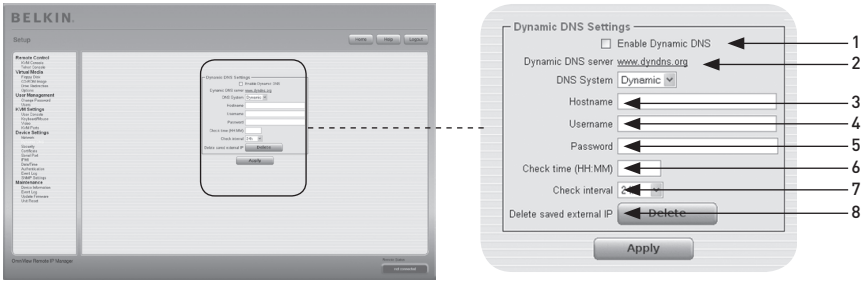
Vous pouvez atteindre la CIPD via l'adresse IP du routeur ADSL, qui assigné dynamiquement par le fournisseur. Puisque l'administrateur ne connaît pas l'adresse IP attribuée par le fournisseur, la CIPD se connecte à un serveur DNS dynamique spécial à intervalles réguliers et y enregistre son adresse IP. L'administrateur également peut contacter ce serveur et prendre la même adresse IP appartenant à la CIR. L'administrateur doit enregistrer un CIPD pour utiliser le serveur de DNS dynamique et y attribuer un certain nom d'hôte. Un nom d'utilisateur et un mot de passe seront attribués pendant le processus d'enregistrement. Ces indentifiants, ainsi que le nom d'hôte, sont requis pour déterminer l'adresse IP de la CIPD enregistré.

Vous devez effectuer la procédure suivante afin d'activer le DNS dynamique :

- Assurez-vous que l'interface LAN de la CIPD est configurée adéquatement.
- Entrez les paramètres DNS dynamique tel que montré en page 55.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:34:03 AM

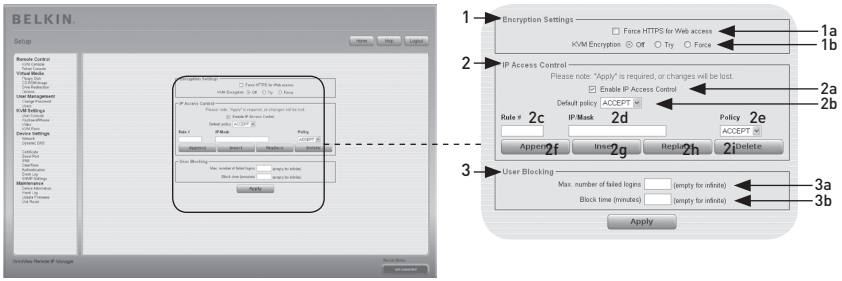
Paramètres DNS dynamique



1. **Enable Dynamic DNS (activer le DNS dynamique)**
   Active le service DNS dynamique Nécessite l'adresse IP d'un serveur DNS configuré.
2. **Dynamic DNS Server (serveur DNS dynamique)**
   la CIPD s'y enregistre à intervalles réguliers. Au moment de publier, le DNS dynamique est un paramètre fixe puisque dyndns.org est le seule service pris en charge.
3. **Host Name (nom d'hôte)**
   « RIPM » est le nom d'hôte fourni par le DNS dynamique. Utilisez le nom entier, y compris le domaine, c'est-à-dire « testserver.dyndns.org » (ou « RIPM. dyndns.org ») et non pas uniquement le nom d'hôte.
4. **Username (nom d'utilisateur)**
   Pendant l'enregistrement manuel avec le DNS dynamique, vous devez avoir enregistré ce nom d'utilisateur.
   Remarque : Les espaces ne sont pas acceptés dans le nom d'utilisateur.
5. **Password (mot de passe)**
   Pendant l'enregistrement manuel avec le DNS dynamique, vous devez avoir enregistré ce mot de passe.
6. **Check Time (temps de vérification)**
   La carte de la CIPD s'enregistre elle-même dans le DNS dynamique au « temps de vérification ».
7. **Check Interval (intervalle de vérification)**
   Il s'agit de l'intervalle pendant lequel la CIPD se rapporte au DNS dynamique.
   Remarque : la CIPD possède sa propre horloge temps-réel indépendante. Assurez-vous que le temps de la CIPD est réglé correctement.
8. Servez-vous de l'option **« Delete saved external IP [Supprimer IP externe enregistrée] »** Si vous désirez mettre à jour votre adresse IP externe enregistrée. Pour supprimer une adresse enregistrée, appuyez sur le bouton « Delete [Supprimer] ».

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:34:04 AM

Sécurité



1. **Paramètres de chiffrement**

   1a. Force HTTPS (forcer HTTPS)
   Si cette option est activée, l'accès à l'interface Web est uniquement possible en utilisant une connexion HTTPS. la CIPD n'« écoutera » pas via le port HTTP pour des connexions entrantes. Si vous désirez créer votre propre certificat SSL pour identifier la CIPD, veuillez consulter la section « Certificat » en page 58

   1b. Chiffrement KVM
   Cette option contrôle le chiffrement du protocole RFB (Remote Frame Buffer). La console distante utilise le RFB pour transmettre les données de l'écran à la machine de l'administrateur, et les données clavier/souris à l'hôte en retour. Si l'option est réglée à « Off », aucun chiffrement n'est utilisé. Si l'option est réglée à « Try (essayer) », l'appliquette tente d'établir une connexion chiffrée. Si la connexion ne peut être établie, une connexion non chiffrée est utilisée. Si l'option est réglée à « Force (forcer) », l'appliquette tente d'établir une connexion chiffrée. Si la connexion échoue, le système génère un relevé d'erreur.

2. **Contrôle d'accès IP**
   Cette section explique les paramètres relatifs au contrôle d'accès IP. Ce paramètre sert à limiter l'accès à un certain nombre déterminé de clients. Ces clients seront identifiés par l'adresse IP avec laquelle ils tentent d'établir une connexion.

   Avertissement : Les paramètres de contrôle d'accès IP s'appliquent à l'interface LAN uniquement.

   2a. Enable IP-Access Control (activer le contrôle d'accès IP)
   Active le contrôle d'accès basé sur les adresses IP source.

   2b. Default Policy (règle par défaut)
   Cette option contrôle la mesure à prendre avec les paquets IP qui arrivent et qui ne correspondent pas aux règles configurées. Ils peuvent être acceptés ou refusés.

   Avertissement : Si vous avez choisi l'option « DROP » (refuser) et qu'aucune règle « ACCEPT » (accepter) n'est configurée, l'accès au Web par le LAN est impossible. Pour réactiver l'accès, vous pouvez modifier les paramètres de sécurité via le modem ou en désactivant le contrôle d'accès IP temporairement, avec la procédure de configuration initiale.

   2c. Rule Number (numéro de la règle)
   Doit contenir le numéro d'une règle à laquelle s'appliqueront les commandes suivantes. S'il s'agit d'une nouvelle règle, veuillez ignorer ce champ.

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:34:04 AM

2d. IP/Mask (IP/masque)
Indique l'adresse IP ou la plage d'adresses IP à laquelle la règle s'applique. Exemples (le numéro concaténé à une adresse IP avec un ' / ' correspond au nombre de bits valides de l'adresse IP donnée qui sera utilisé) :

192.168.1.22/32 correspond à l'adresse IP 192.168.1.22

192.168.1.0/24 correspond à tous les paquets IP dont les adresses source vont de 192.168.1.0 à 192.168.1.255

0.0.0.0/0 correspond à n'importe quel paquet IP

2e. Policy (règle)
La règle détermine la marche à suivre avec les paquets correspondants. Ils peuvent être acceptés ou refusés.

Avertissement : L'ordre des règles est important. Les règles sont vérifiées en ordre ascendant jusqu'à ce qu'une règle correspondante est trouvée. Toutes les règles situées sous la règle correspondante seront ignorées. La règle par défaut s'applique si aucune règle correspondante n'a été trouvée.

2f. Appending a Rule (ajouter une règle)
Entrez l'IP et le masque et enregistrez la règle. Pour terminer, appuyez sur le bouton « Append [Ajouter] ».

2g. Inserting a Rule (insérer une règle)
Entrez le numéro de la règle, ainsi que l'IP/masque. Enregistrez la règle. Pour terminer, appuyez sur le bouton « Insert [Insérer] ».

2h. Replacing a Rule (remplacer une règle)
Entrez le numéro de la règle, ainsi que l'IP/masque. Enregistrez la règle. Pour terminer, appuyez sur le bouton « Replace [Remplacer] ».

2i. Deleting a Rule (supprimer une règle)
Entrez le numéro de la règle et appuyez sur le bouton « Delete [Supprimer] ».

3. User Blocking (verrouillage d'utilisateur)
Le mécanisme de verrouillage d'utilisateur permet à l'administrateur de désactiver un utilisateur en particulier si son mot de passe a été saisi incorrectement un certain nombre de fois. La durée du verrouillage peut également être configurée.

3a. Maximum Number of Failed Logins (nombre maximum d'échecs de connexion)
Entrez le nombre maximum de tentatives de connexions échouées après lesquelles un utilisateur est verrouillé. Laissez ce champ vide pour désactiver la fonction de verrouillage d'utilisateur.

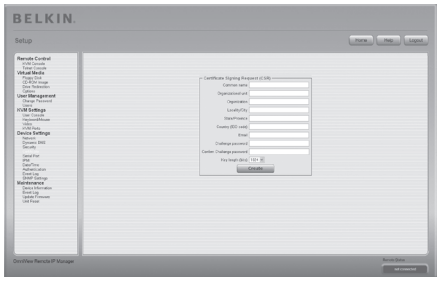
3b. Block Time (durée du verrouillage)
Nombre de minutes pendant lesquelles l'utilisateur est verrouillé après qu'il ou elle ait dépassé le nombre de maximum d'échecs de connexion. Laissez ce champ vide pour verrouiller cet utilisateur jusqu'à ce qu'il ou elle soit déverouillé(e) manuellement.

Unblocking Users (déverrouillage des utilisateurs)
Il y a deux façons de déverrouiller un utilisateur verrouillé.

- Un utilisateur parent peut aller aux paramètres de gestion des utilisateurs (voir la section correspondante) et appuyer sur le bouton « Unblock [Déverrouiller] » pour cet utilisateur.
- Un administrateur peut utiliser la console série pour la configuration initiale et se connecter en tant que l'utilisateur « déverrouillé ». la CIPD demandera le mot de passe administrateur et présentera une liste d'utilisateurs verrouillé qui peuvent être déverrouillés.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:34:04 AM

Certificat



Paramètres de certification

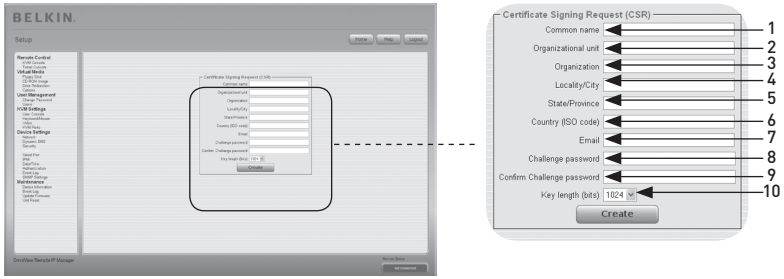
la CIPD utilise le protocole SSL pour les transmissions réseau chiffrées entre lui-même et un client connecté. Lors de l'établissement de la connexion, la CIPD doit indiquer son identité à un client en se servant d'un certificat de chiffrement. À la livraison du produit, ce certificat et sa clé secrète est identique pour tous les CIPD qui seront produits et ne correspondra pas à la configuration réseau qui sera appliquée à la CIPD par son utilisateur. La clé secrète du certificat sert également pour assurer le handshake SSL. Il est possible de générer et installer un nouveau certificat base64 x.509, unique à un CIPD en particulier. Pour ce faire, la CIPD peut générer une nouvelle clé de chiffrement et le CSR (Certificate Signing Request) associé, qui doit être certifié par une autorité de certification (AC). Cette dernière vérifie que vous êtes bien qui vous prétendez être. Ensuite, elle signe et émet un certificat SSL pour vous. Pour créer et installer un certificat SSL pour la CIPD, procédez comme suit :

- Créez un CSR SSL au moyen du tableau montré ci-dessous. Vous devrez remplir un certain nombre de champs, lesquels sont expliqués ci-dessous. Ensuite, cliquez sur le bouton « Create [Créer] » afin d'initier la création du CSR. Le CSR peut être téléchargé sur l'ordinateur de l'administrateur à l'aide du bouton « Download CSR [Télécharger CSR] ».
- Envoyez la CSR à l'autorité de certification pour obtenir la certification. Vous recevrez le nouveau certificat de la part de l'AC.
- Téléchargez le certificat en amont vers la CIPD au moyen du bouton « Create [Créer] ».

Après avoir effectué ces trois étapes, la CIPD possède maintenant son propre certificat qui permettra d'identifier la carte auprès de ses clients.

Avertissement : Si vous détruisez le CSR de la console, vous ne pourrez plus la récupérer ! Si vous l'effacez par mégarde, répétez les trois étapes de la procédure.

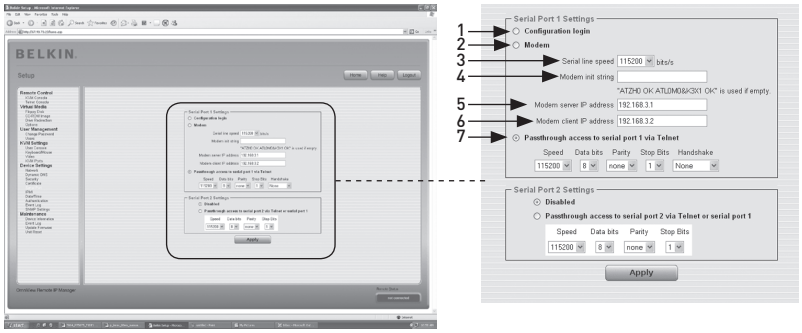
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:34:05 AM



1. **Common Name (nom courant)**
   Il s'agit du nom réseau de la CIPD après son installation dans le réseau de l'utilisateur (habituellement le nom de domaine complet). Ce nom est identique au nom qui sert pour accéder à la CIPD avec un navigateur Web, sans toutefois utiliser le préfixe http://. Si l'on accède à la CIPD via le HTTPS, et si le nom donné ici et le nom du réseau sont différents, le navigateur fera apparaître un avertissement lié à la sécurité.
2. **Organizational Unit (unité organisationnelle)**
   Ce champ indique le département de l'organisation auquel la CIPD appartient.
3. **Organization (organisation**
   Nom de l'entreprise à laquelle la CIPDappartient.
4. **Locality/City (ville)**
   Ville où l'organisation est situé.
5. **State/Province (état/province)**
   L'état ou la province où l'organisation est située.
6. **Country (pays - code ISO)**
   Pays où est situé l'organisation (code ISO à 2 lettres, par exemple : US pour États-Unis).
7. **Challenge Password (mot de passe)**
   Certains organismes de certification exigent la vérification du mot de passe pour autoriser les modifications ultérieures du certificat (comme sa révocation, par exemple). Le mot de passe doit contenir au minimum quatre caractères.
8. **Confirm Challenge Password (confirmer le mot de passe)**
   Saisissez de nouveau le mot de passe.
9. **E-mail**
   Il s'agit de l'adresse e-mail d'une personne-ressource responsable de la CIPD et sa sécurité.
10. **Key Length (longueur de la clé)**
    Longueur de la clé générée en bits. La plupart du temps, 1024 bits suffisent. Des clés plus longues peuvent ralentir la réponse de la CIPD pendant l'établissement d'une connexion.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:34:05 AM

Serial Port (port série)



Les paramètres série de la CIPD vous permettent d'indiquer le périphérique connecté au port série et comment l'utiliser. Pour accéder à l'interface série, vous aurez besoin d'un câble inverseur.

1. **Configuration or Console Login (configuration ou connexion à la console)**
   N'utilisez pas le port série pour n'importe quelle fonction spéciale ; ne l'utilisez que pour la configuration initiale.
2. **Modem**
   la CIPD permet un accès distant en utilisant une ligne téléphonique en plus de l'accès standard par l'intermédiaire de la carte Ethernet intégrée. Le modem doit être connecté à l'interface série de la CIPD. Logiquement, la connexion à la CIPD par la ligne téléphonique revient à établir une connexion poste à poste depuis l'ordinateur jusqu'à la CIPD. En d'autres mots, la CIPD agit comme un fournisseur d'accès à Internet (FAI) auquel vous vous connectez. La connexion est établie à l'aide du protocole PPP (Point-to-Point). Avant de pouvoir vous connecter à la CIPD, vous devez vous assurer que votre ordinateur console est correctement configuré. Par exemple, sous Windows, vous pouvez configurer une connexion d'accès réseau à distance dont les valeurs par défaut correspondent aux paramètres qui conviennent (comme PPP). La fenêtre des paramètres du modem vous permet de configurer l'accès distant à la CIPD au moyen d'un modem. La signification de chaque paramètre est décrite ci-dessous. Les paramètres du modem font partie du tableau des paramètres série.
3. **Serial-Line Speed (débit de la ligne série)**
   Débit de communication entre la CIPD et le modem. La plupart des modems d'aujourd'hui prennent en charge la valeur par défaut de 115 200 bps. Si vous utilisez un modèle ancien et que vous rencontrez des problèmes, réduisez ce débit.
4. **Modem Init String (chaîne d'initialisation du modem)**
   Chaîne d'initialisation utilisée par la CIPD pour initialiser le modem. La valeur par défaut fonctionne avec tous les modems standard directement connectés à une ligne téléphonique. Si vous disposez d'un modem spécial ou si le modem est connecté à un commutateur téléphonique local qui exige une séquence de numérotation spéciale pour établir la connexion au réseau téléphonique public, vous pouvez changer ce paramètre et entrer une nouvelle chaîne. Référez-vous à la section du manuel de votre modem à propos de la syntaxe de la commande AT.

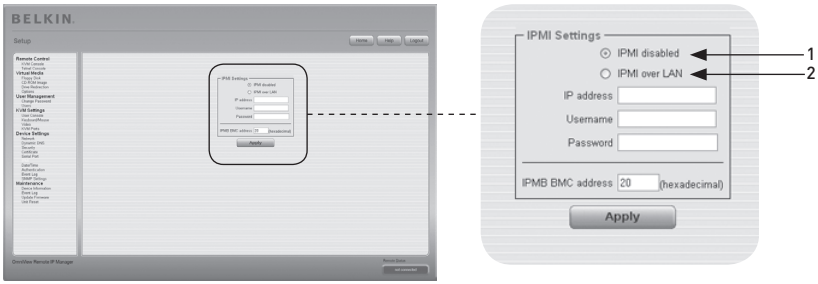
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:34:06 AM

5. **Modem Server IP Address (adresse IP serveur du modem)**
   Cette adresse IP sera attribuée à la CIPD pendant le handshake PPP. Étant donné qu'il s'agit d'une connexion IP poste à poste, il est possible d'utiliser pratiquement n'importe quelle adresse IP. Vous devez toutefois vous assurer qu'elle est conforme aux paramètres IP de la CIPD et de son ordinateur. La valeur par défaut fonctionne dans la majorité des cas.
6. **Modem Server IP Address (adresse IP client du modem)**
   Cette adresse IP sera attribuée à votre console pendant le handshake PPP. Étant donné qu'il s'agit d'une connexion IP poste à poste, il est possible d'utiliser pratiquement n'importe quelle adresse IP. Vous devez toutefois vous assurer qu'elle est conforme aux paramètres IP de la CIPD et de son ordinateur. La valeur par défaut fonctionne dans la majorité des cas.
7. **Pass-Through Access to Serial Port via Telnet (accès pass-through au port série via Telnet)**
   Cette option vous permet de vous connecter à tout périphérique branché sur le port série et d'y accéder (s'il permet la prise en charge de terminal) via Telnet. Choisissez les options adaptées au port série et utilisez la console Telnet ou un client Telnet standard pour vous connecter su CIPD. Pour en savoir plus sur l'interface Telnet, consultez la section « Console Telnet ».

   Remarque : Visitez www.belkin.com pour une liste des modems compatibles.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:34:06 AM

Interface intelligente de gestion de plateforme (IPMI)



L'IPMI de la CIPD offre d'autres manières d'allumer ou d'éteindre le système ou d'effectuer un redémarrage à froid. Qui plus est, ces options vous permettent de voir un journal des événements du système hôte et l'état de certains capteurs du système (par ex. : la température). Si votre système hôte prend en charge l'IPMI, vous pouvez y accéder de l'une des façons suivantes :

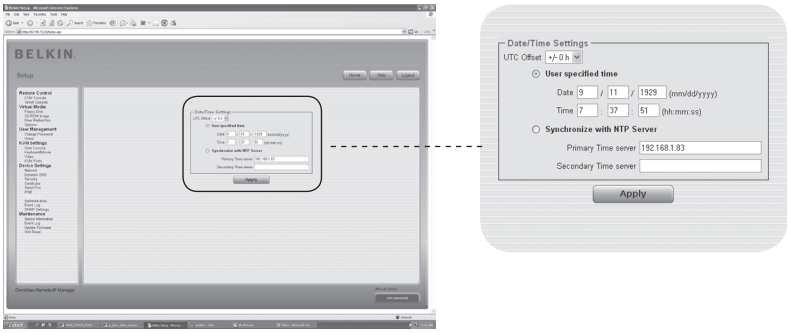
- IPMI sur LAN (IPMI v1.5 requis)
- Paramètres IPMI

L'illustration ci-dessus montre le tableau des paramètres IPMI de la CIPD. Ses options sont décrites ci-dessous.

1. **IPMI Disabled (IPMI désactivé)**
   Désactive l'IPMI sur la CIPD. Ceci veut dire que l'État via IPMI et le Journal des événements via IPMI ne sont disponibles ; les fonctions de mise sous/hors tension et de redémarrage n'utilisent pas l'IPMI, mais plutôt l'ATX (Advanced Technologie Extended) ; le câble de redémarrge est connecté de la CIPD vers la carte-mère.
2. **IPMI over LAN (IPMI sur LAN)**
   Vous pouvez également connecter l'IPMI sur une connexion LAN. La condition pour ce type d'accès est un système hôte avec IPMI v1.5 et un adaptateur réseau avec une connexion à bande latérale au contrôleur BMC (baseboard management controller)
   (habituellement intégré). Dans les paramètres IPMI, vous devez entrer l'adresse IP de ce système hôte et le mot de passe requis pour la connexion LAN. Vous pouvez également accéder à d'autres systèmes IPMI en entrant leurs adresses IP respectives.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:34:06 AM

Date et heure

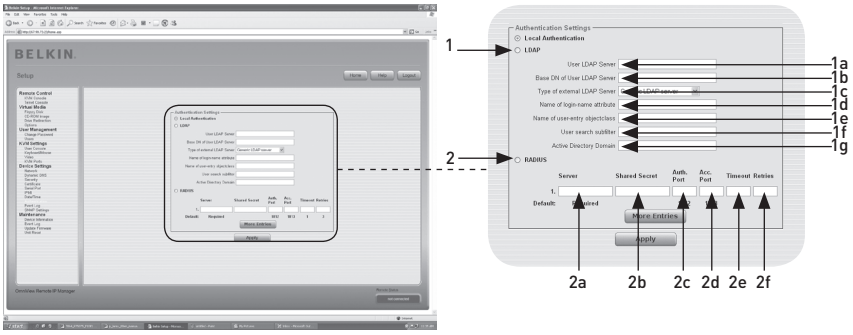


Ce lien réfère à une page où il est possible de régler l'horloge en temps réel de la CIPD. Vous pouvez régler l'horloge manuellement ou au moyen d'un serveur temps NTP (Network Time Protocol). Sans l'aide d'un serveur temps, votre réglage du temps peut ne pas être continu ; vous devrez alors le régler chaque fois où la CIPD est victime d'une coupure de courant de plus de quelques minutes. Pour éviter cette situation, vous pouvez utiliser un serveur temps NTP, qui règle l'horloge interne au temps universel coordonné (UTC). Puisque le serveur temps NTP est toujours au UTC, il y a un paramètre pour régler votre décalage et ainsi obtenir votre heure locale.

Avertissement : Il n'existe aucune façon de régler automatiquement l'heure d'été. Vous devez régler le décalage UTC deux fois l'an, selon la réglementation de votre pays.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:34:07 AM

Authentification



la CIPD vous permet d'utiliser une authentification local ou conserver l'information dans un protocole LDAP (Lightweight Directory Access Protocol) central ou sur un serveur RADIUS (Remote Authentication Dial-In User Service). Pour le LDAP ou le RADIUS, vous devez donner des informations dans le tableau des paramètres d'authentification. Pour en savoir plus sur le LDAP et le RADIUS, voir ci-dessous.

1. LDAP

1a. User LDAP Server (utilisateur serveur LDAP)
Entrez le nom ou l'adresse IP du serveur LDAP qui contient toutes les entrées utilisateurs. Si vous choisissez d'entrer un nom au lieu d'un adresse IP, vous devrez configurer un serveur DNS dans les paramètres réseau.

1b. Base DN of User LDAP Server (base DN de serveur utilisateurs LDAP)
Spécifiez le nom distinctif (DN) où commence l'arbre de répertoires sur le serveur utilisateurs LDAP.

1c. Type of External LDAP Server (type de serveur LDAP externe)
Définissez le type de serveur LDAP externe. Ceci est nécessaire car certains types de serveurs nécessitent une procédure spécifique. De plus, les valeurs par défaut du programme LDAP sont définies correctement. Vous pouvez choisir entre un Generic LDAP Server, un Novell Directory Service et un Microsoft Active Directory. Si vous ne possédez pas de Novell Directory Service ni de Microsoft Active Directory, choisissez alors un Generic LDAP Server et modifiez le programme LDAP (voir ci-dessous).

1d. Name of Login-Name Attribute (attribut du nom ou du nom de connexion)
Il s'agit du nom de l'attribut comprenant le nom de connexion unique d'un utilisateur. Pour utiliser la valeur par défaut, laissez ce champ vide. La valeur par défaut dépend du type de serveur LDAP sélectionné.

1e. Name of User-Entry Object Class (nom de classe d'objets des utilisateurs)
Il s'agit de la classe d'objets qui identifie un utilisateur dans le répertoire LDAP. Pour utiliser la valeur par défaut, laissez ce champ vide. La valeur par défaut dépend du type de serveur LDAP sélectionné.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:34:08 AM

1f. User Search Sub-Filter (sous-filtre de recherche des utilisateurs)
Vous pouvez ici préciser la recherche d'utilisateurs qui doivent être connus de la CIPD.

1g. Active Directory Domain (domaine Active Directory)
Représente le domaine du répertoire actif configuré dans le serveur Microsoft Active Directory. Cette option n'est valide que si vous avez choisi Microsoft Active Directory comme type de serveur LDAP.

2. Remote Authentication Dial In User Service (RADIUS)
Le RADIUS est un protocole spécifié par le groupe de travail Internet Engineering Task Force (IETF). Il y a deux spécifications entrant dans le protocole RADIUS : l'authentification et la comptabilisation. Ces fonctions tendent vers une authentification, une configuration et une comptabilisation centralisées des services de connexion vers un serveur indépendant. Le protocole RADIUS existe sous plusieurs implémentations, telles que « free RADIUS », « open-RADIUS » ou RADIUS sur systèmes UNIX. Le protocole est testé et spécifié rigoureusement. Nous pouvons vous recommander tous les produits ci-dessus, en particulier le « free RADIUS ».

Remarque : À l'heure actuelle, nous n'offrons pas de prise en charge challenge/réponse. Une réponse « Access Challenge » est vue et perçue comme une « Access Reject ».

Pour accéder à une unité distante au moyen d'un protocole RADIUS, vous devez vous connecter. Vous serez invité à entrer un nom d'utilisateur et un mot de passe. Le serveur RADIUS lit les données saisies (authentification) et la CIPD recherche votre profil (autorisation). Le profil définit (ou limite) vos actions et peut varier selon votre cas particulier. Si aucun profil n'existe, votre accès via RADIUS sera refusé. En termes de mécanismes d'activité à distance, la connexion via RADIUS fonctionne comme la console distante. S'il n'y a pas d'activité pendant 30 minutes, votre connexion à la CIPD est interrompue et fermée.

2a. Server (serveur)
Entrez l'adresse IP ou le nom d'hôte du serveur RADIUS devant être connecté. Si vous utilisez un nom d'hôte, le DNS doit être configuré et activé.

2b. Shared Secret (secret partagé)
Un secret partagé est une chaîne de caractères texte qui sert de mot de passe entre le client et le serveur RADIUS. la CIPD agit comme un client RADIUS. Un secret partagé sert à vérifier que les messages RADIUS sont envoyés par une unité RADIUS qui est configuré avec le même secret partagé et pour vérifier que le message RADIUS n'a pas été modifié pendant la transmission (pour en vérifier l'intégrité). Pour le secret partagé, vous pouvez utiliser tous les caractères alphanumériques standards et les caractères spéciaux. Un secret partagé peut comprendre jusqu'à 128 caractères et peut contenir des lettres majuscules ou minuscules (A-Z, a-z), des chiffres (0-9) et autres symboles (caractères non définis comme étant des lettres ou des chiffres), tel un point d'exclamation (!) ou un astérisque (*).

2c. Authentication Port (port d'authentification)
Port auquel le serveur RADIUS « écoute » pour les requêtes d'authentification. La valeur par défaut est 1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:34:08 AM

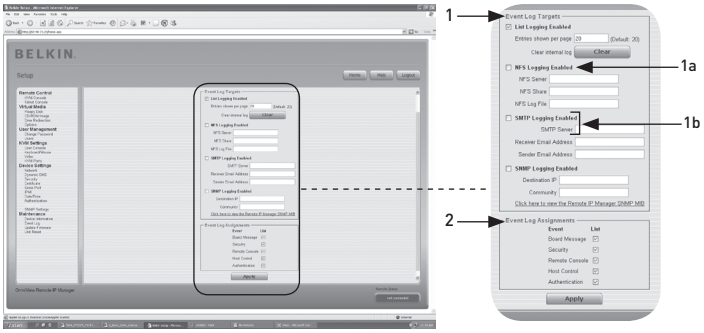
2d. Accounting Port (port de comptabilisation)
Port auquel le serveur RADIUS « écoute » pour les requêtes de comptabilisation. La valeur par défaut est 1813.

2e. Timeout (temporisation)
Définit la durée de vie d'une requête en secondes. La durée de vie est le temps d'attente pour la complétion de la requête. Si la tâche associée à la requête n'est pas complétée avant la fin de l'intervalle de temps, la tâche est annulée. La valeur par défaut est une seconde.

2f. Retries (retransmissions)
Définit le nombre de retransmissions si une requête n'a pu être complétée. La valeur par défaut est trois.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:34:08 AM

Journal des événements



Les événements importants, comme un échec de connexion ou une mise à jour du micrologiciel, sont consignées dans diverses destinations de journalisation. (illustration 6-33). Chaque événement appartient à un groupe, qui peuvent être activés séparément. La façon habituelle de noter les événements est d'utiliser le journal des événements interne de la CIPD. Pour montrer la liste des journaux, cliquez sur « Event Log [Journal des événements] » à la page d'Entretien. Sous Event Log Settings [Paramètres de journalisation des événements], vous pouvez choisir combien d'entrées seront montrées par page. Vous pouvez également effacer le contenu du journal des événements.

1. **Event Log Targets (cibles du journal des événements)**
   Pour enregistrer des événements, vous pouvez utiliser la liste de la CIPD. Pour montrer la liste des journaux, cliquez sur « Event Log [Journal des événements] » à la page d'Entretien. Puisque la mémoire système de la CIPD sert à sauvegarder toutes les informations, le nombre d'entrées maximum dans le journal est 1000. Chaque entrée au-delà de cette limite efface l'entrée la plus ancienne.

   Avertissement : Si le bouton de réinitialisation de l'interface HTML est utilisé pour redémarrer la CIPD, toutes les informations consignées seront sauvegardées de façon permanente et seront disponibles après le redémarrage de la CIPD. Si la CIPD subit une coupure de courant ou si un redémarrage à froid est effectué, toutes les entées consignées seront perdues. Pour éviter cela, procédez comme suit :

   1a. Network File System (NFS) Logging Enabled (activer la journalisation NFS)
   Définissez un serveur NFS vers lequel les répertoires et les liens fixes doivent être exportés ; toutes les données de journalisation y seront ensuite consignées dans un fichier. Pour consigner des données de plusieurs CIPD vers une seule ressource NFS, vous devez définir un nom de fichier unique à chaque unité CIPD. Lorsque vous modifiez les paramètres NFS et appuyez sur le bouton « Apply [Appliquer] », la ressource NFS sera introduite immédiatement. Cela veut dire que la ressource NFS et le serveur NFS doivent comporter des sources valides, sinon un message d'erreur apparaît.

   Remarque : À l'opposé du journal des événements interne de la CIPD, la taille du journal NFS n'est pas limitée. Chaque événement sera consigné à la fin du fichier, sa taille augmentant ainsi au fur et à mesure. Vous aurez peut-être besoin de le supprimer ou de retirer certains événements à l'intérieur du fichier de temps à autre.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:34:09 AM

1b. Paramètres SNMP

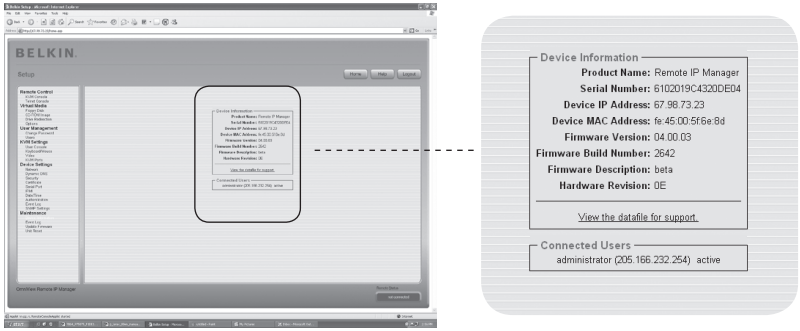
Simple Mail Transfer Protocol (SMTP) Logging Enabled (activer la journalisation SMTP)
Avec cette option, la CIPD est en mesure d'envoyer un message à une adresse électronique spécifiée dans le champ e-mail des paramètres de journalisation des événements. Ces e-mails contiennent les mêmes informations que le journal des événements interne, et le sujet du message contient le groupe d'événements auquel appartient l'événement en question. Pour utiliser cette destination de journalisation, vous devez spécifier un serveur SMTP pouvant être rejoint à partir de la CIPD et pour lequel aucune authentification est requise (<ipserveur>:<port>).

SNMP Logging Enabled (
Si cette option est activée, la CIPD envoie une interruption SNMP vers une adresse IP spécifiée chaque fois qu'un événement est consigné. Si le destinataire requiert une chaîne communautaire, vous pouvez la définir dans le champ approprié. La plupart des interruptions contiennent une chaîne descriptive, renfermant toutes les informations relatives à l'événement. L'authentification et l'alimentation de l'hôte possèdent leur propre interruption standard, crée automatiquement, qui consiste en plusieurs champs renfermant des informations sur l'événement. Pour recevoir cette interruption SNMP, servez-vous ne n'importe quel détecteur (« listener ») d'interruptions SNMP.

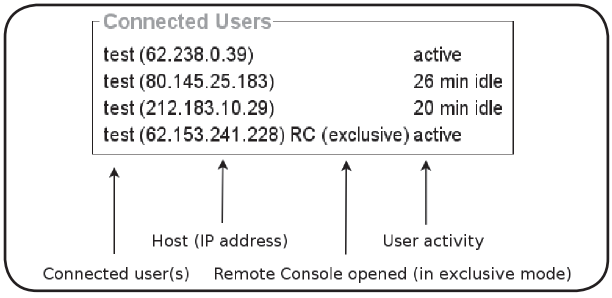
2. **Event Log Assignments (affectations de la journalisation des événements)**
Vous pouvez choisir les actions de la CIPD qui seront sauvegardées dans le fichier journal des événements. Cochez les cases désirées et cliquez sur « Apply [Appliquer] » pour confirmer votre sélection.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:34:09 AM

Information sur l'unité



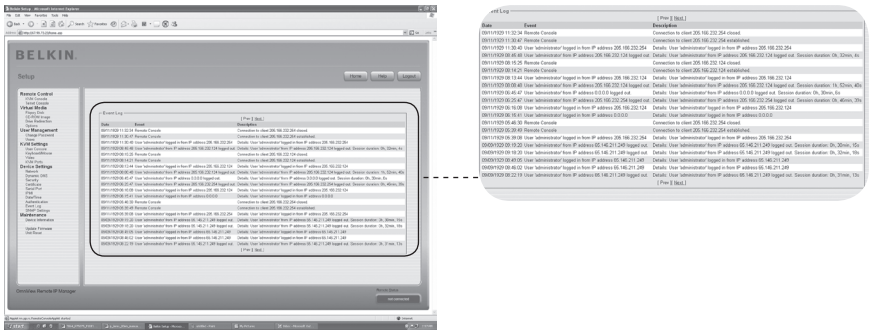
Cette section contient le récapitulatif des informations concernant la CIPD et son micrologiciel et vous permet, en outre, de le réinitialiser. Le fichier de données d'assistance vous permet de télécharger le fichier de données de la CIPD comprenant des informations spécifiques. Il s'agit d'un fichier XML (eXtensible Markup Language) avec des informations personnalisées, telles que le numéro de série.



L'illustration ci-dessus montre l'activité de la CIPD. De gauche à droite, s'affichent les utilisateurs connectés, l'adresse IP de l'utilisateur hôte et l'état de la CIPD. « RC » indique que la console distante est ouverte. Si la console distante est ouverte en mode exclusif, le terme « (exclusive mode) » apparaît également. Pour en savoir plus sur les paramètres de surveillance seulement et d'accès exclusif, voir la section Barre de contrôle de la console distante en page 23 de ce manuel de l'utilisateur. Pour afficher l'activité par utilisateur, la dernière colonne contient soit le terme « active » (actif) pour indiquer un utilisateur actif, ou « 20 min idle » pour indiquer qu'un utilisateur est inactif depuis un temps donné.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:34:09 AM

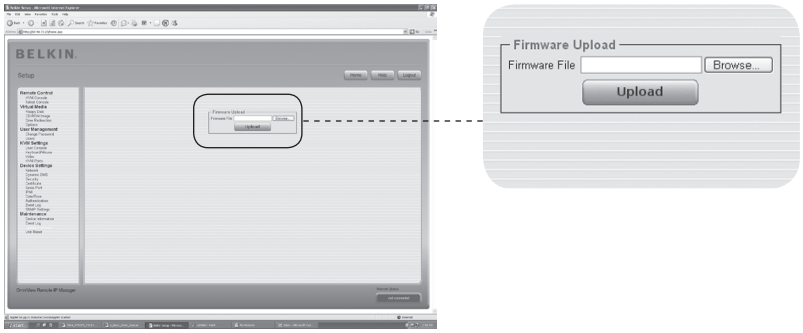
Journal des événements



La liste « Event Log [Journal des événements] » comprend les événements consignés par la CIPD, avec la date, une courte description et l'adresse IP de l'origine de la requête de l'événement. Vous pouvez utiliser les boutons « Prev [Précédent] » ou « Next [Suivant] » pour parcourir les données.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:34:10 AM

Mise à jour du micrologiciel



la CIPD est une ordinateur entièrement autonome, possédant son propre micrologiciel inscrit dans sa mémoire morte (ROM). Le micrologiciel de la CIPD peut être mis à jour à distance, afin d'installer de nouvelles fonctions ou des fonctions améliorer ainsi que des fonctions spéciales. Un fichier de mise à jour est un fichier binaire qui doit être téléchargé à partir du site Web Belkin. Si le fichier est compressé (si l'extension du fichier est .zip), vous devez le décompresser avant de procéder à la mise à jour. Sous Windows, vous pouvez vous servir du logiciel WinZip (http://www.winzip.com/) pour décompresser le fichier de mise à jour.

Remarque : Pour mettre à jour le micrologiciel de la CIPD, vous devez sauvegarder le fichier du nouveau micrologiciel sur le système avec lequel vous vous connectez à la CIPD.

La mise à jour du micrologiciel se déroule en trois étapes :

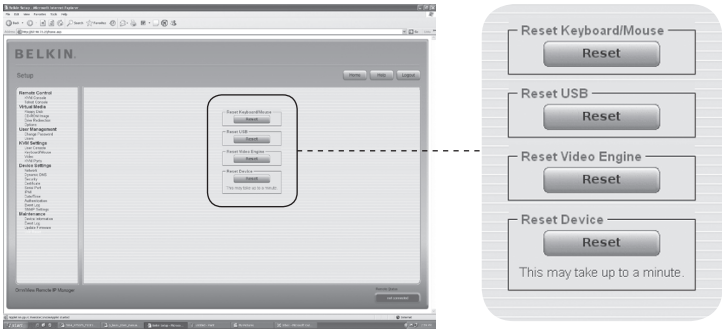
1. Téléchargez en amont le fichier du nouveau micrologiciel sur la CIPD. Pour ce faire, sélectionnez le fichier sur votre système local au moyen du bouton « Browse [Parcourir] ». Ensuite, cliquez sur « Upload [Télécharger] » pour transférer vers la CIPD le fichier sélectionné précédemment. Après le téléchargement du micrologiciel, la CIPD vérifie automatiquement sa validité et confirme qu'aucune erreur de transmission n'est survenue. Si une erreur survient, la mise à jour est avortée et le micrologiciel actuel demeure intact.
2. Si le téléchargement est réussi, la fenêtre de mise à jour du micrologiciel apparaît. La fenêtre affiche le numéro de la version du micrologiciel en fonction et le numéro de la version du micrologiciel téléchargé. Cliquez sur « Update [Mise à jour] » pour remplacer l'ancienne version avec la nouvelle.

   Avertissement : Ce processus est irréversible et prend habituellement plusieurs minutes. Assurez-vous que la CIPD ne subisse aucune coupure de courant pendant la mise à jour. Si une coupure survient, la CIPD peut devenir instable.
3. Après la mise à jour du micrologiciel, la CIPD redémarre automatiquement. Après environ une minute, vous serez redirigé vers la page de connexion pour l'ouverture d'une session.

   Avertissement : Le processus de mise à jour en trois étapes et la vérification exclut pratiquement toute possibilité d'erreur pendant la mise à jour. Toutefois, la mise à jour du micrologiciel devrait être réservée au personnel qualifié ou aux administrateurs. La prévention des coupures dans l'alimentation de la CIPD pendant la mise à jour est d'une importante capitale.

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:34:10 AM

Réinitialisation de l'unité



Cette section décrit les méthodes de réinitialisation de parties spécifiques de l'unité, comme le clavier et la souris, le moniteur de l'ordinateur auquel la CIPD est branché et la CIPD lui-même. Pour activer le nouveau micrologiciel, vous devez réinitialiser (redémarrer) la CIPD. Ce processus ferme toutes les connexions en cours avec la console d'administration et la CIPD, et prend environ 30 secondes. La réinitialisation d'unités secondaires (comme la vidéo) ne prend quelques secondes et n'entraîne pas de déconnexions. Pour redémarrer un CIPD en particulier, cliquez sur le bouton « Reset [Réinitialisation] » tel que montré ci-haut.

Remarque : Seul l'administrateur peut redémarrer la CIPD.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:34:11 AM

La souris distante ne fonctionne pas ou n'est pas synchrone.

D'abord, vérifiez la connexion VGA. la CIPD et le moniteur local doivent prendre en charge la même résolution vidéo. Assurez-vous que les paramètres de la souris conviennent à votre souris (PS/2 ou USB). Aussi, le modèle de souris doit être envoyé à la CIPD et au système d'exploitation de l'hôte (l'ordinateur branché à la CIPD). Dans certains cas, la synchronisation de la souris peut entraîner des erreurs. Consultez la section « Configuration du clavier, de la souris et du moniteur » au chapitre 3 pour en savoir plus.

La vidéo est de mauvaise qualité ou granuleuse.

Utilisez l'entrée du menu « Reset [Réinitialisation] » pour rétablir les valeurs par défaut de la CIPD. Ensuite, cliquez sur le bouton « Auto-Adjust [Ajustement automatique] » pour sélectionner une sortie vidéo. Vérifier le branchement des câbles vidéo.

Échec de la connexion à la CIPD.

Vérifiez l'exactitude de votre nom d'utilisateur et de votre mot de passe. Le nom d'utilisateur par défaut est « administrator » et le mot de passe par défaut est « belkin ». Assurez-vous que votre navigateur est configuré de façon à accepter les témoins (cookies).

La fenêtre console distante de la CIPD ne s'ouvre pas.

Assurez-vous que le Java a été chargé. Un pare-feu peut empêcher l'accès à la console distante. Les ports TCP ports 80 (pour HTTP) et 443 (pour HTTPS et RFB) doivent être ouverts (le serveur avec le pare-feu doit accepter les connexions TCP entrantes sur ces ports).

La console distante ne peut se connecter et affiche une erreur de temporisation.

Vérifiez la configuration de votre matériel et de votre réseau. S'il y a un serveur proxy entre la CIPD et votre hôte, vous ne pouvez transférer des données vidéo avec le RFB. Établissez une connexion directe entre la CIPD et le client. De plus, vérifiez les paramètres de la CIPD et choisissez un port serveur différent pour le transfert RFB. Si vous utilisez un pare-feu, vérifiez le port approprié pour l'acceptation des connexions. Vous pouvez restreindre ces connexions aux adresses IP utilisées par la CIPD et votre client.

Aucune connexion ne peut être établie avec la CIPD.

Vérifiez le matériel. Est-ce que la CIPD est sous tension ? Vérifiez la configuration de votre réseau (adresse IP, routeur). Envoyez un « ping » à la CIPD afin de vérifier s'il peut être rejoint via le réseau.

Des combinaisons de touches(ALT+F2, ALT+F3, etc.) sont interceptées par le système de la console et ne sont pas transmises à l'hôte.

Définissez un clavier à touches. Vous pouvez le faire dans les paramètres de la console distante (voir Barre de contrôle de la console distante en page 23).

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:34:11 AM

Les pages Web de la CIPD ne s'affiche pas correctement.

Vérifiez les paramètres de la cache de votre navigateur. Assurez-vous que les paramètres cache ne son PAS réglés à « never check for newer pages » (ne jamais rechercher de nouvelles pages). Sinon, les pages de la CIPD sont chargées à partir de la cache et non pas de la CIPD, ce qui entraîne le problème.

Windows XP ne quitte pas le mode veille.

Le problème vient probablement de Windows XP. Essayez de ne pas déplacer le pointeur de la souris pendant qu'XP passe en mode veille. Veuillez consulter le manuel de votre système d'exploitation pour en savoir plus.

Chaque fois que j'ouvre la fenêtre de dialogue de la console distante, les pointeurs des souris ne sont plus synchronisés.

Désactivez le paramètre « Automatically move mouse pointer to the default button of dialog boxes [Déplacer le pointeur de la souris vers le bouton par défaut des boîtes de dialogue] » dans les paramètres souris de votre système d'exploitation.

La console distante affiche un écran noir.

Vérifiez si la CIPD est alimenté par le bus USB uniquement. S'il n'y a pas assez d'alimentation via l'USB, la console distante s'ouvre mais affiche un écran noir. Vérifiez les paramètres CIPD en page 26 de ce manuel de l'utilisateur. Vérifier le branchement des câbles vidéo.

Les données vidéo du moniteur local sont entourées d'une bordure noire.

Ceci n'est pas un défaut. Le moniteur local est programmé selon un mode vidéo fixe qui peut être sélectionné dans les paramètres vidéo de la CIPD. Référez à la section Barre de contrôle de la console distante en page 23 de ce manuel de l'utilisateur.

J'ai oublié mon mot de passe. Comment puis-je rétablir les paramètres par défaut de la CIPD ?

Vous pouvez utiliser l'interface série. Pour une description détaillée, voir la section Rétablissement des paramètres d'origine de la Console IP de prise en main à distance en page 31 de ce manuel de l'utilisateur.

Veuillez consulter le site web www.belkin.com pour de l'assistance et voir la liste des matériels compatibles avec la CIPD.

Remarque : Si aucune de ces solutions n'a réussi à corriger le problème, veuillez communiquer avec l'assistance technique Belkin.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:34:11 AM

Déclaration FCC

Déclaration de conformité à la réglementation FCC en matière de compatibilité électromagnétique

Nous, Belkin Corporation, sis au 501 West Walnut Street , Compton CA, 90220, États-Unis, déclarons sous notre seule responsabilité que le produit :
F1DE101H

auquel se réfère la présente déclaration, est conforme aux normes énoncées à l'alinéa 15 de la réglementation de la FCC. Le fonctionnement est assujetti aux deux conditions suivantes: (1) cet appareil ne peut pas provoquer d'interférence nuisible et (2) cet appareil doit accepter toute interférence reçue, y compris des interférences pouvant entraîner un fonctionnement non désiré.

Déclaration de conformité CE
Nous, Belkin Corporation, déclarons que le produit F1DE101H auquel se rapporte la présente déclaration, a été élaboré dans le respect des normes d'émissions EN55022 ainsi que des normes d'immunité EN55024, LVP EN61000-3-2 et EN61000-3-3 en vigueur.

ICES
This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Garantie limitée de 2 ans du produit de Belkin Corporation

Couverture offerte par la garantie
Belkin Corporation garantit à l'acheteur initial de ce produit Belkin que le produit est exempt de défauts de conception, de montage, de matériau et de fabrication.

Période de garantie.
Belkin Corporation garantit ce produit Belkin pour une période de deux ans.

Mesures correctives.
Garantie du produit
Belkin s'engage à réparer ou à remplacer gratuitement, à sa convenance, tout produit défectueux (à l'exception des frais d'expédition du produit).

Limites de la couverture offerte par la garantie
Toutes les garanties susmentionnées sont caduques si le produit Belkin n'est pas retourné à Belkin Corporation à la demande expresse de celui-ci, l'acheteur étant responsable de l'acquittement des frais d'expédition, ou si Belkin Corporation détermine que le produit Belkin a été installé de façon inadéquate, a été modifié d'une quelconque façon ou falsifié. La garantie du produit Belkin ne protège pas contre des calamités naturelles (autre que la foudre) comme les inondations, les tremblements de terre ou la guerre, le vandalisme, le vol, l'usure normale, l'érosion, l'épuisement, l'obsolescence, l'abus, les dommages provoqués par des perturbations de basse tension (baisses ou affaissements de tension, par exemple), un programme non autorisé ou une modification de l'équipement du système.

Entretien et réparation.
Vous devez prendre les mesures suivantes pour faire réparer ou entretenir votre produit Belkin :

1. Communiquez avec Belkin Corporation, au 501 W. Walnut St., Compton CA 90220, à l'attention : Customer Service (service client) ou appelez le (800)-223-5546, 15 jours maximum après l'événement. Préparez-vous à fournir les informations suivantes :
   a. Référence du produit Belkin.
   b. Lieu d'achat du produit.
   c. Date d'achat du produit.
   d. Copie de la facture d'origine.
2. Le représentant du service client Belkin vous donnera alors toutes les instructions sur la façon d'expédier votre facture et le produit Belkin et la façon de présenter votre réclamation.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:34:12 AM

6-0 Information

Belkin Corporation se réserve le droit d'examiner le produit Belkin endommagé. Tous les frais d'expédition du produit Belkin à Belkin Corporation pour inspection seront entièrement à la charge de l'acheteur. Si Belkin détermine, à son entière discrétion, qu'il est peu pratique d'expédier l'équipement endommagé à Belkin Corporation, elle peut désigner, à son entière discrétion, un atelier de réparation pour inspecter l'équipement et évaluer le coût des réparations. Les coûts, s'il en est, pour l'expédition de l'équipement jusqu'à l'atelier de réparation et le retour, et pour l'estimation, seront entièrement assumés par l'acheteur. L'équipement endommagé doit être disponible pour inspection jusqu'à ce que la demande de réclamation soit réglée. Lorsqu'un règlement intervient, Belkin Corporation se réserve le droit d'être subrogé en vertu de quelque police d'assurance que l'acheteur pourrait avoir.

Relation entre le Droit national et la garantie.
BELKIN REJETTE PAR LE PRÉSENT DOCUMENT TOUTES LES AUTRES GARANTIES, EXPLICITES OU IMPLICITES, Y COMPRIS MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES AFFÉRENTES À LA QUALITÉ LOYALE ET MARCHANDE ET À L'ADÉQUATION À UNE FIN DONNÉE.

Certains états n'autorisent pas de limite quant à la durée d'une garantie implicite; il se pourrait donc que les limites indiquées ci-dessus ne s'appliquent pas dans votre cas.

"BELKIN CORPORATION NE PEUT EN AUCUN CAS ÊTRE TENU RESPONSABLE DE DOMMAGES ACCESSOIRES, DIRECTS, INDIRECTS OU MULTIPLES, Y COMPRIS, MAIS SANS S'Y LIMITER, LA PERTE DE REVENUS OU D'AFFAIRES DÉCOULANT DE LA VENTE OU DE L'UTILISATION DE TOUT PRODUIT BELKIN, MÊME LORSQU'ELLE EST AVISÉ DE LA PROBABILITÉ DES DITS DOMMAGES.

La garantie vous confère des droits légaux spécifiques. Vous pouvez également bénéficier d'autres droits qui varient d'un pays à l'autre. Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:34:12 AM

BELKIN®

Console IP de prise en main à distance OmniView®

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, États-Unis
310-898-1100
310-898-1111 Fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Royaume-Uni
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Pays-Bas
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

Belkin Iberia
Avda Cerro del Aguila 3
28700 San Sebastián de los Reyes
Espagne
+34 9 16 25 80 00
+34 9 02 02 00 34 Fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, France
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 Fax

Belkin GmbH
Hanebergstrasse 2
80637 Munich, Allemagne
+49 (0) 89 143405 0
+49 (0) 89 143405 100 Fax

© 2006 Belkin Corporation. Tous droits réservés. Toutes les raisons commerciales sont des marques déposées de leurs fabricants respectifs. Mac OS et Macintosh sont des marques de commerce d'Apple Computer, Inc., enregistrées aux États-Unis et dans d'autres pays.

P75075ea

BELKIN®

OmniView®
Remote IP-Manager

Control

Steuerung Ihres Computers oder KVM-Switches mit einem Internet-Browser—von jedem Ort aus

EN
FR
DE
NL
ES
IT

Benutzerhandbuch

F1DE101Hea

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:34:13 AM

Inhaltsverzeichnis

Inhaltsverzeichnis

1-1 Einleitung und Verpackungsinhalt

Wir freuen uns über Ihren Kauf des Belkin OmniView Remote IP-Manager (RIPM). Der RIPM wurde für Unternehmen entwickelt, die auf einfache Weise KVM-over-IP-Technik mit vorhandenen KVM-Geräten und Servereinstellungen benutzen möchten. Der RIPM ermöglicht dies effizient und reduziert dadurch Server-Ausfallzeiten und Servicekosten erheblich. Über den Fernzugriff können Administratoren Probleme schneller rund um die Uhr lösen.

Der RIPM ist leicht in Ihr vorhandenes LAN-Netzwerk zu integrieren, egal wie groß dies ist. In diesem Benutzerhandbuch finden Sie alle Details, die Sie für die Installation und den Einsatz des RIPM und besondere Problemlösungen benötigen. Wir hoffen, Sie zu unseren zufriedenen Stammkunden zählen zu können. In kurzer Zeit werden
Sie selbst sehen, warum weltweit über eine Million Belkin OmniView-Produkte pro Jahr zum Einsatz kommen.


OmniView Remote IP Manager


PS/2 -Kabelgarnitur


VGA-Kabel


DB9 Nullkabel


Mini-USB-Kabel


Ein Netzteil (5V-Gleichstrom, 2A)


Rack-Halterungen mit


CD mit


Benutzerhandbuch


Installationsanleitung

Registrierkarte

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:34:15 AM

- **Fernzugriff über "Remote Access"**
  Der RIPM ermöglicht den Fernzugriff auf Ihre KVM-Einstellungen und alle verbundenen Server. Es kann auch ein Fernzugriff auf einzelne Computer oder Server eingerichtet werden.

- **Digitale Benutzer**
  Der RIPM ermöglicht einem digitalen Benutzer den Zugriff auf und die Kontrolle über angeschlossene KVM-Switches und Server. Außerdem können weitere 25 Benutzer gleichzeitig in Digitalgrafiken einsehen, um gemeinsam Probleme zu lösen.

- **Internetbasiert**
  Die Schnittstelle des RIPM ist internetbasiert; es kann mit jedem Computer darauf zugegriffen werden, wenn dieser mit dem LAN, WAN oder dem Internet über eine Standard TCP/IP-Verbindung verbunden ist. Für die Einrichtung ist keine zusätzliche Software erforderlich.

- **Benutzerfreundliche Bedienoberfläche**
  Die benutzerfreundliche Bedienoberfläche ermöglicht Ihnen die einfache Einrichtung und Änderung der Funktionen des RIPM. Sie benötigen einfach einen Internetbrowser und brauchen keine weitere Software zu installieren.

- **Zugriff auf das BIOS**
  Der RIPM ermöglicht Ihnen den Zugriff auf das BIOS (Basic Input/Output System) Ihrer Server für Änderungen oder Neustarts.

- **Unterstützung für serielle Geräte**
  Der RIPM bietet die Unterstützung für ein serielles Gerät, wie eine Stromverteilungseinheit (Power Distribution Unit - PDU), sodass Sie über die Fernverwaltung einen Neustart Ihrer Server durchführen können.

- **Verbesserte Sicherheit**
  Der RIPM bietet 256-Bit SSL-Verschlüsselung und Mehrfach-Kennwortschutz für den Schutz Ihrer Server.

- **Virtual Media***
  Mit der Nutzung virtueller Medien können Sie Bilder und Dateien zwischen lokalen und entfernten Computern austauschen, Software ferngesteuert laden, Patches für Anwendungen und Betriebssysteme ausführen und Diagnoseprogramme von einer CD aus ausführen.

  *Nur für Windows®-Computer.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:34:16 AM

- **Kontoverwaltung**
  Der RIPM ermöglicht dem Administrator die Einrichtung mehrer Server- und Zugriffskonten.
- **Event Log (Ereignisprotokoll)**
  Das Ereignisprotokoll zeichnet alle Aktivitäten über den RIPM auf.
- **E-Mail-Meldung**
  Der RIPM ermöglicht dem Administrator die Kontrolle der Benutzeraktivitäten und erstellt E-Mail-Meldungen bei Anmeldungen, ungültigen Anmeldungen und Abmeldungen.
- **Plattformübergreifende Technik**
  Der RIPM funktioniert mit KVM-Switches oder Servern mit PS/2- oder USB-Konsolenverbindungen.
- **Bildschirmauflösung**
  Durch die Bandbreite von 400 MHz werden Bildschirmauflösungen bis zu 1600 x 1200 / 75 Hz unterstützt.
- **Rack-Befestigung: 0 Höheneinheiten**
  Der RIPM ist so kompakt, dass es auf Ihrem Schreibtisch untergebracht oder an der Rückseite Ihres Serverschranks angebracht werden kann und keine Höheneinheiten belegt.
- **Firmware aktualisieren**
  Mit einer Flash-Aktualisierung sorgen Sie dafür, dass auf Ihrem RIPM stets die aktuellste Firmware läuft. Diese Firmwareaktualisierungen stellen sicher, dass der RIPM immer mit den aktuellsten Geräten und aktuellster Hardware kompatibel ist. Besuchen Sie für Aktualisierungsinformationen und Service unsere Website www.belkin.de.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:34:16 AM

Hardwareanforderungen

- OmniView IP-Manager (enthalten)
- PS/2-Kabelgarnitur (enthalten)
- VGA-Kabel (enthalten)
- Mini-USB-Kabel (enthalten)
- Netzteil (5 V DC, 2 A) (enthalten)
- Tastatur, Bildschirm und Maus
- Netzwerkverbindung über 10/100Base-T Ethernet-Schnittstelle (RJ45)
- CAT5-Kabel
- Rack-Halterungen mit Befestigungsschrauben (zur Montage im Rack, enthalten)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:34:16 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x und höher;
UNIX®; Mac OS® X v10.0 und höher (KVM erforderlich);
Sun™ Solaris™ 8.x und höher (mit Sun-Adapter—Belkin Artikel-Nr. F1DE083)

Unterstützte Browser

- Microsoft® Internet Explorer 6.0 und höher
- Netscape® Navigator® 7.0

P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:34:16 AM

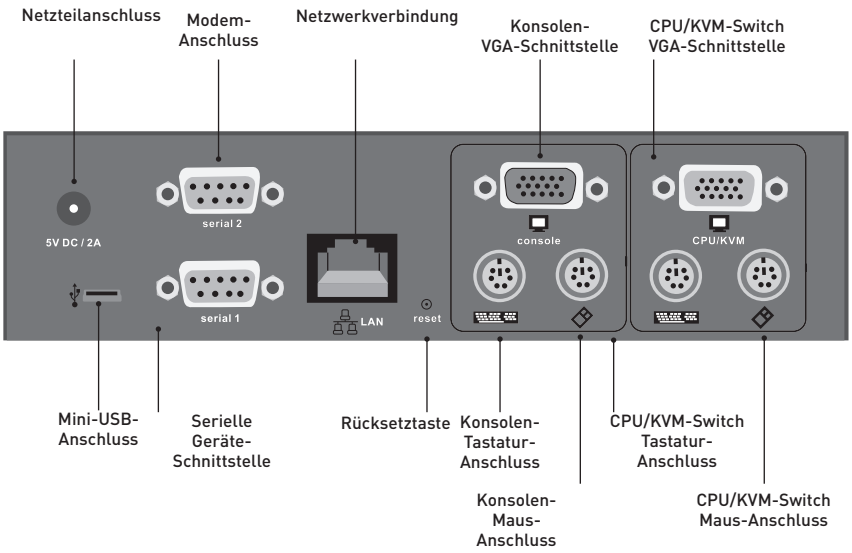
Artikelnummer:	F1DE101H
Stromversorgung:	5 V DC, 2 A
Anzahl unterstützter Benutzer:	1 lokal, 1 digital (1 Benutzer zugleich)
Tastaturemulation:	PS/2 und USB
Mausemulation:	PS/2 und USB
Unterstützte Bildschirme:	CRT und LCD (VGA-Unterstützung)
Unterstützte Auflösung:	Bis zu 1600 x 1200 / 75 Hz
Maximale Fernzugriffs-Bandbreite:	5 MB
Tastatureingang:	MiniDIN6 (PS/2)
Mauseingang:	MiniDIN6 (PS/2)
Bildschirmanschluss:	HDDB15-Buchse (VGA)
CPU-USB-Anschluss:	Mini-USB
Netzwerkverbindung:	RJ45
Verschlüsselungs-Techniken:	256-Bit SSL, 128-Bit, AES, DES, 3DES
Authentifizierung:	LDAP (über lokalen LDAP-Client), RADIUS, AD
Unterstützte Protokolle:	SNMP v1, IPv4
Serielle Geräteschnittstelle:	DB9
LED-Anzeigen:	2
Gehäuse:	Metall
Abmessungen:	171 mm (B) x 44 mm (H) x 114 mm (L)
Gewicht:	0,75 kg
Betriebstemperatur:	0° C bis 48,89° C
Lagertemperatur:	-20° C bis 60° C
Relative Luftfeuchtigkeit:	5% bis 80%
Garantie:	2 Jahre

Hinweis: Unangekündigte technische Änderungen jederzeit vorbehalten.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:34:16 AM

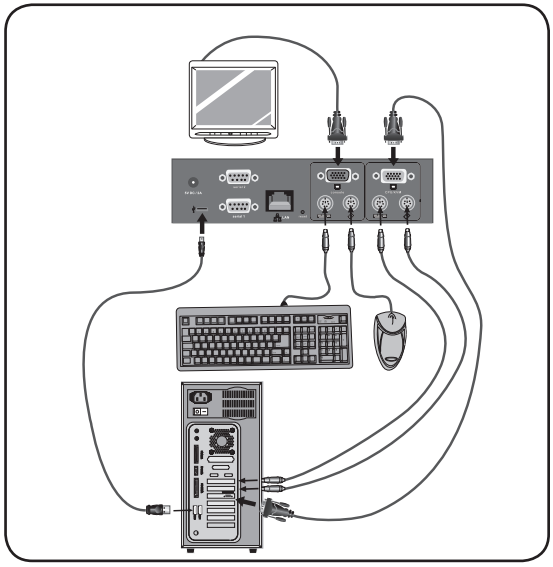
Vorderseite

Rückseite

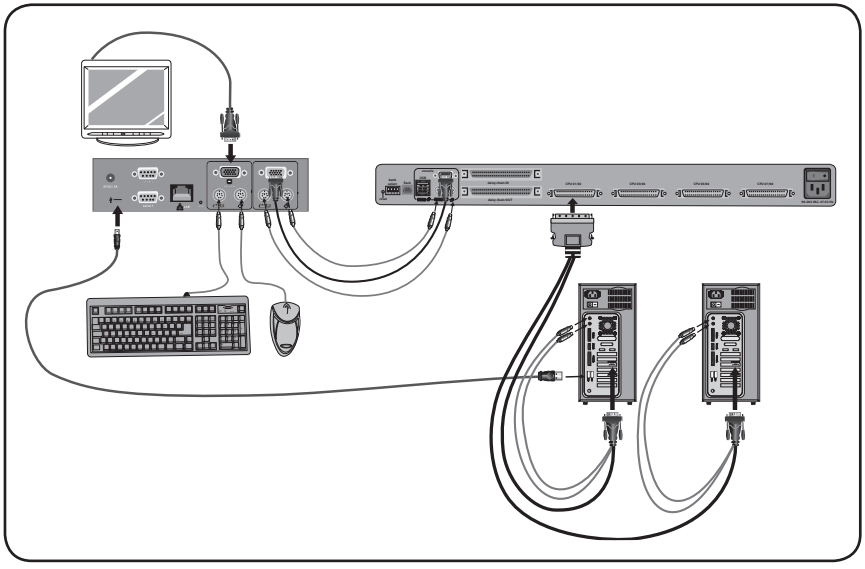


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:34:17 AM

Typische RIPM-Konfiguration mit einem Computer



Typische RIPM-Konfiguration mit einem KVM-Switch



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:34:21 AM

Schritt 1 Einbau des RIPM in ein Server-Rack

Der RIPM enthält Halterungen für den Einbau in ein 19”-Rack.

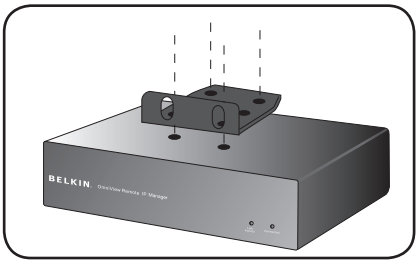


Fig. 1

1.1 Bringen Sie die mitgelieferte Halterung mit den enthaltenen Schrauben oben oder unten am RIPM an.

1.2 Befestigen Sie den RIPM im Rack. Siehe **Abb. 1.**

Hinweis: Die Befestigungsschrauben für das Rack sind nicht enthalten. Bitte verwenden Sie die vom Rack-Hersteller angegebenen Schrauben.

Achtung: Vor dem Anschluss von Geräten am RIPM oder dem/den Computer(n) muss sichergestellt werden, dass alle Computer und Geräte abgeschaltet sind. Belkin Corporation übernimmt keine Haftung für Schäden, die durch eingeschaltete Geräte entstehen.

Schritt 2 Anschließen der Konsole an den RIPM

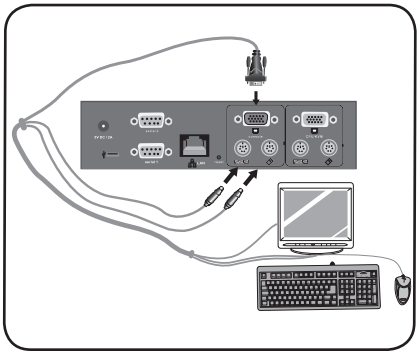


Fig. 2

2.1 Schließen Sie Ihre Tastatur und Maus an die jeweiligen Eingabegeräteanschlüsse im Konsolenbereich (Console) des RIPM an.

2.2 Schließen Sie Ihren Bildschirm an den VGA-Anschluss im Konsolenbereich (Console) des RIPM an.
Siehe **Abb. 2.**

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:34:24 AM

Schritt 3 | Option 1: Anschließen des RIPM an einen KVM-Switch (Host-System)

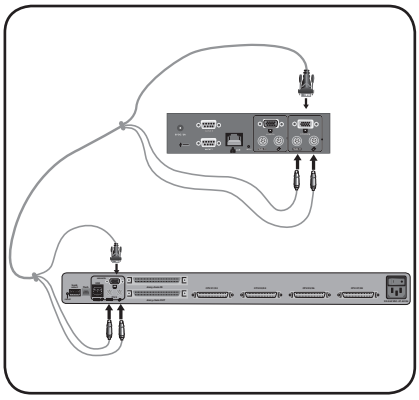


Fig. 3

3.1 Schalten Sie den KVM-Switch aus.

3.2 Verwenden Sie den mitgelieferten PS/2- und VGA-Kabelsatz zum Anschluss. Schließen Sie ein Kabelende an den “CPU/KVM switch” Bildschirm-, Tastatur- und Mausanschluss am RIPM an. Siehe**Abb. 3.**

3.3 Schließen Sie das andere Ende an den Bildschirm-, Tastatur- und Mausanschluss am KVM-Switch an.

Schritt 3 | Option 2: Anschließen des RIPM an einen Computer (Host-System)

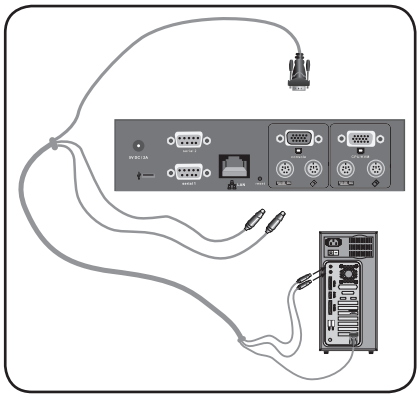


Fig. 4

3.1 Schalten Sie den Computer ab.

3.2 Verwenden Sie die mitgelieferten PS/2- und VGA-Kabel zum Anschluss. Schließen Sie ein Kabelende an den “CPU/KVM switch” Bildschirm-, Tastatur- und Mausanschluss am RIPM an. Siehe**Abb. 4.**

3.3 Schließen Sie das andere Ende an den Bildschirm-, Tastatur- und Mausanschluss am Computer an.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:34:27 AM

Schritt 4 | Anschließen des Mini-USB-Kabels Verwendung von Virtual Media

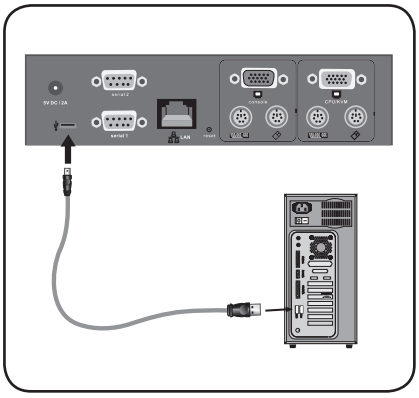


Fig. 5

4.1 Schalten Sie den Computer ab.

4.2 Schließen Sie das eine Ende des mitgelieferten Mini-USB-Kabels an den Mini-USB-Anschluss des RIPM und das andere an einen freien USB-Anschluss Ihres Computers an. Siehe**Abb. 5.**

Hinweis: Sie können jeden Computer mit einem Windows-Betriebssystem an den RIPM anschließen—der Computer muss nicht das Host-System sein.

Hinweis: Wenn auf Ihrem Computer KEIN Windows ausgeführt wird, müssen Sie die oben beschriebene Einrichtung nicht vornehmen.

Schritt 5 | Hochfahren des RIPM

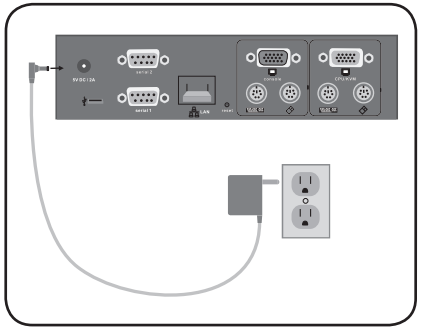


Fig 6

5.1 Schließen Sie das mitgelieferte Netzteil an eine freie geerdete Netzsteckdose an.

5.2 Stecken Sie den runden Stecker des Netzteils in die Netzbuchse des RIPM.
Siehe**Abb. 6.**

5.3 Schalten Sie den KVM-Switch oder den Computer an.

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:34:29 AM

Der RIPM kann auf zwei Arten eingerichtet und konfiguriert werden. Sie können die Einrichtungssoftware verwenden, die auf der beiliegenden CD angeboten wird oder Sie können über ein serielles Schnittstellenkabel Terminal-Software (z. B.: HyperTerminal®) mit dem RIPM nutzen.

Hinweis: Belkin empfiehlt die mitgelieferte Gerätesoftware.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:34:29 AM

Gerätesoftware

Die Software auf der mitgelieferten CD hilft Ihnen bei der Einrichtung des RIPM in Ihrem Netzwerk, auf das Sie anschließend leicht von außen zugreifen können.

1. Schließen Sie den RIPM über das lokale Netzwerk an Ihren Computer an. Starten Sie das Installations-Tool von der CD-ROM auf dem Computer, auf dem der RIPM installiert werden soll.
2. Folgen Sie der Anweisung des Assistenten zur Einrichtung des RIPM. Sie benötigen dazu eine IP-Adresse, eine Subnet-Mask und Gateway-Informationen für den RIPM. Sie erhalten diese Informationen ggf. von Ihrem Netzwerkadministrator. Wenn die Konfiguration erfolgreich abgeschlossen ist, wird eine entsprechende Mitteilung angezeigt. Der RIPM ist nun konfiguriert und kann verwendet werden.
3. Diese CD-ROM enthält auch die Software, die benötigt wird, um Dateien zwischen den lokalen und den Fernsteuerungscomputern (Remote-Computer) auszutauschen. Diese wird im Abschnitt “Virtual Media” in diesem Benutzerhandbuch beschrieben.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:34:30 AM

Um den RIPM über eine serielle Schnittstelle einzurichten, benötigen Sie ein Modemkabel (mitgeliefert). Verbinden Sie das Modemkabel mit dem Anschluss “Serial 01” am RIPM und der seriellen Schnittstelle am Computer. Die serielle Schnittstelle muss auf die folgenden Parameter eingestellt sein:

Parameter	**Wert**
Bit/Sekunde	115200
Datenbits	8
Parität	nein
Stoppbits	1
Flusskontrolle	keine

Verwenden Sie für die Verbindung mit dem RIPM ein Terminal-Programm (z. B. HyperTerminal). Setzen Sie den RIPM zurück und drücken Sie sofort danach die “ESC”-Taste. Daraufhin erscheint eine “=>”-Eingabeaufforderung. Geben Sie den Befehl “config” ein und drücken Sie die Eingabetaste. Sie werden aufgefordert, die IP-Autokonfiguration einzustellen sowie die IP-Adresse, die Net-Mask und den Standardgateway. Durch Drücken der Eingabetaste, ohne einen Wert einzugeben, werden die Einstellungen nicht geändert. Der Gateway-Wert muss auf “0.0.0.0” (kein Gateway) oder einen anderen Wert für die IP-Adresse des Gateway eingestellt sein. Nach der Bestätigung der Eingaben, wird der RIPM mit den aktuellen Werten neu gestartet .

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:34:30 AM

Benutzeroberfläche

Der RIPM kann über einen Java™-aktivierten Internetbrowser erreicht werden. Sie verwenden dazu das HTTP-Protokoll oder eine sichere verschlüsselte Verbindung wie HTTPS. Geben Sie einfach die IP-Adresse des RIPM in die Adresszeile des Internetbrowsers ein. Die Login-Einstellungen sind:

Parameter	Wert
Anmelden	administrator
Kennwort	belkin

Diese Einstellungen sollten auf jeden Fall geändert werden. Sie können dies auf der Seite “User Management” (Benutzerverwaltung) tun.

Telnet

Mit einem Telnet-Standardclient können Sie über einen Terminal-Modus ein frei gewähltes Gerät ansteuern, das mit einer seriellen Schnittstelle des RIPM verbunden ist.

Die primäre Schnittstelle des RIPM ist die HTTP-Schnittstelle. Voraussetzung für die Nutzung des Remote-Konsole-Fensters Ihres verwalteten Hostsystems ist ein Browser mit Java Laufzeitumgebung (Version 1.1 oder höher). Wenn der Browser kein Java unterstützt (wie bei kleinen Handheld-Geräten), können Sie das Remote-Hostsystem immer noch über die Administrationsformulare bedienen, die vom Browser selbst angeboten werden.

Bei einer nicht gesicherten Verbindung zum RIPM empfehlen wir die folgenden Internetbrowser:

- Microsoft Internet Explorer Version 5.0 oder höher unter Windows 2000 und XP
- Netscape Navigator 7.0 unter Windows 2000 und XP

Für den Zugriff auf das entfernte Hostsystem über eine gesicherte, verschlüsselte Verbindung benötigen Sie einen Browser, der das HTTPS-Protokoll unterstützt. Eine sichere Verbindung garantiert die 128-Bit-Verschlüsselung.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:34:30 AM

Öffnen Sie Ihren Internet-Browser. Geben Sie die Adresse des RIPM ein, die Sie während der Einrichtung eingestellt haben. Dazu können Sie eine IP-Adresse oder einen Host- und Domänennamen verwenden, wenn Sie dem RIPM einen symbolischen Namen im Domänennamenserver (DNS) zugeteilt haben.

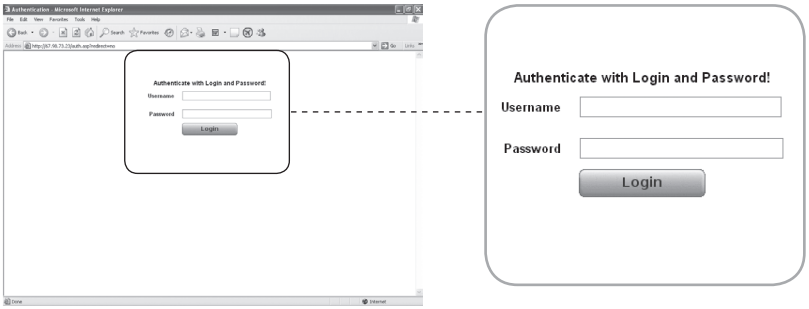
Geben Sie zum Beispiel die folgende Adresse in die Adresszeile Ihres Internetbrowsers ein, um eine nicht gesicherte Verbindung zu erstellen:

http://192.168.1.22/

Wenn Sie eine gesicherte Verbindung verwenden, geben Sie etwa Folgendes ein:

https://192.168.1.22/

Es wird die RIPM-Anmeldeseite geöffnet:



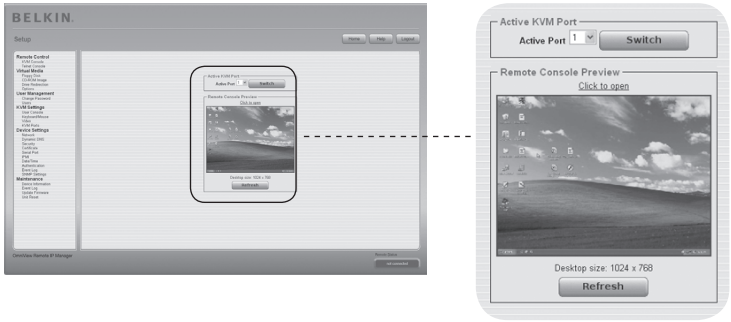
Im RIPM ist ein Benutzer mit Administratorbefugnissen voreingestellt, der Ihr System verwalten kann:

Parameter	Wert
Anmelden	administrator
Kennwort	belkin

Hinweis: Ihr Internetbrowser muss Cookies akzeptieren; die Anmeldung ist sonst nicht möglich.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:34:30 AM

Die Remote-Konsole ist Bildschirm, Tastatur und Maus des umgeleiteten entfernten Hostsystems, auf dem der RIPM installiert ist. Der Webbrowser für den Zugriff auf den RIPM muss eine Java Laufzeitumgebung (Version 1.1 oder höher) bereitstellen. Sie sollten aber unbedingt Sun JVM (Java Virtual Machine) 1.4 installieren. Die Remote-Konsole wird genauso bedient, als würden Sie direkt vor dem Bildschirm Ihres Systems sitzen; Sie können Tastatur und Maus wie gewohnt verwenden. Öffnen Sie die Remote-Konsole, indem Sie das Vorschaufenster der Hauptseite des HTML-Titels auswählen.



Einige der verfügbaren Menüoptionen sind:

Auto Adjust (Einstellautomatik)

Wenn das angezeigte Bild verzerrt ist oder eine schlechte Qualität hat, klicken Sie auf die Schaltfläche “Automatic Adjust” (Einstellautomatik). Nach einigen Sekunden stellt der RIPM die bestmögliche Bildqualität ein.

Sync Mouse (Maus synchronisieren)

Mit dieser Option synchronisieren Sie den lokalen mit dem entfernten Mauszeiger. Dies ist vor allem dann angebracht, wenn die Zeigergeschwindigkeit auf dem Host-System anders eingestellt ist.

Grafikeinstellungen im Menü “Optionen”

Mit dieser Option öffnen Sie ein neues Fenster mit Steuerelementen für die Grafikeinstellungen des RIPM. Sie können bestimmte Werte einstellen, die sich auf die Helligkeit und den Kontrast des angezeigten Bilds auswirken und dadurch die Bildqualität verbessern. Außerdem können Sie die Standardeinstellungen für alle Videomodi oder den aktuellen Videomodus wiederherstellen.

Hinweis: Klicken Sie beim ersten Start, wenn der lokale Mauszeiger nicht mit dem entfernten Mauszeiger übereinstimmt, einmal auf die Schaltfläche “Auto-Adjust” (Einstellautomatik).

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:34:31 AM

Zwischen dem RIPM und dem Host gibt es zwei Schnittstellen für die Übertragung von Tastatur- und Mausdaten: USB und PS/2. Der fehlerfreie Betrieb der Maus hängt von verschiedenen Einstellungen ab, die in den folgenden Unterkapiteln erläutert werden.

Remote IP-Manager: USB-Schnittstelle

Um die USB-Schnittstelle zu verwenden, müssen Sie den Host und das Gerät mit den richtigen Kabeln miteinander verbinden. Wenn der verwaltete Host zum Beispiel keine USB-Tastaturen im BIOS unterstützt und Sie nur ein USB-Kabel angeschlossen haben, haben Sie während des Startvorgangs keinen Tastatur-Zugriff auf den Host. Bitte beachten Sie den Abschnitt “Tastatur/Maus” auf Seite 48.

Remote IP-Manager: Tastatur-Einstellungen

Die RIPM-Einstellungen für den Host-Tastaturtyp müssen korrekt sein, damit die entfernte Tastatur richtig funktionieren kann. Prüfen Sie die Einstellungen im RIPM. Bitte beachten Sie den Abschnitt “Tastatur/Maus” auf Seite 48.

Remote-Maus-Einstellungen

Ein verbreitetes Problem mit KVM-Geräten ist die Synchronisation von lokalen und entfernten Mauszeigern. Der RIPM verarbeitet dieses Problem mit einem intelligenten Synchronisationsalgorithmus. Es gibt drei Maus-Modi, die auf dem RIPM eingestellt werden können.

- **Auto-Mouse Speed (Automatische Geschwindigkeitseinstellung)**
  Die automatische Geschwindigkeitseinstellung erkennt automatisch die Einstellungen der Maus auf dem Hostsystem. Weitere Informationen darüber finden Sie im folgenden Kapitel.

- **Fixed-Mouse Speed (Feste Geschwindigkeitseinstellung)**

  In diesem Modus werden die Mausbewegungen der Remote-Konsole so übersetzt, dass eine Pixelbewegung genau eine Pixelbewegung auf dem entfernten System bewirkt. Dieser Parameter kann unterschiedlich eingestellt werden. Dies funktioniert aber nur dann, wenn die Mausgeschwindigkeit auf dem entfernten (Remote)-System deaktiviert ist.

- **Einzel-/Doppelmausmodus**
  Dieser Modus wird im Abschnitt “Einzel- und Doppelmausmodus” auf Seite 20 beschrieben.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:34:31 AM

Maus-Geschwindigkeit und Maus-Synchronisation

Der Auto-Geschwindigkeitsmodus ermöglicht eine Geschwindigkeitserkenn ung während der Synchronisation. Immer, wenn sich der Mauszeiger nicht korrekt verhält, können lokaler und entfernter Mauszeiger auf zwei Arten neu synchronisiert werden:

- **Fast Sync (Schnellsynchronisierung)**
  Mit der Schnellsynchronisierung beheben Sie einen vorübergehenden, aber festen Zeitversatz. Wählen Sie diese Option aus dem Remote-Konsolenmenü. Falls möglich, können Sie auch
  den Tastaturbefehl für die Maus-Synchronisation verwenden (siehe Abschnitt “Remote-
  Konsole-Kontrollleiste auf Seite 23).

- **Intelligente Synchronisation**
  Wenn die Schnellsynchronisierung nicht funktioniert oder die Mauseinstellungen auf dem Hostsystem geändert wurden, verwenden Sie die intelligente Synchronisierung. Mit dieser Methode richten Sie die Parameter für die Bewegung des Mauszeigers so ein, dass der Mauszeiger an richtiger Stelle auf dem Bildschirm angezeigt wird. Diese Methode dauert länger als die Schnellsynchronisierung und kann mit dem entsprechenden Menübefehl im Remote-Konsolenmenü “Options” (Optionen) ausgewählt werden. Für die intelligente Synchronisierung ist ein korrekt eingestelltes Bild erforderlich. Richten Sie das Bild mit der Einstellautomatik oder der manuellen Korrektur im Bedienfeld “Video Settings” (Grafikeinstellungen) ein. Die Form des Mauszeigers hat erheblichen Einfluss auf die Erkennung des Zeigers. Belkin empfiehlt, eine einfache, herkömmliche Form zu verwenden. In der Regel wird die Erkennung und Synchronisation von animierten Zeigern nicht funktionieren. Im allgemeinen können Zeigerformen, die sich während der Zeigererkennung verändern, nicht erkannt und damit nicht übertragen werden. Die Verwendung eines Standard-Mauszeigers gewährleistet einen einfacheren Erkennungsvorgang und eine gute Synchronisation.

  Der “Maus”-Schalter oben auf der Remote-Konsole kann verschiedene Funktionen haben, je nach aktuellem Stand der Maus-Synchronisation. In der Regel wird über den Schalter die schnelle Synchronisation gestartet, es sein denn, der Grafikmodus wurde kurz zuvor geändert. Beachten Sie dazu auch den Abschnitt “Remote-Konsole-Kontrollleiste” auf
  Seite 23.

Hinweis: Klicken Sie beim ersten Start, wenn der lokale Mauszeiger nicht mit dem entfernten Mauszeiger übereinstimmt, einmal auf die Schaltfläche “Auto-Adjust” (Einstellautomatik).

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:34:31 AM

Hostsystem: Maus-Einstellungen

Das Betriebssystem des Host ermöglicht verschiedene Einstellungen für den Maustreiber.

Der RIPM arbeitet zwar mit beschleunigten Mäusen und kann die Mauszeiger synchronisieren, die folgenden Beschränkungen können diesen Vorgang jedoch negativ beeinflussen:

- **Spezieller Maustreiber**
  Bestimmte Maustreiber beeinflussen den Synchronisierungsprozess und unterbinden damit ein synchrones Verhalten der Mauszeiger. Wenn dies der Fall ist, stellen Sie sicher, dass Sie keinen speziellen, herstellerspezifischen Maustreiber auf dem Hostsystem verwenden.

- **Mauseinstellungen unter Windows 2003 Server/XP**
  Windows XP verfügt über die Einstellung “Zeigerbeschleunigung verbessern”. Diese muss
  deaktiviert werden.

- **Active Desktop**
  Wenn die Microsoft-Funktion “Active Desktop” aktiviert ist, sollten Sie keinen leeren Hintergrund verwenden. Wählen Sie stattdessen ein Bild als Desktop-Hintergrund aus. Alternativ können Sie den “Active Desktop” auch ganz deaktivieren.

  Bewegen Sie den Mauszeiger nach links oben im Applet-Schirm und bewegen Sie ihn langsam hin und her. Dadurch wird die Maus neu synchronisiert.
  Wenn die Neusynchronisierung nicht funktioniert, deaktivieren Sie die Zeigergeschwindigkeit und wiederholen Sie
  den Vorgang.

- **Einzel- und Doppelmausmodus**
  Die oben aufgeführten Informationen beziehen sich auf den Doppelmausmodus, in dem
  Remote- und lokale Maus angezeigt werden und synchronisiert werden müssen.
  Der RIPM verfügt über einen weiteren Modus, den Einzelmausmodus, in dem nur die Remote-Maus angezeigt wird. Aktivieren Sie diesen Modus auf der Remote-Konsole (siehe Abschnitt Remote-Konsole-Kontrollleiste auf Seite 23) und klicken Sie in den Fensterbereich. Der lokale Mauszeiger wird ausgeblendet und der entfernte kann direkt gesteuert werden. Um diesen Modus zu verlassen, müssen Sie einen Tastaturbefehl in den Einstellungen der Remote-Konsole festlegen. Verwenden Sie diesen dann, um blockierte lokale Mauszeiger wieder zu aktivieren.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:34:31 AM

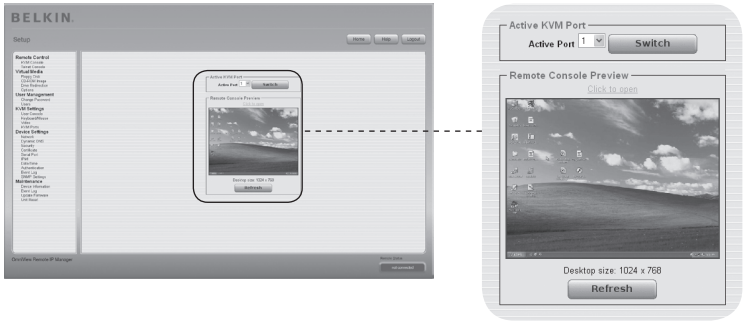
Empfohlene Maus-Einstellungen

Windows 2000, 2003, XP (Alle Versionen)	Für die meisten Fälle empfiehlt Belkin die Verwendung einer Maus über einen USB-Anschluss. Wählen Sie USB ohne Maussynchronisation aus.
Mac OS X	Belkin empfiehlt den Einzelmausmodus.
Sun Solaris	Stellen Sie die Mauseinstellungen über “xset m 1” oder über das CDE Control Panel auf “1:1, no acceleration (1:1, keine Beschleunigung) ein. Alternativ können Sie den Einzelmausmodus verwenden.
Linux	Wählen Sie erst die Option “Other Operating Systems” (Andere Betriebssysteme) in dem Auswahlfeld “Mouse Type” (Maustyp) aus. Wählen Sie anschließend die Option “Auto Mouse Speed” (automatische Zeigergeschwindigkeit). Dies gilt für USB- und für PS/2-Mäuse.

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:34:31 AM

Steuerung

Wenn Sie sich erfolgreich am RIPM angemeldet haben, wird die Hauptseite des RIPM geöffnet. Auf dieser Seite befinden sich drei Abschnitte mit unterschiedlichem Inhalt. Die Schaltflächen oben auf der Seite helfen Ihnen bei der Steuerung
(Details siehe Tabelle). Im Rahmen unten links befindet sich eine Navigationsleiste, mit der Sie zwischen den verschiedenen Abschnitten des RIPM wechseln können. Aufgabenspezifische Informationen, abhängig vom zuvor gewählten Abschnitt, werden im rechten Rahmen angegeben.



Hinweis: Nach 30 Minuten Inaktivität werden Sie automatisch von RIPM abgemeldet. Klicken Sie einmal auf eine Verknüpfung, um den Anmeldebildschirm zu öffnen.

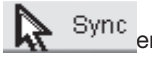
P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:34:32 AM

Das Fenster oben rechts enthält eine Steuerleiste. Mit den Elementen dieser Leiste können Sie den Status der Remote-Konsole anzeigen lassen und die Einstellungen der lokalen Remote-Konsole bearbeiten. Beschreibung aller Steuerfunktionen:

- **Auto Adjust (Einstellautomatik)**

Wenn das angezeigte Bild verzerrt ist oder eine schlechte Qualität hat, klicken Sie auf die Schaltfläche “Automatic Adjust” (Einstellautomatik). Nach einigen Sekunden stellt der RIPM die bestmögliche Bildqualität ein.

- **Sync Mouse (Maus synchronisieren)**



Mit dieser Option synchronisieren Sie den lokalen mit dem entfernten Mauszeiger. Dies ist vor allem dann wichtig, wenn die Zeigergeschwindigkeit auf dem Host-System anders eingestellt ist. In der Regel müssen die Mauseinstellungen nicht geändert werden.

- **Einzel-/Doppelmausmodus**

Wählen Sie diese Funktion, um vom Einzelmausmodus (in dem nur die Remote-Maus angezeigt wird) und dem Doppelmausmodus (in dem die Remote- und die lokale Mauszeiger angezeigt werden und synchronisiert werden müssen). Der Einzelmausmodus steht nur zur Verfügung, wenn Sie Sun JVM 1.4 oder höher verwenden.

- **Optionen**

Sie öffnen das Optionsmenü, indem Sie auf die Schaltfläche “Options” (Optionen) klicken.

Es wird eine kurze Beschreibung der Optionen angezeigt:

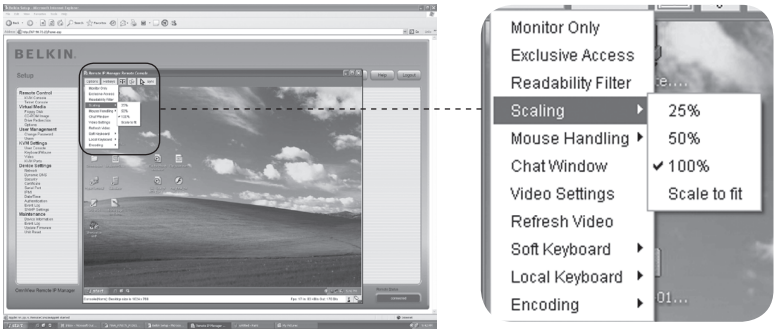
- **Monitor Only (Nur Kontrolle)**
  Schaltet den Filter “Monitor Only” (Nur Kontrolle) aus oder ein. Wenn der Filter aktiviert ist, ist keine Interaktion mit der Remote-Konsole möglich. Kontrolle ist jedoch möglich.

- **Exclusive Access (Alleinzugriff)**
  Mit der richtigen Zugangsberechtigung können Sie die Remote-Konsole für alle andere Nutzer sperren. Keiner kann die Remote-Konsole öffnen, bis Sie den Alleinzugriff wieder deaktiviert oder sich abgemeldet haben.

P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:34:32 AM

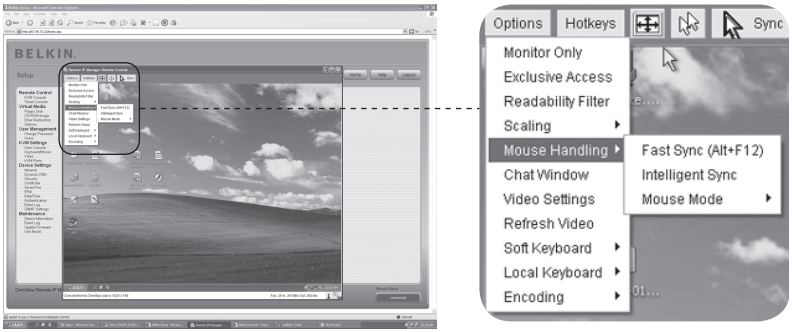
- **Scaling (Skalierung)**

  Ermöglicht es, die Remote-Konsole zu verkleinern. Sie können die Maus und die Tastatur weiterhin nutzen. Allerdings bleiben bei der Skalierung nicht alle Bilddetails erhalten.



- **Mouse Handling (Mausverarbeitung)**

  Das Untermenü für die Verwendung der Maus bietet zwei Optionen für die Synchronisation der lokalen und der entfernten Mauszeiger, wie im Kapitel “Maus-, Tastatur-, und Grafik-Konfiguration” erläutert wird.



- **Fast Sync (Schnellsynchronisierung)**

  Mit der Schnellsynchronisierung beheben Sie einen vorübergehenden, aber festen Zeitversatz.

- **Intelligente Synchronisierung.**

  Verwenden Sie diese Option, wenn die Schnellsynchronisierung nicht funktioniert oder die Mauseinstellungen auf dem Hostsystem geändert wurden.

  Achtung: Diese Methode dauert länger als die Schnellsynchronisierung und erfordert ein korrekt eingestelltes Bild. Richten Sie das Bild mit der Einstellautomatik oder der manuellen Korrektur im Bedienfeld “Video Settings” (Grafikeinstellungen) ein.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:34:33 AM

- **Lokaler Mauszeiger**
  Öffnet eine Liste mit verschiedenen Zeigerformen, aus denen Sie eine für den lokalen Mauszeiger auswählen. Die gewählte Form wird für den aktuellen Benutzer gespeichert und aktiviert, wenn die Remote-Konsole das nächste Mal geöffnet wird. Die Anzahl der verfügbaren Formen hängt von Java Virtual Machine (JVM) ab—mit den Versionen 1.2 und höher steht eine vollständige Liste zur Verfügung.

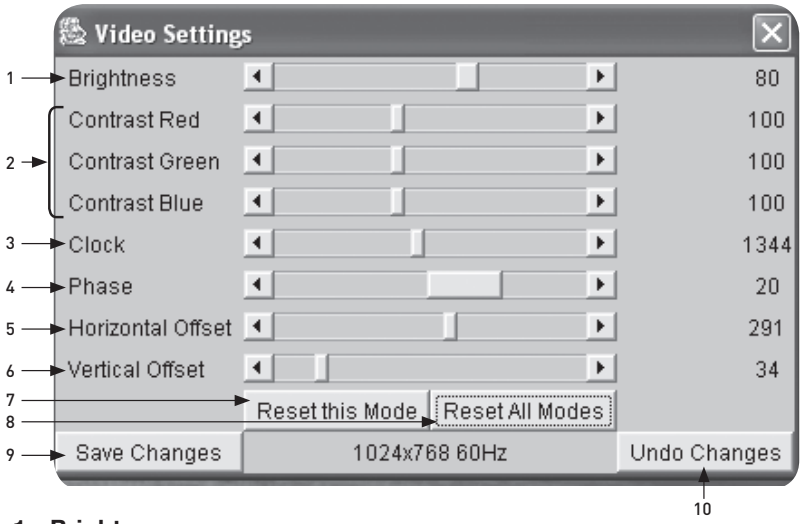
- **Video Settings (Grafikeinstellungen)**
  Öffnet eine Leiste für die Änderung der RIPM-Grafikeinstellungen. Der RIPM verfügt über zwei verschiedenen Dialoge für die Grafikeinstellungen.

- **Grafikeinstellung über HTML.**
  Wählen Sie diese Option, um den lokalen Grafikport zu aktivieren. Mit dieser Option bestimmen Sie, ob der lokale Grafikausgang des RIPM aktiv ist und die eingehenden Signale vom Hostsystem akzeptiert.

  Mit der Option “Noise Filter” (Entstörfilter) bestimmen Sie, wie der RIPM auf kleine Änderungen des Grafiksignals reagiert. Eine umfassende Filtereinstellung benötigt weniger Netzwerkverkehr und führt zu einer schnelleren Grafikanzeige, allerdings könnten kleine Änderungen in einigen Anzeige-Bereichen nicht sofort erkannt werden. Eine kleine Filtereinstellung zeigt sofort alle Änderungen an, führt aber zu einer konstanten Netzwerkbelastung, auch dann, wenn sich die Anzeige nicht wirklich ändert (je nach Qualität des Grafiksignals). Die Standardeinstellung sollte an die meisten Situationen angepasst sein.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:34:34 AM

Grafikeinstellungen über die Remote-Konsole



1. **Brightness**
(Bildhelligkeit) Steuerung der Bildhelligkeit.
2. **Contrast (Kontrast)**
Steuert den Bildkontrast
3. **Clock (Uhr)**
Bestimmt die horizontale Frequenz einer Grafikleitung und resultiert aus dem Grafikmodus. Für verschiedenen Grafikkartentypen müssen hier verschiedene Werte eingegeben werden. Die Standardeinstellung mit Einstellautomatik sollte für alle herkömmlichen Konfigurationen eingestellt werden. Für eine bessere Bildqualität ändern Sie die Einstellungen während der Abtastphase.
4. **Phase**
Bestimmt die Phase des Grafiksamplings. Damit wird die Anzeigequalität geprüft und eine Abtastuhr eingestellt.
5. **Horizontal Offset (Horizontalabstand)**
Wenn diese Option ausgewählt ist, können Sie das Bild mit der linken und rechten Pfeilschaltfläche horizontal verschieben.
6. **Vertical Offset (Vertikalabstand)**
Wenn diese Option ausgewählt ist, können Sie das Bild mit der linken und rechten Pfeilschaltfläche vertikal verschieben.
7. **Reset this Mode (Modus zurücksetzen)**
Setzt die modusspezifischen Einstellungen auf die Werkseinstellungen zurück.
8. **Reset all Modes (Alle Modi zurücksetzen)**
Setzt alle Einstellungen auf die Werkseinstellungen zurück.
9. **Save Changes (Änderungen speichern)**
Speichert die Änderungen.
10. **Undo Changes (Wiederherstellen)**
Stellt die letzten Einstellungen wieder her.

P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:34:34 AM

Belegsequenz

Soft Keyboard (Virtuelle Tastatur)
Öffnet das Menü für die virtuelle Tastatur.

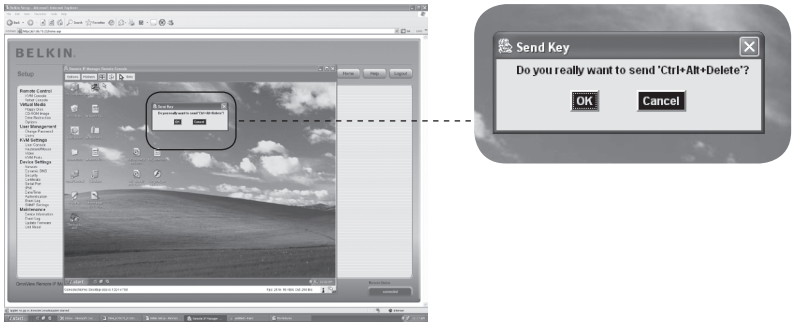
Show (Anzeige)
Öffnet die virtuelle Tastatur. Die virtuelle Tastatur wird benötigt, wenn auf Ihrem Hostsystem eine andere Spracheinstellung und eine andere Landesauswahl, als auf dem verwalteten Computer verwendet wird.

Mapping (Belegung)
Wird für die Auswahl der richtigen Sprache und der Landeseinstellung der virtuellen Tastatur verwendet.

P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:34:34 AM

Local Keyboard (Lokale Tastatur)
Wird verwendet, um die Sprachbelegung Ihres Browsers zu ändern, mit dem das Applet für die Remote-Konsole ausgeführt wird. In der Regel wird der richtige Wert vom Applet automatisch bestimmt. Dies wird aber dennoch nicht bei allen JVM und Browser-Einstellungen funktionieren Ein typisches Beispiel ist ein deutsches System, dass mit einer US-Englischen Tastaturbelegung bedient wird. In diesem Fall müssen Sie die lokalen Tastatureinstellungen manuell auf die richtige Sprache einstellen.

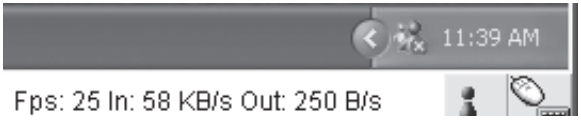
Hot Keys (Tastaturbefehle)
Öffnet eine Liste mit voreingestellten Tastaturbefehlen. Wählen Sie einen Eintrag. Der Befehl wird anschließend an das Hostsystem weitergeleitet. Sie können eine Bestätigungsnachricht hinzufügen, bevor der ausgewählte Befehl an das Hostsystem weitergeleitet wird. Wählen Sie “OK”, um den Befehl auf dem Remote-Host auszuführen.



P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:34:35 AM

Auf der Statusleiste sollten sowohl die Remote-Konsole als auch der Verbindungsstatus angezeigt werden. Die Größe des Remote-Bildschirms wird links angegeben. Der Wert in Klammern beschreibt die Verbindung mit der Remote-Konsole. “Norm” bezeichnet eine Standardverbindung ohne Verschlüsselung; “SSL” bezeichnet eine sichere Verbindung mit SSL-Verschlüsselung.

Der eingehende (“In”; [Ein]) und der ausgehende (“Out” [Aus]) Netzwerkverkehr werden in Kilobytes pro Sekunde angegeben. Bei aktivierter Kodierungskomprimierung wird die komprimierte Übertragungsrate in Klammern angegeben.



Die nächste Schaltfläche zeigt die Remote-Konsole-Zugangseinstellungen an.

Einer oder mehrere Benutzer können mit der Remote-Konsole des RIPM verbunden sein.

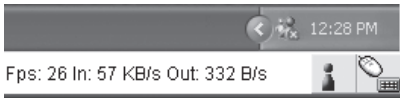
Für Sie ist der Alleinzugriff eingestellt. Kein anderer Benutzer kann über die Remote-Konsole auf den Host zugreifen, wenn Sie diese Option nicht deaktivieren.

P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:34:36 AM

Ein Remote-Benutzer verfügt über exklusive Zugangsrechte (Alleinzugriff). Sie können nicht über die Remote-Konsole auf den Host zugreifen, wenn der entsprechende andere Benutzer diese Option nicht deaktiviert.

Die Schaltfläche unten rechts gibt den Status der “Nur Kontrolle”-Einstellungen wieder.

Die Option “Nur Kontrolle” ist deaktiviert.



Die Option “Nur Kontrolle” ist aktiviert

Weitere Informationen über die Einstllungen “Nur Kontrolle” und “Alleinzugriff” finden Sie im Abschnitt “Remote-Konsole-Kontrollleiste” auf Seite 23 dieses Handbuchs.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:34:36 AM

Zurücksetzen des Remote IP-Manager auf Werkseinstellungen

Die RIPM- und die Netzwerkeinstellungen auf die Werkseinstellungen zurücksetzen:

1. Erstellen Sie für die erste Konfiguration (HyperTerminal) eine serielle Verbindung

Bits pro Sekunde:	115200
Datenbits:	8
Parität:	keine
Stoppbits:	1
Flusskontrolle:	Hardware oder keine

2. Drücken Sie die Rücksetztaste, die sich zwischen dem Netzanschluss und dem Netzwerkanschluss befindet. Lassen Sie die Taste wieder los und drücken Sie sofort danach im Seriellen Terminalprogramm (HyperTerminal) einige Male die ESC-
   Taste, bis eine Eingabeaufforderung geöffnet wird (“=>”).

   Hinweis: Wenn die Eingabeaufforderung nicht innerhalb der ersten drei Sekunden, nachdem Sie die Rücksetztaste wieder losgelassen haben, geöffnet wird, wiederholen Sie Schritt 1 und 2. Der RIPM erkennt die ESC-Taste nur während der ersten drei Sekunden des Startvorgangs.
3. Wenn Sie dazu aufgefordert werden, geben Sie die “Vorgaben” ein und drücken Sie die Eingabetaste. Der RIPM wird dann neu mit den Werkseinstellungen gestartet.
4. Schalten Sie Ihren Server ab (der Computer, mit dem der RIPM lokal verbunden ist).
5. Trennen Sie den RIPM von der Netzverbindung und den “CPU/KVM-Switch”-Anschlusskabeln sowie dem Netzwerkkabel.
6. Schließen Sie die Kabel wieder an und starten Sie den Server.

Jetzt können Sie den RIPM über eine HyperTerminal-Verbindung oder die Einrichtungs-Software neu auf Ihr Netzwerk einstellen.

Am Remote IP-Manager abmelden

Mit dieser Schaltfläche melden Sie den aktuellen Benutzer ab und öffnen ein neues Anmeldefenster. Bitte beachten Sie, dass nach einer halben Stunde Inaktivität die Abmeldung automatisch erfolgt.

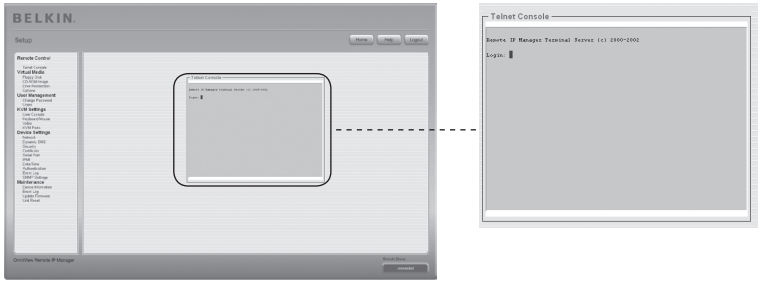
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:34:36 AM

KVM-Konsole

Remote-Konsole: Vorschau

Um die KVM-Konsole zu öffnen, klicken Sie auf den Menüeintrag links oder die Konsolenabbildung rechts. Um die Abbildung zu aktualisieren, klicken Sie auf die Schaltfläche “Refresh” (Aktualisieren).

Telnet-Konsole



Die RIPM-Firmware verfügt über ein Telnet-Gateway, über das Benutzer eine Verbindung mit dem RIPM über einen Standard-Telnet-Client herstellen können. Um eine Telnet-Protokollverbindung mit dem RIPM herzustellen, verwenden Sie ein Terminalprogramm wie xterm, TeraTerm oder PuTTY. Alternativ können Sie den Telnet-Befehl auch in der Befehlszeile eingeben oder die Funktion “Ausführen” im Windows Startmenü verwenden. Sie können beispielsweise den folgenden Befehl eingeben:

Telnet: 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:34:37 AM

Ersetzen Sie die IP-Adresse mit derjenigen, die dem RIPM während der Installation zugeteilt wurde. Sie werden anschließend aufgefordert, den Benutzernamen und das Kennwort einzugeben, um sich am Gerät anmelden zu können. Die Zugangsdaten für die Authentifizierung sind dieselben wie für die Web-Schnittstelle. Das heißt, die Benutzerverwaltung für die Telnet-Schnittstelle wird ganz mit den entsprechenden Funktionen der Web-Schnittstelle gesteuert. Wenn Sie sich erfolgreich am RIPM angemeldet haben, wird eine Befehlszeile angeboten und Sie können die Verwaltungsbefehle dort eingeben. Im Allgemeinen unterstützt die Telnet-Schnittstelle zwei Betriebsmodi: den Befehlszeilen-Modus und den Terminal-Modus. Der Befehlszeilen-Modus wird verwendet, um einige Parameter zu kontrollieren oder anzuzeigen. Im Terminal-Modus ist der Durchlass zur seriellen Schnittstelle 1 aktiviert (wenn die seriellen Einstellungen korrekt vorgenommen wurden). Um auf den RIPM über eine serielle Schnittstelle zuzugreifen, benötigen Sie ein Modemkabel. Alle Eingaben werden über die serielle Schnittstelle 1 auf das Gerät umgeleitet, die Reaktionen werden über die Telnet-Schnittstelle angezeigt.

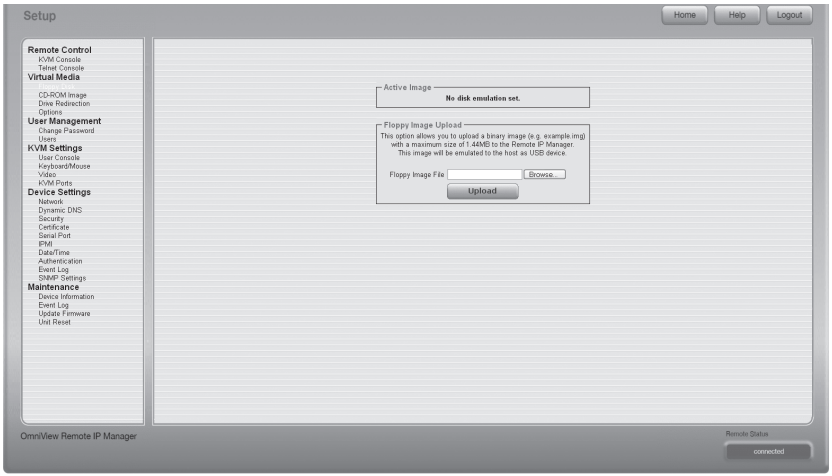
In der folgenden Liste sind die Befehlssyntax und ihre Verwendung aufgeführt.

Hilfe	Öffnet eine Liste der möglichen Befehle.
cls	Löschen der Bildschirmeinträge
quit	Beendung der aktuellen Sitzung und Trennung der Client-Verbindung.
version	Anzeige der Versions-Infos.
terminal	Start des Terminal-Durchlassmodus für die serielle Schnittstelle 1. Die Tastenkombination “esc exit” schaltet wieder zum Befehlsmodus um. Der Befehl hat einen optionale Parameter (1 oder 2), um die erforderliche serielle Schnittstelle für den Durchlass-Zugriff auszuwählen.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:34:37 AM

Diskette



Mit dieser Funktion können Abbilddateien hochgeladen und übertragen werden. Mit dieser Option können Sie ein Binärabbild (beispiel.img) mit einer Maximalgröße von 1,44 MB an den RIPM senden. Dieses Abbild wird für den Host wie ein USB-Gerät emuliert. Alle anderen Formate müssen mit der Laufwerks-Umleitungsfunktion übertragen werden. Zur Verwendung eines größeren Abbildes, verwenden Sie einen “Windows Share”.

Hochladen eines Disketten-Abbilds

Schritt 1: Klicken Sie auf “Browse” (Suchen), um die zu übertragende Datei auszuwählen.

Schritt 2: Klicken Sie auf “Upload” (Hochladen), um die Datei zum RIPM hochzuladen. Es wird eine Betätigung für den erfolgreichen Upload zum RIPM angezeigt.

Schritt 3: Klicken Sie im Abschnitt Remote-Konsole der RIPM-Schnittstelle auf “KVM Console” (KVM-Konsole), um auf den Desktop des Remote-Computers zuzugreifen.

Schritt 4: Klicken Sie doppelt auf das Symbol “Arbeitsplatz”, um den Ordner zu öffnen.

Schritt 5: Im “Arbeitsplatz” wird ein zweiter Eintrag für das Diskettenlaufwerk angezeigt. Dies ist der Eintrag “3-1⁄2 Floppy (B)”. Sie können auf die Dateien zugreifen, die Sie hierhin übertragen haben.

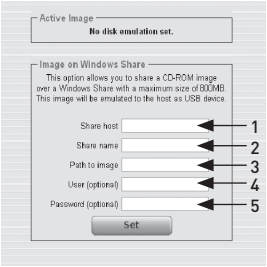
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:34:38 AM

CD-ROM-Abbild

Verwenden Sie Grafiken über Windows Share (SAMBA).

Um ein Abbild aus einem Windows Share einzubinden, wählen Sie “CD-ROM” aus dem Untermenü aus.

Sie müssen die folgenden Informationen angeben, um das ausgewählte Abbild richtig einbinden zu können:



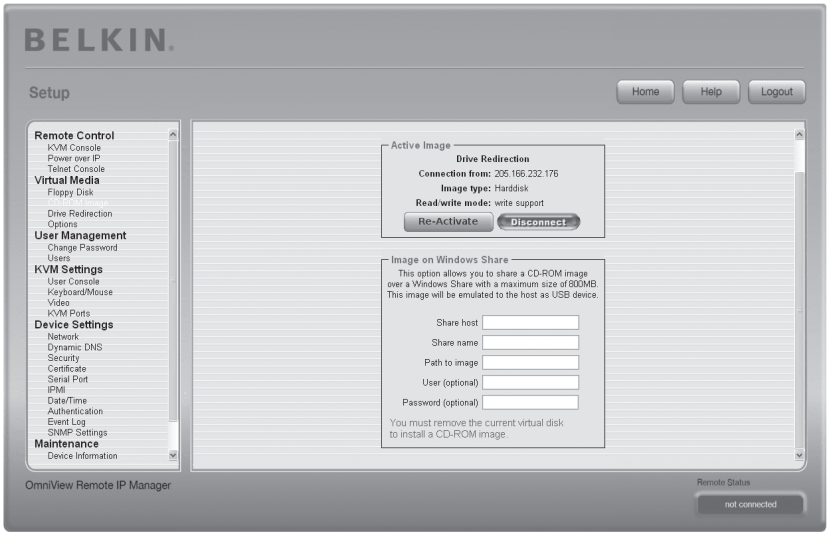
1. **Share Host**
   Servernamen oder IP-Adresse. (Diese IP-Adresse wird über die Laufwerks-Umleitungssoftware erteilt—Erläuterung folgt.)
2. **Share Name**
   Name des verwendeten Share-Ordners.
3. **Path to Image (Abbildpfad)**
   Der Abbild-Dateipfad auf dem Share.
4. **User (Benutzer - Optional)**
   Geben Sie, falls notwendig, den Benutzernamen für den Share an. Wird dieser nicht angegeben und ein Gastzugang ist aktiviert, werden die Daten des Gastzugangs für die Anmeldung verwendet.
5. **Password (Kennwort - Optional)**
   Wenn ein Kennwort angegeben werden muss, geben Sie das Kennwort für den angegebenen Benutzernamen an.

P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:34:38 AM

CD-ROM-Abbild hochladen

Schritt 1: **Öffnen Sie die Laufwerks-Umleitungssoftware und führen Sie sie aus.**

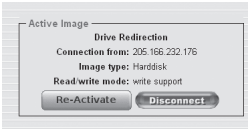
Schritt 2: Wenn die Laufwerks-Umleitungssoftware verbunden ist, lassen Sie dieses Fenster geöffnet und öffnen Sie das CD-ROM-Abbild im RIPM-Abschnitt “Virtual Media”.



Hinweis: Die IP-Adresse, die unter “Connection From” (Verbindungsliste) aufgelistet ist, ist die IP-Adresse, die als Share-Host-Adresse verwendet wird. Um die Richtigkeit dieser IP-Adresse zu prüfen, verbinden Sie ein serielles Kabel mit dem RIPM und dem Computer und starten Sie eine Hyperterminal-Sitzung. Melden Sie sich als “ping” an und geben Sie die IP-Adresse genau wie im “Share host”-Feld ein. Es sollte die Meldung “<IP> is alive!” angegeben werden.

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:34:39 AM

Schritt 3: Klicken Sie im Abschnitt “Active Image” (Aktuelles Abbild) auf “Re-Activate” (Aktivieren).



Schritt 4: Geben Sie die IP-Adresse an, die von der Laufwerks-Umleitungssoftware angeboten wird, in das Feld “Share Host” ein.

Schritt 5: Geben Sie den “Share name” (Share-Name) und den “Path to Image” (Abbildpfad) ein.

Schritt 6: Um die Datei hochzuladen, klicken Sie auf die Schaltfläche “Set” (Einstellen). Die Datei wird auf dem Remote-Computer als USB-Gerät angegeben.

Auf die angegebene Datei sollte von RIPM zugegriffen werden können. Die oben stehenden Informationen müssen auf der Perspektive des RIPM erteilt werden. Die Angabe von richtigen IP-Adressen und Gerätenamen ist sehr wichtig. Andernfalls kann der RIPM auf die entsprechenden Bilddateien nicht ordentlich zugreifen und anstatt der Datei wird eine Fehlermeldung angezeigt. Belkin empfiehlt, dass Sie die richtigen Werte verwenden und diesen Schritt bei Bedarf wiederholen.

Der angegebene Share muss richtig konfiguriert sein, daher müssen Sie über Administratorenrechte verfügen. Als normaler Benutzer haben Sie diese Rechte nicht. Sie sollten entweder als Systemadministrator angemeldet sein oder den Systemadministrator um Unterstützung in dieser Frage bitten.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:34:39 AM

Laufwerks-Umleitung

Die Funktion “Laufwerks-Umleitung” bietet eine andere Möglichkeit, ein virtuelles Laufwerk auf dem Remote-Computer zu verwenden. Sie können mit einem Laufwerk auf Ihrem lokalen Computer vom Remote-Computer aus arbeiten, indem Sie das Laufwerk über eine TCP-Netzwerkverbindung zugänglich machen. Speichermedien, einschließlich Disketten und Festplatten*, CD-ROMs und Wechseldatenträger wie USB-Sticks können umgeleitet werden. Sie können sogar Ihren Remote-Computer so einstellen, dass die Daten auf die lokale Festplatte geschrieben werden.

*** Hinweis:** Belkin rät von der Möglichkeit ab, Schreibrechte zu aktivieren, wenn eine Festplatte umgeleitet wird und ist für Datenverluste oder Datenbeschädigungen durch diesen Vorgang nicht verantwortlich.

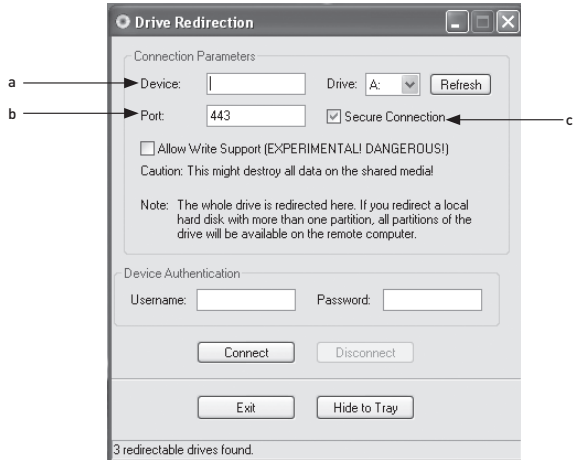
Bitte verwenden Sie diese Funktion umsichtig. Die Laufwerks-Umleitung funktioniert auf einer Ebene, die über dem Betriebssystem liegt, sodass weder das lokale noch das entferne Betriebssystem erkennen kann, dass ein Laufwerk umgeleitet wurde. Es kann dann zu inkonsistenten Daten führen, wenn eines der Betriebssysteme (auf dem lokalen oder dem Remote-Computer) Daten auf das Gerät schreibt. Mit aktivierten Schreibrechten kann es zu Datenbeschädigungen und Beschädigungen des Dateisystems auf dem umgeleiteten Gerät kommen. Wenn, andererseits, das lokale Betriebssystem Daten auf das umgeleitete Gerät schreibt, kann der Laufwerks-Cache des Remote-Betriebssystems ältere Daten enthalten, die zu Verwirrungen des Host-Betriebssystems führen. Wir raten daher dazu, die Laufwerks-Umleitung, besonders mit aktivierten Schreibrechten, mit großer Vorsicht zu verwenden.

Hinweis: Um die Umleitungs-Funktion verwenden zu können, müssen Sie die Laufwerks-Umleitungs-Software, die mit diesem Produkt geliefert wurde, auf dem Computer verwenden, mit dem Sie eine Fernverbindung zum RIPM herstellen.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:34:39 AM

1. **Öffnen Sie die Anwendung für die Laufwerks-Umleitung.**

2. **Geben Sie die Parameter der Netzwerkverbindung an.**



   a. **Device (Gerät)**
      Dies ist die IP-Adresse des RIPM, mit dem Sie eine Verbindung erstellen möchten.

   b. **Port (Schnittstelle)**
      Dies ist die Netzwerkschnittstelle Der RIPM verwendet standardmäßig die Remote-Konsolenschnittstelle (#443). Sie können diesen Wert ändern, wenn Sie die Remote-Konsolenschnittstelle in den Netzwerkeinstellungen des RIPM geändert haben.

   c. **Secure Connection (Sichere Verbindung)**
      Aktivieren Sie dieses Feld, um eine gesicherte Verbindung über SSL herzustellen. Dadurch wird die Sicherheit erhöht, die Verbindungsgeschwindigkeit aber auch vermindert.

3. **Wählen Sie das Laufwerk aus, das sie umleiten möchten.** Alle verfügbaren Geräte (Laufwerksbuchstaben) werden angezeigt. Bitte beachten Sie, dass der RIPM das gesamte Laufwerk und nicht nur einzelne Partitionen mit dem Remote-Computer teilt. Wenn Sie eine Festplatte mit mehreren Partitionen haben, werde alle Laufwerksbuchstaben, die zu diesem Laufwerk gehören, umgeleitet. Verwenden Sie die Schaltfläche “Refresh” (Aktualisieren), um eine Liste der Laufwerksbuchstaben zu erstellen (speziell bei USB-Sticks).

4. **Schreibrechte**

   Achtung: Verwenden Sie diese Funktion mit Vorsicht. Mit Schreibrechten ist es möglich, vom Remote-Computer aus Ihr lokales Laufwerk zu beschreiben. Wenn sowohl vom Remote- als auch vom lokalen System versucht wird, Daten gleichzeitig auf das selbe Laufwerk zu schreiben, **wird das Dateisystem des Laufwerks erheblich beschädigt oder zerstört.** Bitte verwenden Sie diese Funktion nur, wenn Sie sich absolut sicher sind, dass keine Gefahr der Beschädigung vorliegt.

   Hinweis: Belkin rät von der Möglichkeit ab, Schreibrechte zu aktivieren, wenn eine Festplatte umgeleitet wird und ist für Datenverluste oder Datenbeschädigungen durch diesen Vorgang nicht verantwortlich.

5. **Authentifizieren des Geräts.** Um die Umleitung nutzen zu können, müssen Sie sich am RIPM mit gültigen Benutzernamen und Kennwort authentifizieren. Sie benötigen eine Erlaubnis, um die virtuelle Laufwerks-Konfiguration zu ändern.

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:34:40 AM

6. **Erstellen Sie eine Laufwerks-Umleitung, indem Sie einmal auf die Schaltfläche “Connect” (Verbinden) klicken.**
   Wenn alle Einstellungen korrekt sind, wird in der Statusleiste angezeigt, dass die Verbindung erstellt wurde. Die Schaltfläche “Connect” (Verbinden) ist dann deaktiviert und die Schaltfläche “Disconnect” (Trennen) aktiviert. Sollte ein Fehler auftreten, wird die Fehlermeldung in der Statusanzeige angegeben.

   Die Laufwerks-Umleitungs-Software wird versuchen, das lokale Laufwerk zu sperren, bevor es umgeleitet wird. Dadurch wird vermieden, dass das lokale Betriebssystem auf das Laufwerk während der Umleitung zugreifen kann. Dieser Vorgang kann nicht durchgeführt werden, wenn eine Datei gerade verwendet wird oder geöffnet ist. Wenn diese Sperrung nicht erfolgen kann, werden Sie aufgefordert, die Herstellung der Verbindung zu bestätigen. Bedenken Sie aber, dass aktivierte Schreibrechte bei einer Umleitung des nicht gesperrten Laufwerks zu erheblichen Schäden führen können.
7. Verwenden Sie die Schaltfläche “Disconnect” (Trennen), um die Laufwerks-Umleitung zu beenden.
8. Klicken Sie auf “Exit” (Schließen), um das Laufwerks-Umleitungsprogramm zu beenden. Wenn eine Laufwerks-Umleitung aktiv ist, wird die Verbindung vor Beendigung der Anwendung geschlossen.
9. Verwenden Sie die Schaltfläche “Hide to Tray” (In Symbolleiste minimieren), um die Anwendung zu minimieren, ohne Sie zu schließen. Eine aktive Verbindung wird dann gehalten, bis Sie die Anwendung schließen. Sie können auf die Software zugreifen, indem Sie auf der Symbolleiste doppelt auf das Symbol für das Programm klicken. Das Symbol zeigt auch an, ob eine Verbindung besteht. Klicken Sie mit rechten Maustaste auf das Symbol, um das Untermenü zu öffnen.

Optionen

Disable Drive Redirection (Laufwerks-Umleitung deaktivieren)
Die Laufwerks-Umleitung wird deaktiviert.

Force Read-Only Connections (Schreibgeschützte Verbindung erzwingen)
Damit werden die Schreibrechte für die Laufwerks-Umleitung abgeschaltet.

Klicken Sie auf “Apply” (Übernehmen), um die Änderungen zu versenden.

P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:34:40 AM

Erstellen eines Abbilds

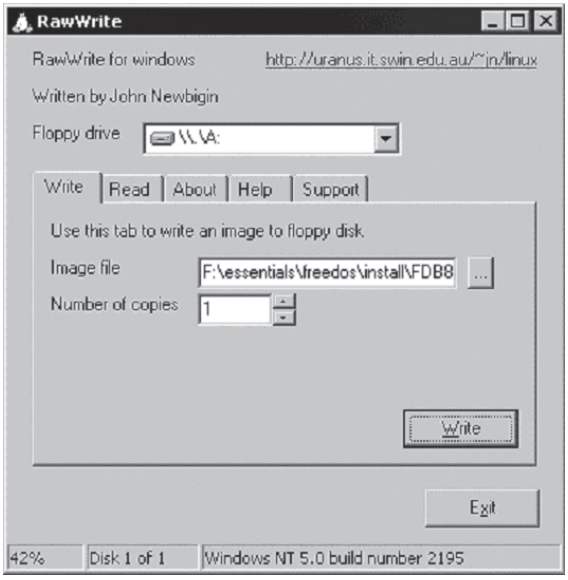
Disketten-Abbilder

UNIX® und UNIX-Like Operating Systems (OS)

Um eine Abbilddatei (Image) zu erstellen, verwenden Sie “dd”. Dies ist eines der originalen UNIX-Hilfsprogramme und ist Teil aller UNIX-Betriebssysteme (UNIX, Sun Solaris, Linux). Um eine Disketten-Abbilddatei zu erstellen, kopieren Sie den Inhalt einer Diskette in eine Datei. Sie können folgenden Befehl verwenden: dd [if=/dev/fd0] [of=/tmp/floppy.image]. “dd” liest in diesem Fall die gesamte Diskette vom Laufwerk “/dev/fd0” und speichert das Ergebnis in der angegebenen Datei “/tmp/floppy.image”. Stellen Sie beide Parameter genau nach Ihren Wünschen ein (Eingabegerät usw.).

MS Windows

Sie können das Hilfsprogramm “RawWrite for Windows” verwenden.



Öffnen Sie im Menü die Registerkarte “Read” (Lesen). Tragen Sie den Namen der Datei ein, in der Sie den Disketteninhalt speichern möchten. Klicken Sie auf die Schaltfläche “Copy” (Kopieren), um den Vorgang der Abbilderstellung zu starten. Ähnliche Hilfsprogramme finden Sie auf der Homepage des Projekts “fdos” **(http://www.fdos.org).**

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:34:40 AM

CD-ROM/ISO 9660-Abbilder

UNIX und UNIX-Like OS

Um eine Abbilddatei zu erstellen, verwenden Sie “dd”. Dies ist eines der Original-UNIX-
Hilfsprogramme und ist Teil aller UNIX-Betriebssysteme (UNIX, Sun Solaris, Linux). Um ein CD-ROM-Abbild zu erstellen, kopieren Sie den Inhalt der CD-ROM in eine Datei. Sie können den folgenden Befehl verwenden:

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

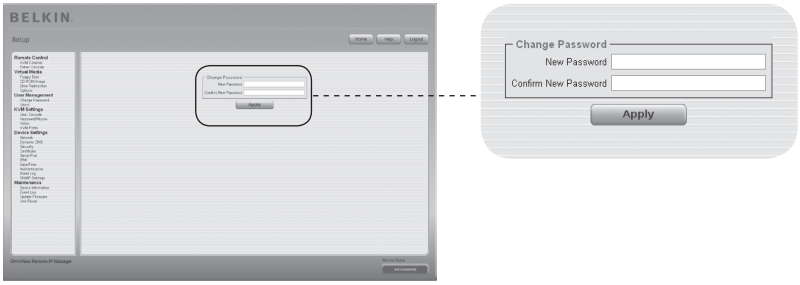
“dd” liest in diesem Fall für die gesamte Disk vom Laufwerk “/dev/cdrom” und speichert das Ergebnis in der angegebenen Datei “/tmp/cdrom.image”. Stellen Sie beide Parameter genau nach Ihren Wünschen ein (Eingabegerät usw.).

MS Windows

Um eine Abbilddatei zu erstellen, verwenden Sie ein CD-Abbildprogramm Ihrer Wahl. Kopieren Sie den gesamten Inhalt der Disc in eine einzige ISO-Abbilddatei auf Ihrer Festplatte. In “Nero” wählen Sie beispielsweise “Copy and Backup” (Rekorder) und öffnen Sie “Copy Disc” (Disk kopieren). Wählen Sie das CD-ROM- oder DVD-Laufwerk aus, von dem Sie ein ISO-Abbild erstellen möchten. Bestimmen Sie den Dateinamen des ISO-Abbilds und speichern den Inhalt der CD-ROM in der Datei.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:34:40 AM

Kennwort ändern

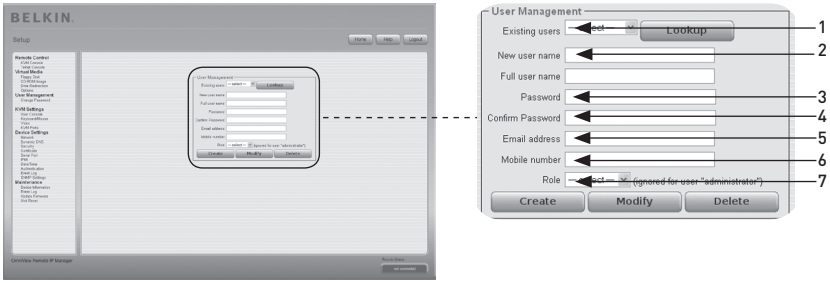


Um das Kennwort zu ändern, geben das neue Kennwort in das obere Eingabefeld ein. Geben Sie das Kennwort erneut in das Feld darunter ein.

Klicken Sie auf “Apply” (Übernehmen), um Ihre Änderungen zu übertragen.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:34:41 AM

Users (Benutzer)



Benutzerverwaltung

Der RIPM ist mit einem vorkonfiguriertem Benutzerkonto für den Administrator ausgestattet, der über feste Rechte verfügt. Dieser Benutzer hat alle Rechte zur Einstellung des Geräts und zur Verwendung aller Funktionen des RIPM. Bei Lieferung lautet das Kennwort für den “administrator”-Benutzer “belkin”. Sie sollten das Kennwort des Administrators sofort nach der Installation beim ersten Zugriff auf den RIPM ändern. Es folgt eine Liste mit den verfügbaren Optionen. Diese Liste kann nur vom Administrator gelesen werden.

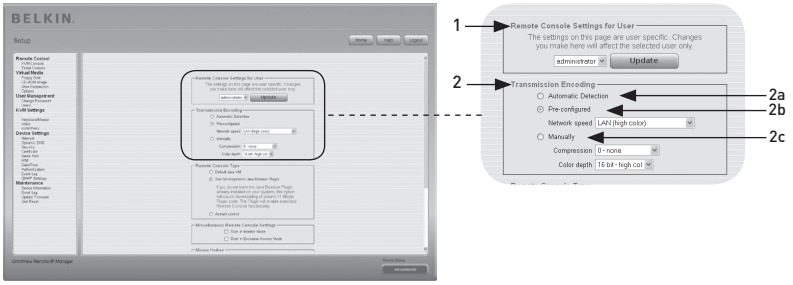
1. **Existing Users (Benutzerliste)**
   Wählen Sie einen aufgeführten Benutzer zur Bearbeitung aus. Nach der Auswahl klicken Sie auf die Schaltfläche “lookup” (nachschlagen), um die Benutzerdaten aufzurufen.
2. **New Username (Neuer Benutzername)**
   Der neue Benutzername für das ausgewählte Konto.
3. **Password (Kennwort)**
   Das Kennwort zum Benutzernamen. Es muss aus mindestens vier Zeichen bestehen.
4. **Confirm Password (Kennwort bestätigen)**
   Hier muss das Kennwort zur Bestätigung nochmals eingegeben werden.
5. **Email Address (E-Mailadresse)**
   Diese Eingabe ist optional.
6. **Mobile Number (Handynummer)**
   Diese Eingabe ist optional.
7. **Role (Rolle)**
   Neben der Registrierung als Administrator oder normaler Benutzer, kann jeder Benutzer Teil einer Gruppe sein (ihm kann eine “Rolle” zugewiesen sein). Wählen Sie die gewünschte Rolle aus der Liste aus.Um einen neuen Benutzer zu erstellen, klicken Sie auf die Schaltfläche “Create” (Erstellen). Über die Schaltfläche “Modify” (Bearbeiten) können die angezeigten Benutzereinstellungen geändert werden. Um einen Benutzer zu entfernen, klicken Sie auf die Schaltfläche “Delete” (Löschen).

   Hinweis: Der RIPM verfügt über einen hostunabhängigen Prozessor, der limitiert ist und einen Speicher, der nur bestimmte Verarbeitungsbefehle ausführen kann. Um eine annehmbare Reaktionszeit zu garantieren, empfiehlt Belkin, dass NICHT mehr als 25 Benutzer zugleich mit dem RIPM verbunden sein sollten. Die Größe des verfügbaren Speicherplatzes auf dem RIPM hängt von der Konfiguration und der Verwendung des RIPM ab (Protokolldateieinträge usw.).

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:34:41 AM

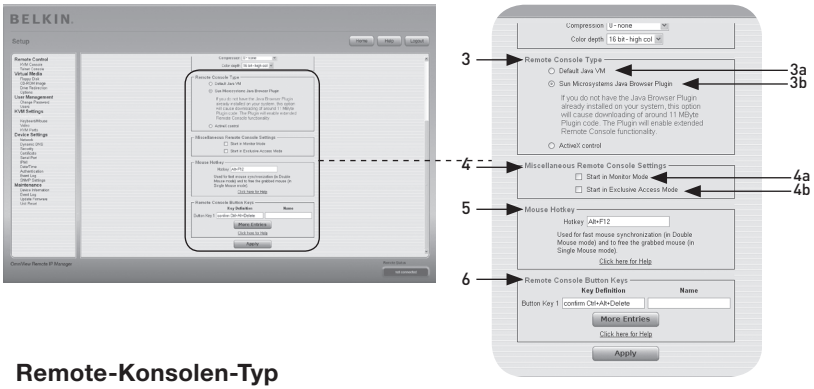
Benutzer-Konsole

Die folgenden Einstellungen sind benutzerspezifisch. Das heißt, dass der Administrator diese Einstellungen für jeden Benutzer einzeln einstellen kann. Die Änderung der Einstellungen für einen Benutzer berührt die Einstellungen für die anderen Benutzer nicht.



1. **Remote-Konsolen-Einstellungen für Benutzer**
   Dieses Auswahlfeld beinhaltet die Benutzer-ID für die die Werte angezeigt werden und für die die Änderungen gültig sind. Wählen Sie den entsprechenden Benutzer aus dem Auswahlfeld aus und klicken Sie auf die Schaltfläche “Update” (Aktualisieren). Die Benutzereinstellungen werden wie hier gezeigt angegeben.
   Hinweis: Sie können die Einstellungen der Benutzer nur bearbeiten, wenn Sie über die notwendigen Rechte dazu verfügen. Für einen normalen Benutzer ist es nicht möglich, ohne besondere Rechte die Einstellungen anderer Benutzer zu ändern.
2. **Transmission Encoding (Übertragungskodierung)**
   Diese Einstellung ermöglicht Ihnen, den Abbild-Kodierungsalgorithmus, mit dem Grafikdaten an die Remote-Konsole übertragen werden, zu ändern. Damit können Sie die Geschwindigkeit des entfernten Bildschirms je nach der Zahl der parallel angemeldeten Benutzer und der Bandbreite der Verbindungsleitung (Modem, ISDN, DSL, LAN usw.) optimieren.
   2a. Automatic Detection (Automatische Erkennung)
   Kodierungs- und Komprimierungsebenen werden auf der Grundlage der verfügbaren Bandbreite und des aktuellen Inhalts des Abbilds automatisch bestimmt.
   2b. Pre-Configured Settings (Voreinstellungen)
   Mit den Voreinstellungen lässt es sich am besten arbeiten, weil die Komprimierungen optimiert sind und die Farbtiefe an die angegebene Netzwerkgeschwindigkeit angepasst ist.
   2c. Manual Configuration (Manuelle Einrichtung)
   Damit richten Sie die Komprimierungsrate und die Farbtiefe individuell ein. Je nach ausgewählter Komprimierungsrate, wird der Datenstrom zwischen RIPM und der Remote-Konsole komprimiert, um Bandbreite zu sparen. Da höhere Komprimierungsraten die Abläufe verlangsamen, sollten Sie sie nicht verwendet werden, wenn mehrere Benutzer mit dem RIPM verbunden sind. Die Standard-Farbtiefe beträgt 16 Bit (65536 Farben). Die anderen Farbtiefen eignen sich für langsamere Netzwerkverbindungen, um mit diesen eine schnellere Datenübertragung zu ermöglichen. Daher verwendet die Komprimierungsebene 0 (keine Komprimierung) nur die Farbtiefe von 16 Bit. Ein niedrigere Bandbreite, nur 4 Bit (16 Farben) und 2 Bit (vier Graustufen) sind für normale Desktop-Schnittstellen empfehlenswert. Fotoartige Bilder werden am besten mit einer Farbtiefe von 4 Bit angezeigt. Ein-Bit-Farbtiefe (schwarz/weiß) sollte nur bei extrem langsamen Netzwerkverbindungen gewählt werden.

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:34:42 AM



3. Remote-Konsolen-Typ
Bestimmt, welcher Remote-Konsolen-Viewer verwendet wird.

3a. Default Java Virtual Machine (Vorgabe-JVM)
Diese Funktion arbeitet mit der voreingestellten JVM des Internetbrowsers, entweder Microsoft JVM für den Internet Explorer oder Sun JVM.

3b. Sun Microsystems Java Browser Plug-In
Dieses Plugin richtet den Internetbrowser Ihres Administrationssystems so ein, dass JVM von Sun Microsystems verwendet werden kann. Die JVM im Browser führt den Code im Remote-Konsolenfenster aus, das eigentlich ein Java Applet ist. Wenn Sie dieses Kontrollkästchen auf Ihrem Verwaltungssystem zum ersten Mal markieren und das entsprechende Java Plugin noch nicht installiert ist, wird es automatisch heruntergeladen und installiert. Damit die Installation möglich wird, müssen Sie noch die entsprechenden Dialogfelder mit “YES” (Ja) bestätigen. Die Datenmenge, die heruntergeladen werden muss, beträgt etwa 11 Mbit/s. Der Vorteil der heruntergeladenen JVM von Sun liegt darin, dass über unterschiedliche Plattformen hinweg eine stabile und einheitliche Java Virtual Machine ausgeführt wird. Die Software der Remote-Konsole ist für diese JVM-Version optimiert und bietet bei einer Ausführung in der JVM von Sun eine größere Bandbreite an Funktionen.

4. Verschiedene Konsoleneinstellungen für die Remote-Konsole

4a. Start in Monitor Mode (Im Kontrollmodus starten)
Mit dieser Einstellung können Sie einen Eingangswert für den Kontrollmodus bestimmen. Die Standardeinstellung des Kontrollmodus ist deaktiviert. Wenn Sie ihn aktivieren, wird das Remote-Konsolenfenster im Modus Schreibschutz-Modus geöffnet.

4b. Start in Exclusive-Access Mode (Im Modus “Alleinzugriff” starten)
Dies aktiviert den Modus “Alleinzugriff” beim Start der Remote-Konsole. Mit diesem Modus wird die Remote-Konsolen-Verbindung aller anderen Benutzer blockiert. Keine anderen Benutzer können die Remote-Konsole gleichzeitig öffnen, bis Sie diese Funktion deaktivieren oder sich abmelden.

5. Mouse Hot Key (Maustastenbefehl)
Mit dem Maustastenbefehl bestimmen Sie eine Tastenkombination für den Start der Maussynchronisation (indem Sie die Kombination in die Remote-Konsole eingeben) oder dem Verlassen des Einzelmausmodus.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:34:43 AM

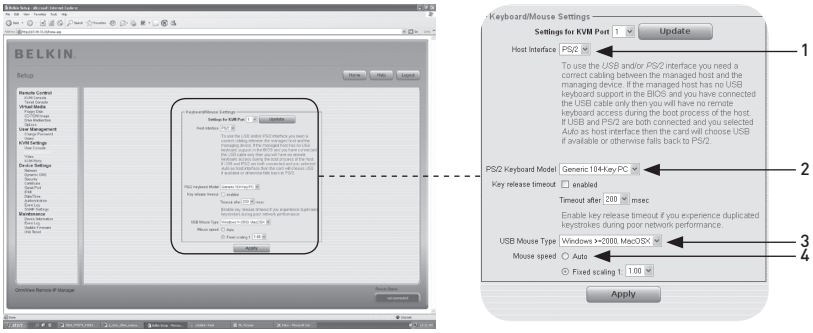
6. Remote Console Button Keys (Tastaturbefehle für die Remote-Konsole)
Mit der Schaltfläche können Sie auf dem Remote-System Tastaturkombinationen simulieren, die lokal nicht generiert werden können. Dies kann notwendig werden, wenn eine Taste fehlt oder das lokale Betriebssystem der Remote-Konsole einen bestimmten Tastenanschlag unbedingt annehmen muss. Typische Beispiele sind “Strg+Alt+Löschen” auf Windows- und DOS-Systemen, oder “Steuerung+Rücktaste” auf Linux-Systemen, um den X-Server zu beenden. Um einen neuen Tastaturbefehl zu bestimmen oder einen vorhandenen zu bearbeiten, beachten Sie die Regeln für die Einstellung eines Tastaturkodes. In der Regel lautet die Syntax für einen Tastaturkode folgendermaßen:

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

Ein Begriff in Klammern ist optional. Das Sternchen am Ende heißt, dass Sie weitere Tastaturkodes eingeben können, je nach Bedarf. Der Begriff “confirm” fügt einen Bestätigungsdialog hinzu, der angezeigt wird, bevor die Tastaturkodes an den Remote-Host übertragen werden können. Der “keycode” ist der jeweilige Tastaturkode. Mehrere Tastaturkodes können mit Plus-, Minus- oder “<”-Zeichen aneinandergereiht werden. Mit dem Pluszeichen werden Tastenkombinationen gebildet; alle Tasten sind zu drücken, bis die Kombination endet oder mit einem Minuszeichen abgeschlossen wird. Alle gedrückten Tasten werden hier in umgekehrter Reihenfolge wieder gelöst. Mit dem Minuszeichen werden einzelne, getrennte Tastenbetätigungen festgelegt. Mit dem “<”-Zeichen wird nur die letzte Tastenbetätigung gelöst. Das Sternchen fügt eine Pause von 100 Millisekunden ein. Zum Bespiel wird die Tastenkombination Strg, Alt und F mit der Sequenz “Strg+Alt+F2” dargestellt.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:34:43 AM

Tastatur/Maus



1. **Host-Schnittstelle**
   Die Host-Schnittstelle aktiviert die Schnittstelle, an der die Maus angeschlossen ist. Sie können “Auto” für automatische Erkennung, “USB” für eine USB-Maus, oder “PS/2” für eine PS/2-Maus wählen.

   Hinweis: Um die USB- und/oder PS/2-Schnittstelle zu gebrauchen, müssen Sie zwischen dem verwalteten Host und dem verwalteten Gerät die richtige Kabelverbindung herstellen. Wenn der verwaltete Host keine USB-Tastatur-Unterstützung im BIOS hat und Sie ein USB-Kabel verwendet haben, werden Sie während des Startvorgangs keinen Fernzugriff mit der Tastatur haben. Wenn USB und PS/2 angeschlossen sind und Sie “Auto” als Host-Schnittstelle gewählt haben, wird USB beim Systemstart ausgewählt werden (falls verfügbar). Ist USB nicht verfügbar, wird “PS/2” ausgewählt.

   Um den ferngesteuerten USB-Tastaturzugriff während des Startvorgangs des Hosts zu erhalten, müssen die folgenden Bedingungen erfüllt sein:

   - das Host-BIOS muss über USB-Tastatur-Unterstützung verfügen
   - das USB-Kabel muss über die Option “Host-Schnittstelle” verbunden oder ausgewählt sein

2. **PS/2-Tastaturlayouts**
   Damit können Sie ein Tastatur-Layout aus “Generic 101-Key PC” für ein standardmäßiges Tastatur-Layout, “Generic 104-Key PC” für ein standardmäßiges Tastatur-Layout mit drei zusätzlichen Windows-Tasten, “Generic 106-Key PC” für eine japanische Tastatur und “Apple Macintosh” für die Macintosh® Tastatur auswählen. Wenn ein Zeitlimit für die Tastatur benötigt wird, wählen Sie die passende Option aus und geben Sie das gewünschte Zeitlimit in das unten stehende Eingabefeld ein.

3. **USB-Maustyp**
   Damit wird der USB-Maus-Typ aktiviert. Wählen Sie eine zutreffende Option aus dem Auswahlfeld aus. Eine ausführliche Beschreibung des Maus-Typs und der empfohlenen Optionen für die verschiedenen Betriebssysteme finden Sie im Abschnitt “Empfohlene Maus-Einstellungen” auf Seite 21 dieses Handbuchs.

*Diese Funktion funktioniert nur mit Windows Betriebssystemen.

P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:34:44 AM

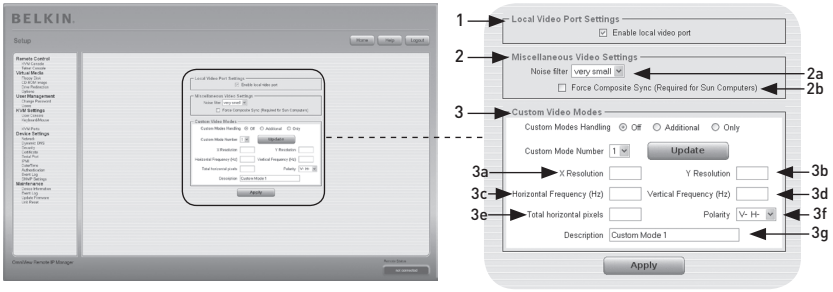
4. Mausgeschwindigkeit

- **Mausgeschwindigkeit**
  Verwenden Sie diese Option, wenn die Maus-Einstellungen des Hosts eine zusätzliche Beschleunigungseinstellung gebrauchen. Der RIPM entdeckt die Beschleunigung und Geschwindigkeit der Maus während des Synchronisieru ngsvorgangs der Maus.
- **Feste Mausgeschwindigkeit**
  Verwenden Sie diese Option für eine direkte Übersetzung der Mausbewegungen zwischen dem lokalen und dem Remote-Mauszeiger. Sie können auch eine feste Skalierung wählen, die die Anzahl der Bewegungen des Remote-Mauszeigers bestimmt, wenn der lokale Mauszeiger um ein Pixel bewegt wird. Diese Option funktioniert nur, wenn die Mauseinstellungen auf dem Host linear sind, wenn also z. B. keine Zeigerbeschleunigung aktiviert ist.

Klicken Sie zum Einstellen der Optionen auf “Apply” (Übernehmen).

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:34:44 AM

Grafik



Klicken Sie zum Einstellen der Optionen (siehe unten) auf “Apply” (Übernehmen).

1. **Einstellungen der lokalen Grafikschnittstelle**

   Enable Local Video Port (Lokale Grafikschnittstelle aktivieren)
   Diese Option überwacht den lokalen Grafikausgang des RIPM und zeigt an, ob dieser aktiv ist und das ankommende Signal des Host-Systems weiterleitet.

2. **Verschiedene Grafikeinstellungen**

   2a. Entstörfilter
   Diese Funktion definiert, wie das RIPM auf kleine Änderungen im Grafikeingangssignal reagiert. Eine umfassende Filtereinstellung benötigt weniger Netzwerkverkehr und führt zu einer schnelleren Grafikanzeige, allerdings könnten kleine Änderungen in einigen Anzeige-Bereichen nicht sofort erkannt werden. Ein kleiner Filter zeigt alle Änderungen sofort an, kann aber zu einem konstanten Netzwerkverkehr führen, selbst dann, wenn sich der Inhalt der Anzeige nicht wirklich ändert (abhängig von der Qualität des Grafikeingangsignals).

   2b. Force Composite Sync (wird für Sun Computer benötigt)
   Aktivieren Sie diese Option, um eine Signalübermittlung von einem Sun Computer zu unterstützen.
   Wenn diese Funktion nicht aktiviert ist, wird das Bild der Remote-Konsole nicht sichtbar sein.

3. **Custom Video Modes (Individueller Grafikmodus)**
   Die maximale Anzahl der individuellen Grafikauflösungen ist vier.

   Die Option “Custom Modes Handling” (Individuelle Modusverwaltung) ermöglicht das Abschalten von individuellen Modi (“Off” [Aus]) oder die Einstellung von standardmäßigen oder exklusiven Grafikauflösungen (“Only” [Nur]). Die letzte Option (“Additional” [Zusätzlich]) erlaubt Ihnen die Einstellung eines besonderen Grafikmodus für den RIPM. Um die Parameter für den individuellen Grafikmodus zu ändern, wählen Sie die betreffende Zahl aus dem Auswahlfeld aus und drücken Sie die Schaltfläche “Update” (Aktualisieren). Sie müssen einige zusätzliche Informationen angeben, damit der Grafikmodus korrekt erkannt werden kann:

   Achtung: Die Option “Host Monitor Settings” (Host-Bildschirm-Einstellungen) ist nur für erfahrene Benutzer geeignet. Eine inkorrekte Anwendung kann die Grafiküb ertragungsleistung beeinträchtigen. Stellen Sie sicher, dass Sie die Funktion genau verstehen, bevor Sie die Host-Bildschirm-Einstellungen verändern.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:34:45 AM

3a. X Resolution (X Auflösung)
Dies bezieht sich auf die sichtbare Anzahl von horizontalen Pixeln.

3b. Y Resolution (Y Auflösung)
Dies bezieht sich auf die sichtbare Anzahl von vertikalen Pixeln.

3c. Horizontale Frequenz (Hz)
Dies bezieht sich auf die horizontale (Linien-)Frequenz in Hertz.

3d. Vertikale Frequenz (Hz)
Dies bezieht sich auf die vertikale (Aktualisierungs-)Frequenz in Hertz.

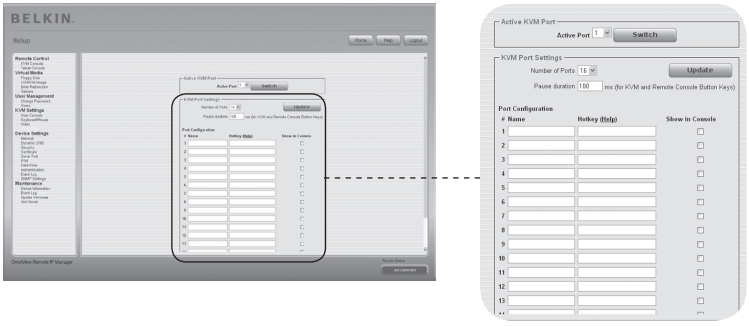
3e. Total horizontal pixels (Gesamtzahl der horizontalen Pixel)
Dies bezieht sich auf die Gesamtzahl von Pixeln pro Linie, einschließlich unsichtbaren und ausgeblendeten Bereichen.

3f. Polarity (Polarität)
Dies bezieht sich auf die positive oder negative Charakteristik der Synchr onisierungssignale. V bedeutet vertikale Polarität; H bedeutet horizontale Polarität.

3g. Description (Beschreibung)
Hier können Sie einen Modusnamen angeben, der in der Remote-Konsole gezeigt wird, wenn der individuelle Modus aktiviert ist.

KVM-Ports

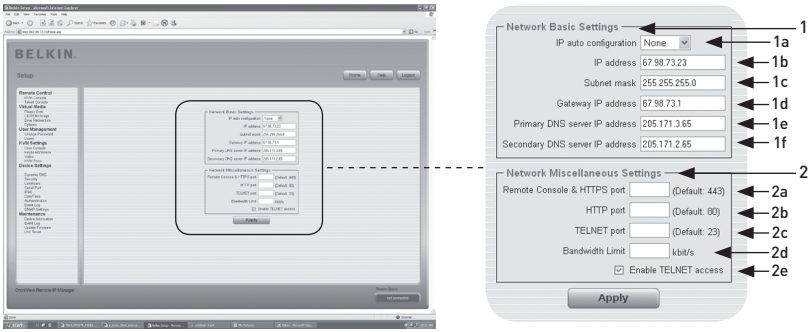
Sie können festlegen, wie viele Anschlüsse vom angeschlossenen KVM-Switch genutzt werden, und jedem Port einen Namen zuweisen. Damit die KVM-Ports über den RIPM durchgeschaltet werden können, muss für jeden Port eine Tastenkombination festgelegt werden.



P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:34:45 AM

Netzwerk

Das Bedienfeld “Netzwerkeinstellungen” (siehe unten) erlaubt Ihnen die Änderung von netzwerkbezogenen Parametern, wie unten erläutert. Einmal übernommen, sind die neuen Netzwerkeinstellungen sofort wirksam.



Achtung: Die Änderung der Netzwerkeinstellungen beim RIPM kann zu einem Ausfall der Netzwerkverbindung führen. Wenn Sie die Einstellungen entfernt bearbeiten, stellen Sie daher sicher, dass alle Werte korrekt sind, so dass Sie weiterhin auf den RIPM zugreifen können.

1. **Grundlegende Netzwerkeinstellungen**

1a. IP Auto Configuration (Automatische IP-Konfiguration)
Mit dieser Option können Sie den Bereich bestimmen, von dem der RIPM seine Netzwerkeinstellungen bezieht—entweder durch einen DHCP- oder BOOTP-Server. Wählen Sie für DHCP, “DHCP”; für BOOTP wählen Sie “bootp”. Wenn Sie “none” (keinen) wählen, ist die Automatische IP-Konfiguration deaktiviert.

1b. The IP address (Die IP-Adresse) wird Ihnen von Ihrem Netzwerk-Administrator zugewiesen.

1c. Der Begriff **“Subnet Mask”** bezieht sich auf die Netzwerkmaske des lokalen Netzwerks, die zur Feststellung des Subnets, zu der eine IP-Adresse gehört, verwendet wird.

1d. Gateway-IP-Adresse
Wenn auf den RIPM von anderen Netzwerken als dem lokalen Netzwerk zugegriffen werden soll, geben Sie diese IP-Adresse bei der IP-Adresse des lokalen Netzwerk-Routers an.

1e. Primäre DNS-Server-IP-Adresse
Dies ist die IP-Adresse des primären Domain Name Server (DNS) in URL-Schreibweise. Sie können diese Option frei lassen; wenn Sie dies aber tun, kann der RIPM keine URL-Namen auflösen.

1f. Sekundäre DNS-Server-IP-Adresse
Dieser Begriff bezieht sich auf die IP-Adresse des sekundären DNS in URL-Schreibweise. Sie wird dann benutzt, wenn der Primäre DNS-Server nicht erreicht werden kann.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:34:46 AM

2. Verschiedene Netzwerkeinstellungen

2a. Remote-Konsole und HTTPS-Port
Dies ist die Port-Nummer, auf die der Server des RIPM und der HTTPS-Server reagieren. Wenn kein bestimmter Wert eingestellt ist, gilt der Standardwert.

2b. HTTP-Port
Dies ist die Port-Nummer, auf die der HTTP-Server des RIPM reagiert. Wenn kein bestimmter Wert eingestellt ist, wird die Voreinstellung verwendet.

2c. Telnet-Port
Dies ist die Port-Nummer, auf die der Telnet-Server des RIPM reagiert. Wenn kein bestimmter Wert eingestellt ist, gilt der Vorgabewert.

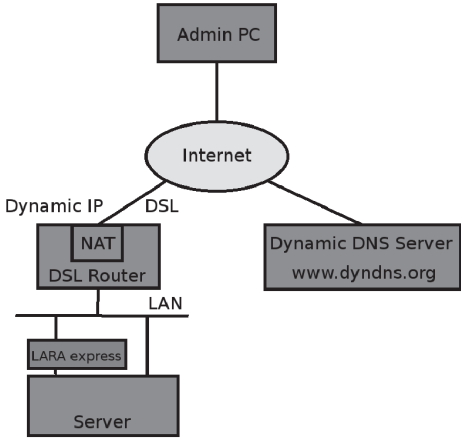
2d. Bandwidth Limit (Bandbreitenbegrenzung)
Diese Option bezieht sich auf den maximalen Netzwerkverkehr, der durch das RIPM Ethernet-Gerät generiert wird (Wert in Kbit/s).

2e. Enable Telnet Access (Telnet-Zugriff aktivieren)
Das Einstellen dieser Option ermöglicht Benutzern, über den Telnet-Gateway auf den RIPM zuzugreifen (siehe den Abschnitt “Telnet-Konsole” auf S. 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:34:46 AM

Dynamische DNS

Ein frei verfügbarer Dynamischer DNS-Service (dyndns.org) kann wie folgt benutzt werden:



Dynamischer DNS-Service

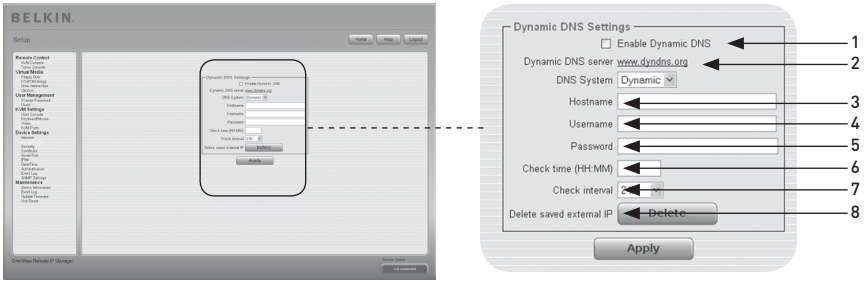
Sie können den RIPM über die IP-Adresse Ihres DSL-Routers erreichen, die Ihnen als dynamische IP-Adresse von Ihrem Internet-Provider zugewiesen wird. Da der Administrator diese zugewiesene IP-Adresse nicht kennt, verbindet sich der RIPM in regelmäßigen Intervallen mit einem speziellen, dynamischen DNS und registriert dort seine IP-Adresse. Der Administrator kann diesen Server ebenfalls kontaktieren und die gleiche, zur Netzwerkkarte (NIC) gehörende IP-Adresse auswählen. Der Administrator muss den RIPM für den Service des dynamischen DNS anmelden und ihm einen bestimmten Host-Namen zuweisen. Während des Anmeldevorgangs werden ein Benutzername und ein Kennwort zugewiesen. Diese Kontodaten sind, zusammen mit dem Host-Namen, nötig, um die IP-Adresse des registrierten RIPM zu bestimmen.

Sie müssen die folgenden Schritte durchführen, um dynamisches DNS zu aktivieren:

- Achten Sie darauf, dass die LAN-Schnittstelle des RIPM richtig eingestellt ist.
- Geben Sie die dynamischen-DNS-Einstellungen ein, wie auf Seite 55 dargestellt ist.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:34:46 AM

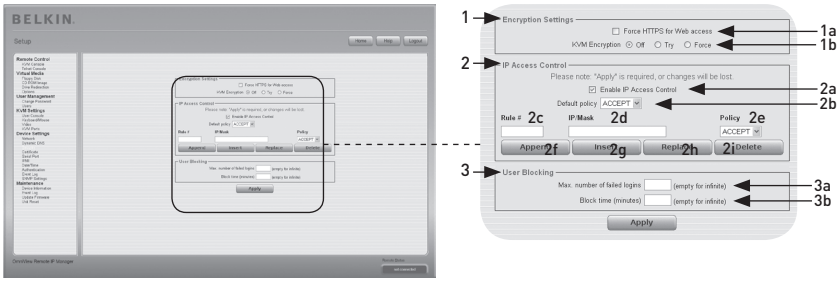
Dynamische DNS-Einstellungen



1. **Enable Dynamic DNS (Dynamisches DNS aktivieren)**
   Dies aktiviert den Dynamischen DNS-Service. Dazu wird eine konfigurierte DNS-Server-IP-Adresse benötigt.
2. **Dynamic DNS Server (Dynamischer DNS-Server)**
   Der RIPM meldet sich selbst in regelmäßigen Intervallen bei diesem Bereich an. Zum Zeitpunkt dieser Anleitung ist das dynamische DNS eine feste Einstellung, da zur Zeit nur dyndns.org unterstützt wird.
3. **Host-Name**
   RIPM ist der Host-Name, der durch das dynamische DNS vergeben wird. Verwenden Sie den ganzen Namen, einschließlich der Domäne, z. B., “testserver.dyndns.org” (oder “RIPM.dyndns.org”) und nicht nur den eigentlichen Host-Namen.
4. **Username (Benutzername)**
   Während Ihrer manuellen Registrierung mit dem dynamischen DNS, müssen Sie diesen Benutzernamen angemeldet haben.
   Hinweis: Innerhalb des Benutzernamens sind keine Leerzeichen erlaubt.
5. **Password (Kennwort)**
   Während Ihrer manuellen Registrierung mit dem dynamischen DNS, müssen Sie das Kennwort zuweisen.
6. **Check Time (Zeitprüfung)**
   Die Karte des RIPM registriert sich selbst bei der der Zeitprüfung des dynamischen DNS.
7. **Check Interval (Intervallprüfung)**
   Das Zeitintervall, mit dem sich der RIPM beim dynamischen DNS meldet.
   Hinweis: Der RIPM hat seine eigene, unabhängige Echtzeit-Uhr. Achten Sie darauf, dass die Zeiteinstellung des RIPM korrekt ist.
8. Nutzen Sie die Option **“Delete saved external IP” (Gespeicherte externe IP-Adresse löschen),** wenn Sie Ihre extern gespeicherte IP-Adresse aktualisieren möchten. Um die gespeicherte IP-Adresse zu löschen, drücken Sie auf die Schaltfläche “Delete” (Löschen).

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:34:47 AM

Sicherheit



1. Verschlüsselungseinstellungen

1a. Force HTTPS (HTTPS erzwingen)
Wenn diese Option aktiviert ist, ist der Zugriff auf die Weboberfläche nur bei einer HTTPS-Verbindung möglich. Der RIPM wird über den HTTPS-Port nicht nach eingehenden Verbindungen suchen. Für den Fall, dass Sie Ihr eigenes SSL-Zertifikat für den Gebrauch mit dem RIPM erstellen möchten, lesen Sie den Abschnitt “Zertifikate” auf Seite 58.

1b. KVM Encryption (KVM-Verschlüsselung)
Diese Option steuert die Verschlüsselung des Remote Frame Buffer (RFB)-Protokolls. Die Remote-Konsole benutzt RFB, um Bildschirmdaten zum Administratorencomputer zu übermitteln und die Tastatur-/Mausdaten zurück zum Host zu senden. Bei der Einstellung “Off” (Aus), ist keine Verschlüsselung aktiviert. Bei der Einstellung “Try” (Versuchen) versucht die Anwendung, eine verschlüsselte Verbindung aufzubauen. Kann diese Verbindung nicht hergestellt werden, wird eine unverschlüsselte Verbindung verwendet. Bei der Einstellung “Force” versucht die Anwendung, eine verschlüsselte Verbindung aufzubauen. Bricht die Verbindung ab, erstellt das System einen Fehlerbericht.

2. IP-Access Control (IP-Zugriffskontrolle)
Dieser Abschnitt erklärt die Einstellungen für die IP-Zugriffskontrolle. Sie wird für die Zugriffsbeschränkung ausgewählter Clients benutzt. Diese Clients werden über die IP-Adressen identifiziert, mit denen sie Verbindungen aufbauen.

Achtung: Die Einstellungen der IP-Zugriffskontrolle gelten nur für die LAN-Schnittstelle.

2a. Enable IP-Access Control (IP-Zugriffskontrolle aktivieren)
Aktiviert die Zugriffskontrolle basierend auf den IP-Quelladressen.

2b. Default Policy (Standardregel)
Diese Option bestimmt, was mit IP-Paketen geschieht, die nicht den eingestellten Regeln entsprechen. Sie können angenommen oder verworfen werden.

Achtung: Wenn Sie die Option “DROP” (VERWERFEN) wählen, aber keine Regeln zum ANNEHMEN (ACCEPT) konfiguriert haben, ist der Webzugang per LAN deaktiviert. Sie können den Zugang wieder ermöglichen, indem Sie die Sicherheitseinstellungen über Modem verändern oder die IP-Zugriffskontrolle mit der Initialisierungskonfigurierung vorübergehend deaktivieren.

2c. Rule Number (Regelnummer)
Hier müsste die Nummer einer Regel stehen, für die die folgenden Befehle gelten. Das Feld wird ignoriert, wenn eine neue Regel hinzugefügt wird.

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:34:48 AM

2d. IP/Mask
Legt die IP-Adresse oder den IP-Adressbereich fest, für die/den die Regel gilt. Bei den folgenden Beispielen gibt die Zahl nach dem Schrägstrich " / " an der IP-Adresse die Anzahl der genutzten gültigen Bits aus der angegebenen IP-Adresse an.

192.168.1.22/32 entspricht der IP-Adresse 192.168.1.22

192.168.1.0/24 entspricht allen IP-Paketen mit einer Quelladresse zwischen 192.168.1.0 und 192.168.1.255

0.0.0.0/0 entspricht allen IP-Paketen

2e. Policy (Regelung)
Die Regelung bestimmt das Vorgehen mit übereinstimmenden Paketen. Sie können angenommen oder verworfen werden.

Achtung: Die Reihenfolge der Regeln ist wichtig. Die Regeln werden aufsteigend geprüft, bis eine Regel zutrifft. Alle Regeln unterhalb der zutreffenden Regel werden ignoriert. Die Standardregel trifft zu, wenn keine Übereinstimmung gefunden wurde.

2f. Appending a Rule (Hinzufügen einer neuen Regel)
Geben Sie die IP/Maske ein und erstellen Sie die Regel. Drücken Sie am Schluss auf die Schaltfläche "Append" (Hinzufügen).

2g. Inserting a Rule (Eine Regel eingeben)
Geben Sie die Regelnummer und die IP/Maske ein. Erstellen Sie die Regel. Drücken Sie am Schluss auf die Schaltfläche "Insert" (Einfügen).

2h. Replacing a Rule (Eine Regel ersetzen)
Geben Sie die Regelnummer und die IP/Maske ein. Erstellen Sie die Regel. Drücken Sie am Schluss auf die Schaltfläche "Replace" (Ersetzen).

2i. Deleting a Rule (Eine Regel löschen)
Geben Sie die Regelnummer ein und drücken Sie auf "Delete" (Löschen).

3. Benutzer sperren
Der Blockiermechanismus erlaubt dem Administrator die Anmeldung eines bestimmten Nutzers zu sperren, wenn sein oder ihr Kennwort einige Male falsch eingegeben wurde. Die Dauer der Sperrung ist ebenfalls einstellbar.

3a. Maximale Anzahl von fehlgeschlagenen Anmeldungen (Failed Logins)
Geben Sie die maximale Anzahl für fehlgeschlagene Anmeldungen ein, nach denen ein Benutzer gesperrt werden sollte. Lassen Sie dieses Feld frei, wenn die Blockierfunktion ausgeschaltet werden soll.

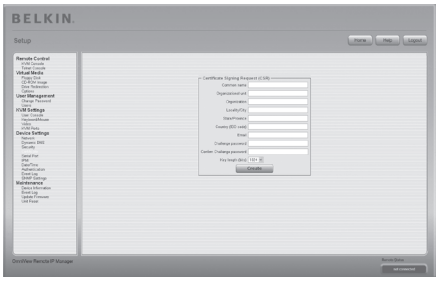
3b. Block Time (Sperrzeit)
Die Minutenzahl, für die ein Benutzer gesperrt ist, nachdem er oder sie die maximale Anzahl für fehlgeschlagene Anmeldungen überschritten haben. Lassen Sie dieses Feld frei, um den Benutzer so lange zu sperren, bis die Sperre manuell aufgehoben wird.

Unblocking Users (Nutzer entsperren)
Es gibt zwei Arten von Sperrungen:

- Ein übergeordneter Benutzer kann zu den Einstellungen des Benutzermanagements gehen (siehe Abschnitt "Benutzermanagement") und für den Benutzer die Schaltfläche "Unblock" (Entsperren) drücken.
- Ein Administrator kann die serielle Konsole für die erste Konfiguration benutzen und sich als zu entsperrendem Nutzer ("unblock") anmelden. Der RIPM wird nach dem Administrator-Kennwort fragen und eine Liste gesperrter Nutzer anzeigen, die entsperrt werden können.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:34:48 AM

Zertifikat



Zertifikateinstellungen

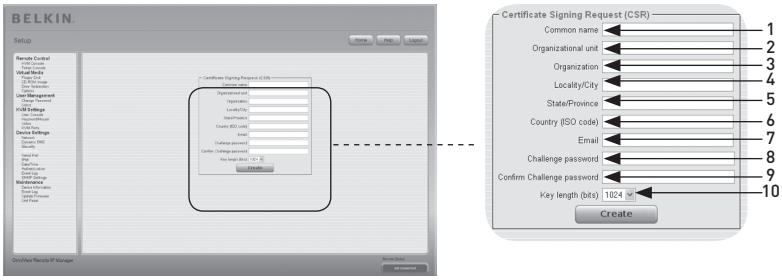
Der RIPM benutzt das Secure Socket Layer (SSL) -Protokoll für den verschlüsselten Netzwerkverkehr mit einem verbundenen Client. Während des Verbindungsaufbaus muss sich der RIPM gegenüber dem Client mit Hilfe eines Verschlüsselungszertifikats ausweisen. Zum Lieferzeitpunkt wird dieses Zertifikat und der darunter liegende Geheimschlüssel für alle RIPMs gleich sein und nicht mit der Netzwerkeinstellung übereinstimmen, der vom Benutzer für den RIPM verwendet wird. Der dem Zertifikat zugrunde liegende Geheimschlüssel wird auch für die Sicherung des SSL-Handshake-Signals benutzt. Allerdings kann ein neues base64 x.509 Zertifikat erzeugt und installiert werden, das nur für einen bestimmten RIPM gilt. Hierzu kann der RIPM einen neuen Schlüssel und die zugehörige Zertifikat-Bescheinigungsanforderung (Certificate Signing Request: CSR) generieren, die von einer Zertifizierungsstelle (ZS) bestätigt werden muss. Die betreffende Zertifizierungsstelle prüft Ihre Identität nach und stellt Ihnen dann ein SSL-Zertifikat aus. Um ein SSL-Zertifikat für den RIPM zu erstellen und zu installieren gehen Sie wie folgt vor:

- Erstellen Sie mit dem in der folgenden Abbildung gezeigten Bedienfeld ein SSL CSR. Sie müssen einige Felder ausfüllen, diese werden unten stehend erklärt. Sobald Sie fertig sind, klicken Sie auf die Schaltfläche “Create” (Erstellen); die CSR-Erstellung wird gestartet. Die Zertifikat-Bescheinigu ngsanforderung (CSR) kann mit der Schaltfläche “Download CSR” (CSR herunterladen) in Ihren Verwaltungscomputer geladen werden.
- Senden Sie die gespeicherte CSR zur Zertifizierung an eine Zertifizierungsstelle. Sie erhalten von der Zertifizierungsstelle ein neues Zertifikat.
- Laden Sie das Zertifikat in den RIPM, verwenden Sie dazu die Schaltfläche “Create” (Erstellen).

Nachdem Sie diese drei Schritte ausgeführt haben, wird der RIPM sein eigenes Zertifikat haben, das die Karte für die Clients erkennbar macht.

Achtung: Wenn die CSR auf dem RIPM verloren geht, kann sie nicht wiederhergestellt werden! Wenn Sie sie versehentlich löschen, wiederholen Sie die drei Schritte.

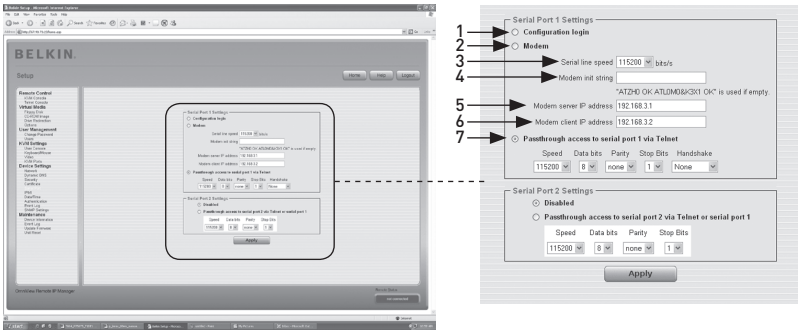
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:34:48 AM



1. **Common Name (Eigenname)**
   Dies ist der Netzwerkname des RIPM, sobald er im Netzwerk des Nutzers installiert ist (gewöhnlich der voll qualifizierte Domänenname). Er ist mit dem Namen identisch,
   der für den Zugriff auf den RIPM über einen Browser genutzt wird, aber ohne das Präfix
   "http://". Wenn auf den RIPM mit HTTPS zugegriffen wird und der hier gegebene Name
   und das aktuelle Netzwerk verschieden sind, wird der Browser eine Sicherheitswarnung anzeigen.
2. **Organizational Unit (Abteilung)**
   Dieses Feld spezifiziert die Abteilung, zu der der RIPM innerhalb der Organisation
   gehört.
3. **Organization (Betrieb/Firma)**
   Der Name des Betriebs, zu dem der RIPM gehört.
4. **Locality/City (Ort)**
   Der Ort, an dem sich der Betrieb befindet.
5. **State/Province (Staat/Bundesland)**
   Der Staat bzw. das Bundesland, in dem sich der Betrieb befindet.
6. **Country (ISO Code) (Land)**
   Das Land, in dem sich der Betrieb befindet (ein ISO-Code bestehend aus 2 Buchstaben, z. B. DE für Deutschland).
7. **Challenge Password (Verifiziertes Kennwort)**
   Bestimmte Zertifizierungsstellen verlangen ein verifiziertes Kennwort, das zur Autorisierung von späteren Änderungen am Zertifikat erforderlich ist (zum Beispiel zur Aufhebung des Zertifikats). Das Kennwort besteht aus mindestens vier Zeichen.
8. **Confirm Challenge Password (Verifiziertes Kennwort bestätigen)**
   Erfordert die Neueingabe des verifizierten Kennwortes.
9. **Email**
   Dies bezieht sich auf die E-Mail-Adresse einer Kontaktperson, die für den RIPM und seine Sicherheit verantwortlich ist.
10. **Key Length (Schlüssellänge)**
    Die Länge des erzeugten Schlüssels, angegeben in Bit. In der Regel sind 1024 Bit ausreichend. Längere Schlüssel können zu einer langsameren RIPM-Reaktion während des Verbindungsaufbaus führen.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:34:49 AM

Serielle Schnittstelle



In den seriellen Einstellungen des RIPM geben Sie an, welche Geräte mit der seriellen Schnittstelle verbunden sind und wie sie genutzt werden. Für den Zugriff auf die serielle Schnittstelle wird ein Nullmodemkabel benötigt.

1. **Konfiguration oder Konsolen-Anmeldung (Login)**
   Benutzen Sie die serielle Schnittstelle nicht für eine Spezialfunktion; benutzen Sie sie nur für die erste Konfiguration.
2. **Modem**
   Der RIPM bietet neben seinem Standardzugang über den integrierten Ethernet-Adapter auch Zugriff über die Telefonleitung. Das Modem muss mit der seriellen Schnittstelle des RIPM verbunden sein. Technisch gesehen ist die RIPM-Verbindung über die Telefonleitung nichts anderes als eine dedizierte Punkt-zu-Punkt-Verbindung zwischen Ihrem Konsolen-Computer und dem RIPM. In anderen Worten: Das RIPM funktioniert als Internet Service Provider (ISP), bei dem Sie sich einwählen können. Die Verbindung wird über ein Punkt-zu-Punkt-Protokoll (PPP) hergestellt. Bevor Sie die Verbindung zum RIPM herstellen, müssen Sie den Konsolen-Computer entsprechend konfigurieren. Auf Windows Systemen können Sie zum Beispiel eine DFÜ-Verbindung einrichten, die die benötigten Einstellungen wie PPP bereits standardmäßig enthält. Das Bedienfeld “Modemeinstellungen” erlaubt Ihnen die Konfigurierung des Fernzugriffs auf den RIPM über ein Modem. Die Bedeutung der einzelnen Parameter wird nachfolgend beschrieben. Die Modemeinstellungen sind Teil des Bedienfelds “Serial Settings” (Serielle Einstellungen).
3. **Serial Line Speed (Serielle Verbindungsrate)**
   Die Geschwindigkeit, in der der RIPM mit dem Modem kommuniziert. Die meisten Modems unterstützen heutzutage den Standardwert 115.200 Bit/s. Wenn Sie ein älteres Modem nutzen und es zu Problemen kommt, setzen Sie diese Geschwindigkeit herab.
4. **Modem Init String (Modem-Initialisierungszeichenfolge)**
   Die Zeichenfolge, mit der der RIPM das Modem initialisiert. Der vorgegebene Wert eignet sich für alle Standardmodems, die direkt an eine Telefonleitung angeschlossen sind. Wenn Sie ein spezielles Modem verwenden oder das Modem an eine Telefonanlage angeschlossen ist, das für die Durchschaltung zum Amt eine spezielle Wahlsequenz benötigt, können Sie dies durch Einstellen einer neuen Zeichenfolge anpassen. Informationen zur AT-Befehlssyntax finden Sie im Modemhandbuch.

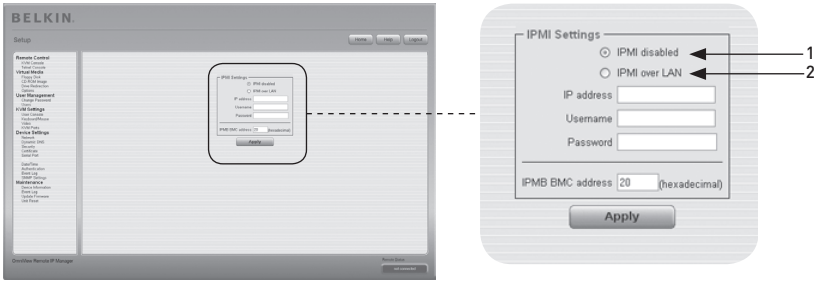
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:34:50 AM

5. **Modem Server IP Address (Modem-Server IP-Adresse)**
   Diese IP-Adresse wird dem RIPM während des PPP-Handshakes. Da es sich um eine reine Punkt-zu-Punkt-IP-Verbindung handelt, kann praktisch jede IP-Adresse, außer der Adresse des RIPM oder des Konsolen-Computers, ausgewählt werden. Normalerweise kann der vorgegebene Wert übernommen werden.
6. **Modem Client IP Address (Modem-Client IP-Adresse)**
   Diese IP-Adresse wird dem Konsolen-Computer während des PPP-Handshakes zugewiesen. Da es sich um eine reine Punkt-zu-Punkt-IP-Verbindung handelt, kann praktisch jede IP-Adresse, außer der IP-Adresse des RIPM oder des Konsolen-Computers, zugewiesen werden. Normalerweise kann der vorgegebene Wert übernommen werden.
7. **Pass-Through Access to Serial Port via Telnet (Passthru-Zugang zur seriellen Schnittstelle über Telnet)**
   Mit dieser Option können Sie ein beliebiges Gerät an die serielle Schnittstelle anschließen und über Telnet darauf zugreifen (das Gerät muss hierzu Terminal-Support bieten.) Wählen Sie die betreffenden Optionen für die serielle Schnittstelle aus und stellen Sie mit dem Telnet-Gerät oder einem Telnet-Standardclient die Verbindung zum RIPM her. Weitere Informationen zur Telnet-Schnittstelle finden Sie im Abschnitte “Telnet-Konsole”.

   Hinweis: Eine Liste von kompatiblen Modems finden Sie auf www.belkin.com.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:34:50 AM

Intelligente Plattform-Verwaltungsoberfläche (IPVO)



Intelligente Plattform-Verwaltungsoberfläche (IPVO) bietet einen zusätzlichen Weg, das System zu starten oder einen Neustart durchzuführen. Außerdem bieten Ihnen diese Einrichtungen die Anzeige eines Host-Systemprotokolls und den Status einiger Systemsensoren (z. B. die Temperatur). Wenn Ihr Host-System IPVO unterstützt, können Sie wie folgt darauf zugreifen:

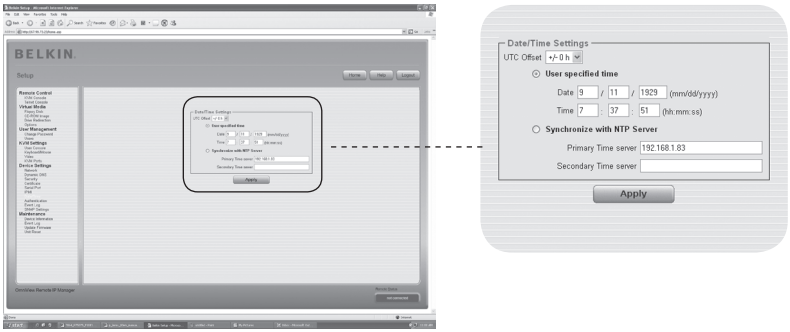
- IPVO über LAN (IPVO v1.5 benötigt)
- IPVO-Einstellungen

Die obige Abbildung zeigt das Bedienfeld der IPVO für den RIPM. Die Optionen werden nachstehend erklärt.

1. **IPMI Disabled (IPVO deaktiviert)**
   Deaktiviert IPVO auf dem RIPM. Das heißt, dass der Status über IPVO und das Protokoll über IPVO nicht verfügbar sind; die Ein-Ausschaltfunktionen sowie die Neustartfunktion setzen statt IPVO ATX (Advanced Technology Extended) ein und das Rücksetzkabel ist über den RIPM mit der Hauptplatine (Motherboard) verbunden.
2. **IPMI über LAN**
   Sie können das IPVO über eine LAN-Verbindung verbinden. Die Systemvoraussetzung für diesen Zugriffstyp ist ein Host-System mit IPMI v1.5 und ein Netzwerkadapter mit einer Side-Band-Verbindung zum Baseboard Management Controller (BMC) (oft eingebaut). Sie müssen bei den IPVO-Einstellungen die IP-Adresse dieses Host-Systems und das richtige Kennwort für die LAN-Verbindung eingeben. Sie können durch Eingabe der jeweiligen IP-Adressen auf andere IPVO-Systeme zugreifen.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:34:50 AM

Datum und Zeit

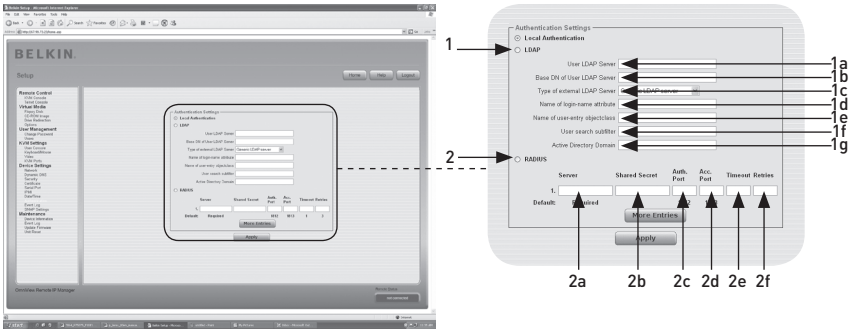


Diese Verknüpfung weist auf eine Seite hin, auf der die interne Echtzeit-Uhr des RIPM eingestellt werden kann. Sie können die Uhr manuell einstellen oder den Network Time Protocol (NTP)-Server benutzen. Ohne den Zeitserver wird Ihre Einstellung nicht dauerhaft sein, Sie müssen sie jedes Mal neu einstellen, wenn der RIPM für einige Minuten ohne Strom ist. Um dies zu vermeiden, können Sie den NTP Zeitserver benutzen, der die interne Uhr automatisch auf die aktuelle GMT-Zeit (CUT) einstellt. Da die NTP-Server-Zeit immer GMT ist, gibt es eine Einstellung die Ihnen erlaubt, ein statisches Offset einzustellen, um Ihre lokale Zeit zu erhalten.

Achtung: Es gibt zur Zeit keinen automatischen Weg für die Einstellung der Sommerzeit. Sie müssen die GMT zweimal jährlich, entsprechend der Regelung Ihres Landes, einstellen.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:34:51 AM

Authentication (Authentifizierung)



Der RIPM erlaubt Ihnen den Gebrauch der lokalen Authentifizierung oder die Speicherung der Informationen in einem Lightweight Directory Access Protocol (LDAP) oder auf einem “Remote Authentication Dial-In User Service Server” (RADIUS-Server). Für LDAP oder RADIUS müssen Sie einige Informationen im Bedienfeld der Authentifizierungs-Einstellungen angeben. Weitere Informationen über LDAP- und RADIUS-Einstellungen werden im Folgenden beschrieben.

1. LDAP

1a. User LDAP Server (Benutzer-LDAP-Server)
Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, auf dem die Nutzerdaten eingetragen sind. Wenn Sie anstelle eines Namens eine IP-Adresse auswählen, müssen Sie einen DNS-Server in den Netzwerkeinstellungen konfigurieren.

1b. Base DN of User LDAP Server (Basisname des Benutzer-LDAP-Servers)
Spezifizieren Sie unter “User LDAP Server” am Anfang des Verzeichnisstamms den entsprechenden Namen (DN).

1c. Type of External LDAP Server (Typ des externen LDAP-Servers)
Stellen Sie den Typ des externen LDAP-Servers ein. Dies ist notwendig, da einige Server-Typen eine besondere Vorgehensweise benötigen. Ergänzend werden die Standardwerte für das LDAP-Schema eingestellt. Sie können zwischen Generic LDAP Server, Novell Directory Service und Microsoft Active Directory wählen. Wenn Sie weder über Novell Directory Service noch über Microsoft Active Directory verfügen, dann wählen Sie Generic LDAP Server und bearbeiten Sie das LDAP-Schema (siehe unten).

1d. Name of Login-Name Attribute (Name des Attributs des Anmeldenamen)
Dies ist der Attributname, in dem der Anmeldename eines Nutzers enthalten ist. Für den Standardwert lassen Sie das Feld leer. Der Standardwert hängt von dem gewählten LDAP-Servertyp ab.

1e. Name of User-Entry Object Class (Name der Benutzer-Objektklasse)
Dies ist die Objektklasse, die einen Nutzer im LDAP-Verzeichnis identifiziert. Für den Standardwert lassen Sie das Feld leer. Der Standardwert hängt von dem gewählten LDAP-Servertyp ab.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:34:52 AM

1f. User Search Sub-Filter (Benutzer-Subfilter für die Suche)
Hier können Sie die Suche für Nutzer verfeinern, die dem RIPM bekannt sein sollten.

1g. Active Directory Domain (Aktive Verzeichnis-Domäne)
Diese Option bezeichnet die aktive Verzeichnis-Domäne, die im Microsoft Active Directory Server konfiguriert ist. Diese Option ist nur gültig, wenn Sie ein Microsoft Active Directory als LDAP-Servertyp gewählt haben.

2. Remote Authentication Dial In User Service (RADIUS) (
RADIUS ist ein Protokoll, das von der Arbeitsgruppe Internet Engineering Task Force (IETF) spezifiziert wurde. Es gibt zwei Spezifikationen für ein RADIUS-Protokoll: Authentifizierung und Accounting. Diese Spezifikationen sollen die Authentifizierung, Konfiguration und Kontoführung für DFÜ-Verbindungen zu einem unabhängigen Server zentralisieren. Das RADIUS-Protokoll gibt es in verschiedenen Ausführungen wie Free RADIUS, Open-RADIUS oder RADIUS auf UNIX-Systemen. Das RADIUS-Protokoll ist gut spezifiziert und getestet. Wir empfehlen alle genannten Produkte, besonders die Free RADIUS Version.

Hinweis: Verifizierung/Antwort wird zur Zeit nicht unterstützt. Eine “Access Challenge”-Antwort wird als “Access Reject” (Zugriffsverweigerung) bewertet.

Um über das RADIUS-Protokoll Zugriff auf ein entferntes Gerät zu bekommen, müssen Sie sich anmelden. Sie werden nach Ihrem Benutzernamen und Kennwort gefragt. Der RADIUS-Server wird die eingegebenen Daten (Authentifizierung) lesen und der RIPM wird Ihr Profil überprüfen (Autorisierung) Das Profil bestimmt (oder beschränkt) Ihre Handlungen und hängt von Ihrer jeweiligen Situation ab. Ist ein solches Profil nicht vorhanden, wird Ihr Zugriff über RADIUS abgelehnt. Hinsichtlich der Fernaktivitäten funktioniert die Anmeldung über RADIUS wie bei der Remote-Konsole. Wird eine halbe Stunde lang keine Aktivität erkannt, wird die Verbindung zum RIPM unterbrochen und beendet.

2a. Server
Geben Sie entweder die IP-Adresse oder den Host-Namen des RADIUS-Servers ein, mit dem eine Verbindung hergestellt werden soll. Wenn Sie den Host-Namen benutzen, muss DNS konfiguriert und aktiviert sein.

2b. Shared Secret
Ein “Shared Secret” ist eine Textzeichenfolge, die als Kennwort zwischen dem RADIUS-Client und dem RADIUS-Server dient. Der RIPM funktioniert als RADIUS-Client. Ein “Shared Secret” wird benutzt, um sicherzustellen, dass RADIUS-Nachrichten von einem RADIUS-aktivierten Gerät versendet wurden, das mit dem gleichen “Shared Secret” konfiguriert ist und um sicherzustellen, dass die RADIUS-Nachricht nicht im Transit modifiziert wurde (z. B. Sicherstellen der Nachrichtenintegrität). Sie können für das “Shared Secret” normale Buchstaben und/oder Ziffern verwenden. Ein “Shared Secret” kann aus maximal 128 Buchstaben bestehen und darf sowohl Klein- und Großbuchstaben (A–Z, a–z), Zahlen (0–9) und weitere Symbole (Zeichen, die nicht als Buchstaben oder Zahlen definiert sind), wie Ausrufungszeichen, (“! ”) oder Sternchen (“ * ”) enthalten.

2c. Authentication Port (Authentifizierungs-Port)
Der Port, mit dem der RADIUS-Server bei Authentifizierungsanfragen kommuniziert. Der Vorgabewert ist #1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:34:52 AM

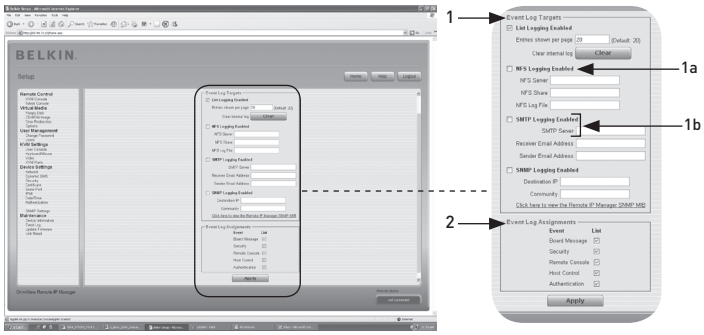
2d. Accounting-Port
Der Port, mit dem der RADIUS-Server bei Kontoanfragen kommuniziert. Der Vorgabewert ist #1813.

2e. Timeout (Zeitlimit)
Legt die Anfragezeit in Sekunden fest. Die Anfragezeit (time-to-live) ist die Zeit, die bis zum Abschluss der Anfrage gewartet werden muss. Wenn die angeforderte Aufgabe nicht in dieser Zeit erledigt ist, wird sie abgebrochen. Der Vorgabewert ist eine Sekunde.

2f. Retries (Wiederholungen)
Die Anzahl der erneuten Versuche, bis die Anfrage abgeschlossen ist. Der Vorgabewert beträgt drei.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:34:52 AM

Event Log (Ereignisprotokoll)



Wichtige Ereignisse, wie fehlgeschlagene Anmeldungen oder eine Firmware-Aktualisierung, werden in einem bestimmten Protokollbereich festgehalten (siehe Abb. 6-33). Jedes Ereignis gehört zu einer Ereignisgruppe, die einzeln aktiviert werden kann. Im Allgemeinen werden Ereignisse über die interne Protokollliste des RIPM notiert. Um das Protokoll zu öffnen, müssen Sie auf der Wartungsseite auf “Event Log” (Ereignisprotokoll) klicken. Sie können in den Protokolleinstellungen festlegen, wie lang die gezeigten Einträge pro Seite sein sollen. Sie können die Protokolldatei auch löschen.

1. **Event Log Targets (Protokollinhalt)**
   Um Ereignisse zu protokollieren, können Sie die interne Protokollliste des RIPM benutzen. Um die Protokollliste zu öffnen, müssen Sie auf der Wartungsseite auf “Event Log” (Ereignisprotokoll) klicken. Da der Systemspeicher des RIPM zum Speichen aller Daten verwendet wird, ist die maximale Anzahl von Protokolleinträgen auf 1000 Ereignisse beschränkt. Jeder weitere Eintrag überschreibt dann den ältesten Eintrag.

   Achtung: Wenn die Rücksetztaste am HTML Front-end für den Neustart des RIPM benutzt wird, wird die gesamte Protokollinformation dauerhaft gespeichert und nach dem Neustart des RIPM zur Verfügung stehen. Wenn der RIPM keinen Strom mehr hat oder wenn ein Neustart (Hard Reset) durchgeführt wird, gehen alle Protokolldaten verloren. Um dies zu vermeiden, verwenden Sie eine der nachfolgend beschriebenen Protokollmethoden.

   1a. Network File System (NFS) Logging Enabled (Network File System (NFS) Protokoll aktiv)
   Definieren Sie einen NFS-Server, zu dem Verzeichnisse und statische Links exportiert werden müssen; alle Protokolldaten werden dann in eine Datei in diesem Bereich notiert. Um Protokolldaten von mehreren RIPM-Geräten auf einen NFS-Server zu schreiben, müssen Sie für jedes Gerät jeweils einen Dateinamen definieren. Wenn Sie die NFS-Einstellungen ändern und auf die Schaltfläche “Apply” (Übernehmen) klicken, wird der NFS-Bereich sofort eingerichtet. Das bedeutet, dass der NFS-Anteil und der NFS-Server mit gültigen Quellen gefüllt werden müssen, da sonst eine Fehlermeldung angegeben wird.

   Hinweis: Im Gegensatz zur internen Protokolldatei des RIPM, ist die Größe der NFS-Protokolldatei nicht limitiert. Jedes Protokollereignis wird an das Ende einer Datei angehängt, so dass diese stetig wächst. Gelegentlich sollten Sie die Ereignisse in dieser Datei verschieben oder entfernen.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:34:53 AM

1b. SNMP Settings (SNMP-Einstellungen)

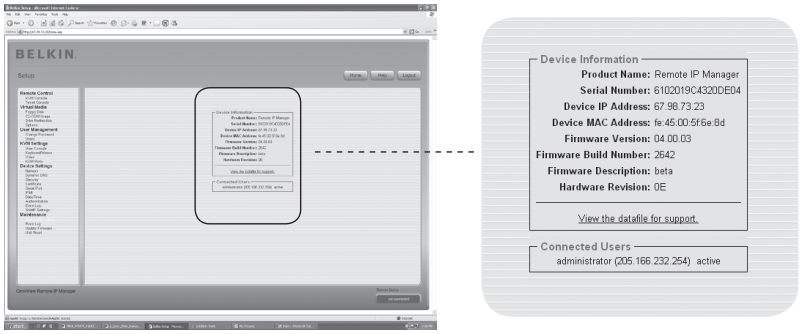
Simple Mail Transfer Protocol (SMTP) Logging Enabled (Simple Mail Transfer Protocol (SMTP) Protokoll aktiv)
Durch diese Option ist der RIPM in der Lage, E-Mails an die Adresse zu senden, die im E-Mail-Adressenfeld der Protokolleinstellungen eingegeben ist. Diese E-Mails beinhalten dieselben Beschreibungen wie die interne Protokolldatei; und der Inhalt der E-Mail beinhaltet die Ereignisgruppe des aufgetretenen Ereignisses. Um dieses Protokollziel zu nutzen, müssen Sie einen SMTP-Server angeben, der erreichbar ist und keine Authentifizierung benötigt (<serverip>:<port>).

SNMP Logging Enabled (SNMP Protokoll aktiv)
Wenn diese Einstellung aktiviert ist, sendet der RIPM immer dann eine SNMP-Trap-Meldung an eine IP-Adresse, wenn ein Protokollereignis auftritt. Wenn der Empfänger einen sogenannten “community string” (Gemeinschaftszeichenkette) benötigt, können Sie das entsprechende Feld markieren. Die meisten Trap-Ereignisse enthalten nur eine beschreibende Zeichenkette, die alle Daten über das Ereignis enthält. Die Authentifizierung und die Host-Stromversorgung haben ihre eigene Standard-Trap-Meldung, die sie automatisch erstellen und die etliche Felder mit Daten über das Ereignis enthält. Um diese SNMP-Trap-Meldung zu empfangen, verwenden Sie einen SNMP Trap-Empfänger.

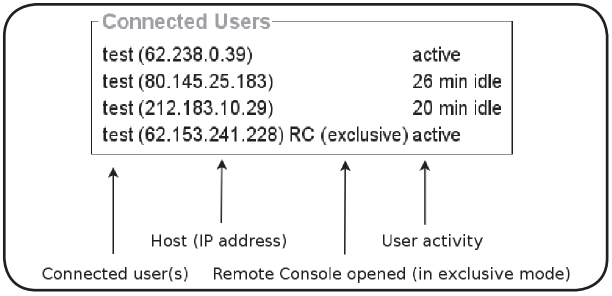
2. Event Log Assignments (Ereignisprotokoll-Zuweisungen)
Sie können auswählen, welche Ereignisse des RIPM in der Protokolldatei gespeichert werden. Markieren Sie die passenden Felder und klicken Sie auf “Apply” (Übernehmen), um die Auswahl zu bestätigen.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:34:53 AM

Device Information (Geräteinformationen)



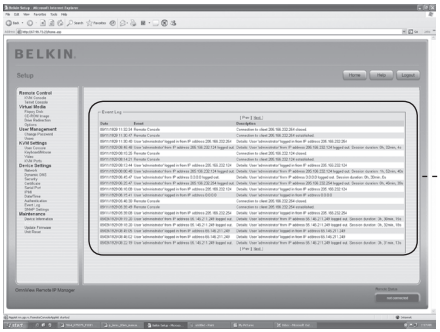
Im Folgenden erhalten Sie einen Überblick über den RIPM und seine aktuelle Firmware. Außerdem wird gezeigt, wie Sie den RIPM zurücksetzen. Die Datei erlaubt Ihnen den Download der RIPM-Datendatei mit spezifischen Support-Informationen. Dies ist eine erweiterbare Markup Language (XML)-Datei mit benutzerdefinierten Support-Informationen wie z. B. der Seriennummer.

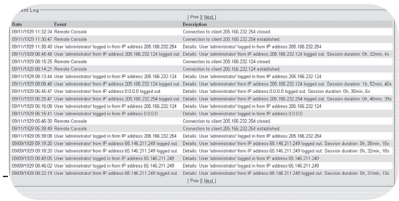


Die RIPM-Aktivität ist oben abgebildet. Die Abbildung zeigt von links nach rechts die verbundenen Nutzer, die Host-IP-Adresse des Nutzers und den Status der RIPM-Aktivität. “RC” bedeutet, dass die Remote-Konsole geöffnet ist. Wenn die Remote-Konsole im “Exclusive mode” (Alleinzugriffsmodus) geöffnet ist, wird der Begriff “Alleinzugriffsmodus” zugefügt. Weitere Informationen über diese Option finden Sie im Kapitel “Remote-Konsole-Kontrollleiste” auf Seite 23 dieses Handbuchs. Um die Benutzeraktivität anzuzeigen, enthält die letzte Spalte entweder den Begriff “active” (aktiv) für einen aktiven Benutzer oder “20 min idle” (20 Min. inaktiv), um anzuzeigen, welcher Benutzer für eine bestimmte Zeit inaktiv war.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:34:54 AM

Event Log (Ereignisprotokoll)

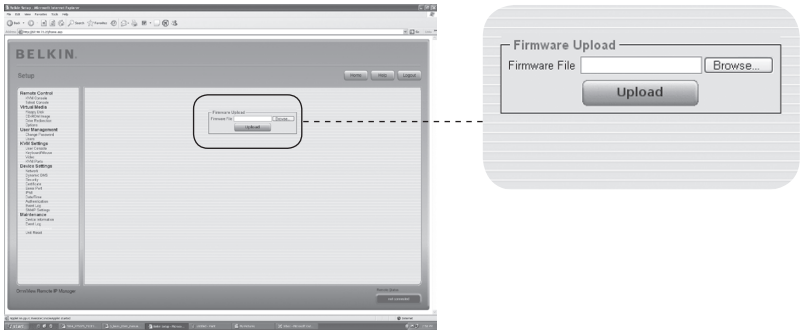




Die Ereignisprotokollliste enthält Ereignisse, die vom RIPM gespeichert werden, jeweils mit Ereignisdatum, einer kurzen Beschreibung und einer IP-Adresse, die die Herkunft des Ereignisses angibt. Sie können mit den Schaltflächen “Prev” (Zurück) und “Next” (Weiter) durch die Daten blättern.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:34:54 AM

Update Firmware (Aktualisieren der Firmware)



Der RIPM ist ein kompletter “Standalone-Computer” (Einzelrechner); er arbeitet mit Firmware, die direkt in seinem schreibgeschützten Speicher (ROM) geschrieben ist. Die Firmware des RIPM kann ferngesteuert monatlich aktualisiert werden, um die Funktionalität zu verbessern oder spezielle Funktionen zu installieren. Ein Firmware-Update ist eine Binärdatei, die von der Belkin Website heruntergeladen werden muss. Wenn die Firmware-Datei komprimiert ist, (z. B. wenn die Dateiendung .zip lautet), müssen Sie sie vor der Anwendung dekomprimieren. Bei Windows Betriebssystemen können Sie WinZip verwenden (im Internet auf http://www.winzip.com), um Ihre Firmware-Updates zu dekomprimieren.
Hinweis: Um die Firmware Ihres RIPM zu aktualisieren, müssen Sie die neue, dekomprimierte Firmware-Datei auf dem System speichern, das mit dem RIPM verbunden ist.

Die Aktualisierung der Firmware geschieht in drei Schritten:

1. Laden Sie die neue Firmware-Datei in den RIPM. Wählen Sie dazu die Datei auf Ihrem lokalen System aus und verwenden Sie im Bedienfeld “Upload Firmware” (Firmware hochladen) die Schaltfläche “Browse” (Durchsuchen). Klicken Sie dann auf “Upload” (Hochladen), um die zuvor ausgewählte Datei von Ihrem lokalen System auf den RIPM zu übertragen. Sobald die Firmware hochgeladen ist, wird der RIPM automatisch seine Gültigkeit überprüfen und bestätigen, dass keine Übertragungsfehler aufgetreten sind. Tritt ein Fehler auf, wird die Funktion “Upload Firmware” (Firmware hochladen) unterbrochen und die aktuelle Firmware bleibt intakt.
2. Wenn der Upload erfolgreich ist (wie es in der Regel der Fall sein dürfte), wird das Bedienfeld “Update Firmware” (Firmware aktualisieren) angezeigt werden. Das Bedienfeld wird die Versionsnummer der zur Zeit benutzten Firmware und die Versionsnummer der hochgeladenen Firmware anzeigen. Klicken Sie auf “Update” (Aktualisieren), um die alte Version gegen die neue Version auszutauschen.

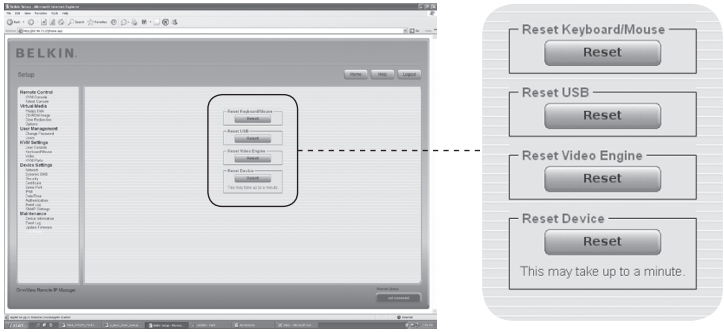
   Achtung: Dieser Vorgang ist unumkehrbar und wird einige Minuten dauern. Stellen Sie sicher, dass die Stromversorgung des RIPM während des Update-Vorgangs nicht unterbrochen wird; eine Stromunterbrechung könnte den RIPM instabil machen.

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:34:55 AM

3. Nach der Aktualisierung der Firmware wird der RIPM automatisch zurückgesetzt. Nach etwa einer Minute werden Sie erneut zur Anmeldeseite geleitet, um sich neu anzumelden.

   Achtung: Der 3-phasige Firmware-Aktualisierungsvorgang und die vollständige Konsistenz-Prüfung sorgen für die fehlerfreie Aktualisierung der Firmware. Allerdings sollten nur erfahrene Mitarbeiter oder Administratoren eine Firmware-Aktualisierung durchführen. Es ist wichtig, dass die Stromzufuhr des RIPM während des Aktualisierungsvorgangs NICHT unterbrochen wird.

Unit Reset (Zurücksetzen)



In diesem Abschnitt werden die Methoden beschrieben, mit denen man bestimmte Teile des Geräts zurückzusetzen kann. Dies beinhaltet Tastatur und Maus, die Bildschirmanzeige des mit dem RIPM verbundenen Computers und den RIPM selbst. Um die neue, aktualisierte Firmware zu aktivieren, müssen Sie den RIPM zurücksetzen. Dieser Vorgang beendet automatisch alle aktuellen Verbindungen mit der Verwaltungs-Konsole und dem RIPM und dauert etwa 30 Sekunden. Das Zurücksetzen der Teilgeräte (z. B. Grafik-Engine) dauert nur wenige Sekunden und unterbricht keine Verbindungen. Um einen spezifischen RIPM zurückzusetzen, klicken Sie auf die Schaltfläche “Reset” (Zurücksetzen), wie in der obigen Abbildung dargestellt.

Hinweis: Nur der Administrator darf den RIPM zurücksetzen.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:34:55 AM

Die Remote-Maus funktioniert nicht oder arbeitet nicht synchron.

Prüfen Sie zuerst die VGA-Verbindung. Sowohl der RIPM als auch der lokale Bildschirm müssen die gleiche Bildschirmauflösung unterstützen. Stellen Sie sicher, dass Ihre Maus-Einstellungen dem Maus-Modell entsprechen, z. B. PS/2 oder USB. Das Maus-Modell muss sowohl auf dem RIPM als auch auf dem Betriebssystem des Host (dem Computer, der an den RIPM angeschlossen ist) eingegeben sein. In einigen Fällen kann die Maussynchronisierung zu Fehlern führen. Bitte beachten Sie hierzu den Abschnitt “Maus-, Tastatur- und Grafik-Konfiguration” in Kapitel 3.

Die Bildqualität ist schlecht und/oder körnig.

Benutzen Sie den Menüeintrag “Reset” (Zurücksetzen), um den RIPM auf seine Vorgabewerte zurückzusetzen. Klicken Sie dann auf die Schaltfläche “Auto-Adjust” (Einstellautomatik), um einen passenden Grafikausgang auszuwählen. Stellen Sie sicher, dass die Bildschirmkabel sicher befestigt sind.

Die Anmeldung des RIPM schlägt fehl.

Überprüfen Sie Ihren Benutzernamen und Ihr Kennwort. Standardmäßig lautet der Benutzername “administrator” und das Kennwort ist “belkin”. Prüfen Sie, ob Ihr Browser Cookies akzeptiert.

Das Remote-Konsolen-Fenster des RIPM öffnet sich nicht.

Prüfen Sie, ob Java geladen wurde. Eine Firewall könnte den Zugriff auf die Remote-Konsole behindern. Die TCP-Ports #80 (für HTTP) und #443 (für HTTPS und RFB) müssen offen sein (der Server der Firewall muss eingehende TCP-Verbindungen auf diesen Ports akzeptieren).

Die Remote-Konsole kann keine Verbindung herstellen und zeigt einen Time-out-Fehler an.

Prüfen Sie das Setup Ihrer Hardware und Ihres Netzwerks. Wenn es einen Proxyserver zwischen dem RIPM und Ihrem Host gibt, können Sie eventuell keine Grafikdaten mit RFB übertragen. Erstellen Sie eine Verbindung zwischen dem RIPM und dem Client. Überprüfen Sie zusätzlich die Einstellungen des RIPM und wählen Sie für den RFB-Transfer einen anderen Server-Port aus. Wenn Sie eine Firewall benutzen, prüfen Sie den entsprechenden Port auf die Akzeptanz von Verbindungen. Sie können diese Verbindungen auf IP-Adressen beschränken, die von Ihrem RIPM und dem Client verwendet werden.

Zum RIPM kann keine Verbindung hergestellt werden.

Überprüfen Sie Ihre Hardware. Ist Ihr RIPM an das Stromnetz angeschlossen? Überprüfen Sie Ihre Netzwerkverbindung (IP-Adresse, Router). Schicken Sie eine “Ping”-Anfrage an den RIPM, um herauszufinden, ob der RIPM über das Netzwerk erreicht werden kann.

Spezielle Tastenkombinationen (z. B. ALT+F2, ALT+F3) werden vom Konsolensystem unterbrochen und können nicht an den Host übermittelt werden.

Definieren Sie einen sogenannten “Button key” (Tastaturbefehl). Dies geschieht über die Einstellungen der Remote-Konsole (siehe “Remote-Konsole-Kontrollleiste” auf Seite 23.)

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:34:56 AM

Die Internetseiten des RIPM werden nicht richtig angezeigt.

Prüfen Sie die Browser-Cache-Einstellungen. Stellen Sie vor allem sicher, dass die Option NICHT auf “Neuere Versionen der gespeicherten Seiten suchen” aktiviert ist. Bei dieser Einstellung könnten die RIPM-Seiten von Ihrem Browser-Cache und nicht vom RIPM geladen werden, was zu Problemen führen kann.

Windows XP startet nicht aus dem Standby-Modus.

Dies ist wahrscheinlich ein Windows XP Problem. Versuchen Sie den Mauszeiger ruhig zu halten, wenn XP in den Standby-Modus wechselt. Beachten Sie das Handbuch des Betriebssystems für weitere Informationen.

Immer wenn ich versuche, das Dialogfenster der Remote-Konsole zu öffnen, sind die Mauzeiger nicht mehr synchron.

Deaktivieren Sie die Einstellung “Automatically move mouse pointer to the default button of dialog boxes” (Mauszeiger automatisch auf Standardflächen der Dialogfelder bewegen) in den Maus-Einstellungen des Betriebssystems.

Die Remote-Konsole bleibt schwarz.

Prüfen Sie, ob der RIPM nur USB-versorgt ist. Wenn zu wenig Strom über USB vorhanden ist, öffnet sich die Remote-Konsole, bleibt aber schwarz. Überprüfen Sie die RIPM-Einstellungen auf Seite 26 dieses Handbuchs. Stellen Sie sicher, dass die Grafikkabel sicher befestigt sind.

Die Grafikdaten auf dem lokalen Bildschirm haben einen schwarzen Rand.

Dies ist kein Fehler. Der lokale Monitor ist auf einen bestimmten Grafikmodus programmiert, der in den Grafikeinstellungen des RIPM ausgewählt werden kann. Beachten Sie den Abschnitt “Remote-Konsole-Kontrollleiste” auf Seite 23 dieses Handbuchs.

Mir ist das Kennwort entfallen. Wie kann ich den RIPM auf die Werkseinstellung zurücksetzen?

Sie können die serielle Schnittstelle benutzen. Eine ausführliche Beschreibung finden Sie im Abschnitt
“Zurücksetzen des Remote IP-Managers auf Werkseinstellungen” auf Seite 31 dieses Handbuchs.

Unter www.belkin.com finden Sie weitere Problemlösungen und eine Auflistung der Hardware, die mit dem RIPM kompatibel ist.

Hinweis: Wenn keiner dieser Lösungsvorschläge erfolgreich ist, wenden Sie sich an den technischen Support von Belkin unter 1-800-2BELKIN.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:34:56 AM

FCC-Erklärung

Konformitätserklärung zur Einhaltung der FCC-Bestimmungen über elektromagnetische Kompatibilität

Wir, Belkin Corporation, eine Gesellschaft mit Sitz in 501 West Walnut Street, Compton, CA 90220, USA, erklären hiermit in alleiniger Verantwortung, dass dieses Produkt mit der Artikel Nr.
F1DE101H

auf den sich diese Erklärung bezieht, dem Abschnitt 15 der FCC-Bestimmungen entspricht. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Dieses Gerät darf schädigende Störungen nicht verursachen, und (2) dieses Gerät muss jedwede Störung annehmen, einschließlich der Störungen, die einen unerwünschten Betrieb verursachen könnten.

CE-Konformitätserklärung
Wir, Belkin Corporation, erklären hiermit in alleiniger Verantwortung, dass der Artikel F1DE101H, auf den sich diese Erklärung bezieht, in Einklang mit der Fachgrundnorm Störaussendung EN55022 und der Fachgrundnorm Störfestigkeit EN55024 sowie LVP EN61000-3-2 und EN61000-3-3 steht.

ICES-Erklärung
Dieses Digitalgerät der Klasse B entspricht der kanadischen Richtlinie ICES-003. Cet appareil numérique de la classe B est conforme á la norme NMB-003 du Canada.

Zwei Jahre eingeschränkte Herstellergarantie von Belkin Corporation

Garantieleistung.
Belkin Corporation garantiert dem ursprünglichen Käufer dieses Belkin-Produkts, dass dieses Produkt frei von Material-, Verarbeitungs-, und Konstruktionsfehlern ist.

Garantiedauer.
Belkin Corporation gewährt für dieses Belkin-Produkt eine zweijährige Garantie.

Problembehebung.
Produktgarantie.
Belkin wird das fehlerhafte Produkt nach eigenem Ermessen entweder kostenlos (abgesehen von den Versandkosten) reparieren oder austauschen.

Was wird durch diese Garantie nicht abgedeckt?
Alle oben genannten Garantien verlieren ihre Gültigkeit, wenn das Belkin-Produkt der Belkin Corporation auf Anfrage nicht auf Kosten des Käufers zur Überprüfung zur Verfügung gestellt wird oder wenn die Belkin Corporation feststellt, dass das Belkin-Produkt nicht unordnungsgemäß installiert worden ist, und dass unerlaubte Änderungen daran vorgenommen worden sind. Die Produktgarantie von Belkin gilt nicht für (Natur)gewalten (mit Ausnahme von Blitzeinschlägen) wie Überschwemmungen und Erdbeben sowie Krieg, Vandalismus, Diebstahl, normalen Verschleiß, Erosion, Wertminderung, Veralterung, schlechte Behandlung, Beschädigung durch Störungen aufgrund von Unterspannung (z. B. Spannungsabfall oder -Senkung) oder nicht erlaubte Programm- oder Systemänderungen.

Wie Sie Unterstützung bekommen.
Um Unterstützung von Belkin zu bekommen, befolgen Sie die folgenden Schritte:

1. Wenden Sie sich an die Belkin Corporation, 501 W. Walnut St., Compton CA 90220, Attn.: Customer Service oder wenden Sie sich innerhalb von 15 Tagen nach dem Vorfall telefonisch unter (800)-223-5546 an Belkin. Halten Sie die folgenden Informationen bereit:

   a. Die Artikelnummer des Belkin-Produkts.
   b. Wo Sie das Produkt erworben haben.
   c. Wann Sie das Produkt erworben haben.
   d. Eine Kopie der Originalquittung.

2. Die entsprechenden Mitarbeiter/innen informieren Sie darüber, wie Sie Ihre Rechnung und das Belkin-Produkt versenden müssen und wie Sie fortfahren müssen, um Ihre Ansprüche geltend zu machen.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:34:56 AM

Belkin Corporation behält sich vor, das beschädigte Belkin-Produkt zu überprüfen. Alle Kosten, die beim Versand des Belkin-Produkts an die Belkin Corporation zum Zweck der Überprüfung entstehen, sind vollständig durch den Käufer zu tragen. Wenn Belkin nach eigenem Ermessen entscheidet, dass es unpraktisch ist, das beschädigte Gerät an die Belkin Corporation zu schicken, kann Belkin nach eigenem Ermessen eine Reparaturstelle damit beauftragen, das Gerät zu überprüfen und einen Kostenvoranschlag für die Reparaturkosten des Gerätes zu machen. Die Kosten für den Versand zu einer solchen Reparaturstelle und die eventuellen Kosten für einen Kostenvoranschlag gehen vollständig zu Lasten des Käufers. Beschädigte Geräte müssen zur Überprüfung zur Verfügung stehen, bis das Reklamationsverfahren abgeschlossen ist. Wenn Ansprüche beglichen werden, behält sich die Belkin Corporation das Recht vor, Ersatzansprüche an eine bestehende Versicherung der Käuferin oder des Käufers
zu übertragen.

Garantiegesetze.
DIE GARANTIE IST DIE ALLEINIGE GARANTIE VON BELKIN. ES GIBT KEINE ANDERE GARANTIE, EXPLIZIT ERWÄHNT ODER IMLIZIT, AUSSER WENN DIES VOM GESETZ VORGESCHRIEBEN IST, EINSCHLIESSLICH DER IMPLIZITEN GARANTIE ODER DES QUALITÄTSZUSTANDS, DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, UND SOLCHE IMPLIZITEN GARANTIEN, WENN ES SOLCHE GIBT, BEZIEHEN SICH AUSSCHLIESSLICH AUF DIE DAUER, DIE IN DIESER GARANTIE ZUGRUNDEGELEGT WIRD.

In manchen Staaten sind Einschränkungen bezüglich der Dauer der Garantie nicht erlaubt. Die oben erwähnten Einschränkungen treffen für Sie dementsprechend nicht zu.

UNTER KEINEN UMSTÄNDEN HAFTET BELKIN CORPORATION FÜR ZUFÄLLIGEN, BESONDEREN, DIREKTEN, INDIREKTEN, MEHRFACHEN SCHADEN ODER FOLGESCHÄDEN WIE, ABER NICHT AUSSCHLIESSLICH, ENTGANGENES GESCHÄFT ODER PROFITE, DIE IHNEN DURCH DEN VERKAUF ODER DIE BENUTZUNG VON EINEM BELKIN-PRODUKT ENTGANGEN SIND, AUCH WENN SIE AUF DIE MÖGLICHKEIT SOLCHER BESCHÄDIGUNGEN AUFMERKSAM GEMACHT WORDEN SIND.

Diese Garantie räumt Ihnen spezifische Rechte ein, die von Land zu Land unterschiedlich ausgestaltet sein können. Da in manchen Ländern der Ausschluss oder die Beschränkung der Haftung für durch Zufall eingetretene oder Folgeschäden nicht zulässig ist, haben die vorstehenden Beschränkungen und Ausschlussregelungen für Sie möglicherweise keine Gültigkeit.

Produktentsorgung von Nutzern in privaten Haushalten in der Europäischen Union.
Dieses Symbol zeigt an, dass dieses Produkt nicht über den Hausmüll entsorgt werden darf. Stattdessen Sie sind verpflichtet, Ihren Abfall zu einem Sammelpunkt zu bringen, der für die Sammlung von wiederverwertbaren elektronischen Materialien und Geräten ausgewiesen ist. Die separate Sammlung und das Recyceln Ihrer alten Geräte zum Zeitpunkt Ihrer Entsorgung trägt zum Schutz der Umwelt bei und gewährleistet, dass sie auf eine Art und Weise recycelt werden, die keine Gefährdung für die Gesundheit des Menschen und der Umwelt darstellt. Weitere Informationen darüber, wo Sie alte Elektrogeräte zum Recyceln abgeben können, erhalten Sie bei den örtlichen Behörden, Wertstoffhöfen oder dort, wo Sie das Gerät erworben haben.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:34:56 AM

BELKIN®

OmniView®
Remote IP-Manager

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 Fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Großbritannien
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 Fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Niederlande
+31 (0) 20 654 7300
+31 (0) 20 654 7349 Fax

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spanien
+34 9 16 25 80 00
+34 9 02 02 00 34 Fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, Frankreich
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 Fax

Belkin GmbH
Hanebergstraße 2
80637 München, Deutschland
+49 (0) 89 143405 0
+49 (0) 89 143405 100 Fax

© 2006 Belkin Corporation. Alle Rechte vorbehalten. Alle Produktnamen sind eingetragene Marken der angegebenen Hersteller. Mac OS und Macintosh sind Marken der Apple Computer, Inc., eingetragen in den USA und anderen Ländern.

P75075ea

BELKIN

OmniView®
IP-manager voor beheer op afstand

Bediening

Bestuur overal ter wereld uw computer of KVM-switch via een webbrowser

EN
FR
DE
NL
ES
IT

Handleiding

F1DE101Hea

Inhoud

Inhoud

1-1 Inleiding en inhoud van de verpakking

Gefeliciteerd met en hartelijk dank voor uw aankoop van deze Belkin OmniView IP-manager voor beheer op afstand (RIPM). RIPM werd ontworpen om eenvoudig KVM-over-IP-technologie aan bestaande KVM- en serverconfiguraties toe te voegen en biedt een doeltreffende manier om stilstand van de server en onderhoudskosten drastisch te verlagen. Netwerkbeheerders kunnen sneller hulp bieden via onbeperkte toegang vanaf elke locatie.

De RIPM is eenvoudig te installeren binnen een klein of groot lokaal netwerk (LAN). In deze handleiding vindt u gedetailleerde informatie over de installatie en bediening van de RIPM en gespecialiseerde ondersteuning in geval van problemen. Wij stellen uw vertrouwen zeer op prijs en twijfelen er niet aan dat u snel zult begrijpen waarom er wereldwijd meer dan één miljoen Belkin OmniView-producten worden gebruikt.

OmniView® IP-manager voor beheer op afstand

PS/2 kabelset

VGA-kabel

DB9 Nullkabel

Mini-USB-kabel

Eén voedingsadapter (5V DC, 2A)

Rekmontagebeugel met schroeven

Cd met installatiesoftware

Handleiding

Verkorte Installatiehandleiding

Registratiekaart

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:35:01 AM

- **Externe toegang**
  De RIPM biedt externe toegang tot uw KVM-configuratie en alle aangesloten servers. Bovendien is de RIPM geschikt voor externe toegang tot afzonderlijke computers of servers.

- **Digitale gebruikers**
  Met de RIPM kan één digitale gebruiker toegang krijgen tot de aangesloten KVM-switches en servers en deze beheren. Bovendien kunnen 25 gebruikers tegelijkertijd digitale videobestanden bekijken om gezamenlijk problemen op te lossen.

- **Gebaseerd op webbrowser**
  De interface van de RIPM kan worden geopend via de webbrowser en kan dus worden bekeken met behulp van elke computer die is aangesloten op een LAN, WAN of op Internet via een standaard TCP/IP-verbinding. Voor de installatie is geen aanvullende software vereist.

- **Gebruikersvriendelijke interface**
  Dankzij de gebruikersvriendelijke interface kunt u de geavanceerde functies van de RIPM snel en eenvoudig instellen en wijzigen via uw webbrowser, zonder dat u extra software moet installeren.

- **Toegang op BIOS-niveau**
  Met de RIPM kunt u toegang krijgen tot het basissysteem voor input/output (BIOS) van uw servers om wijzigingen door te voeren en computers te herstarten.

- **Ondersteuning voor seriële apparaten**
  De RIPM biedt ondersteuning voor één serieel apparaat, zoals een power distribution unit (PDU, voedingseenheid), zodat u op afstand een koude herstart kunt uitvoeren van uw servers.

- **Betere beveiliging**
  De RIPM biedt 256-bit SSL encryptie en wachtwoordbeveiliging voor meerdere gebruikers om ongeautoriseerde toegang tot uw servers onmogelijk te maken.

- **Virtuele media***
  Met behulp van de virtuele-mediafunctie kunt u afbeeldingen en bestanden uitwisselen tussen lokale en externe computers, op afstand software laden, patches voor applicaties en besturingssysteem uitvoeren en diagnostische testen vanaf een cd starten.

*Uitsluitend beschikbaar voor computers met Windows®besturingssysteem.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:35:03 AM

- **Accountbeheer**
  Dankzij de RIPM kan de beheerder meerdere gebruikersaccounts aanmaken en de toegang tot de servers beheren.

- **Gebeurtenissenlogboek**
  In het gebeurtenissenlogboek worden alle activiteiten van de gebruikers binnen de RIPM opgeslagen.

- **Kennisgeving per e-mail**
  De RIPM stelt de beheerder in staat toezicht te houden op activiteiten van gebruikers d.m.v. het versturen van kennisgevingen per e-mail van aanmeldingen, ongeldige aanmeldingen en afmeldingen.

- **Ondersteuning van meerdere platforms**
  De RIPM is geschikt voor KVM-switches of servers met PS/2 of USB console-aansluitingen.

- **Videoresolutie**
  Met een bandbreedte van 117MHz ondersteunt de RIPM videoresoluties tot maximaal 1600x1200 bij 75 Hz.

- **Geschikt voor montage in 0U-rek**
  De RIPM is zo compact dat hij eenvoudig op uw computer of aan de achterkant van uw 0U-serverrek kan worden gemonteerd.

- **De firmware bijwerken**
  Dankzij flash-upgrades beschikt u steeds over de laatste firmware-updates voor uw RIPM. Deze firmware-updates zorgen ervoor dat de RIPM compatibel is met de laatste apparaten en hardware. Deze updates zijn gratis gedurende de levensduur van uw RIPM. Ga naar www.belkin.com voor informatie over upgrades en ondersteuning.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:35:03 AM

Vereiste hardware

- OmniView Series IP-manager voor beheer op afstand (meegeleverd)
- PS/2 kabelset (meegeleverd)
- VGA-kabel (meegeleverd)
- Mini-USB-kabel (meegeleverd)
- Voedingsadapter van 5V DC, 2A (meegeleverd)
- Toetsenbord, monitor en muis
- Verbinding met een netwerk via een 10/100Base-T Ethernet-poort (RJ45)
- CAT5-kabel
- Rekmontagebeugels met schroeven (meegeleverd voor eventuele installatie in een rek)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:35:03 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x en later;
UNIX®; Mac OS® X v10.0 en later (KVM vereist);
Sun™ Solaris™ 8.x en later (Met Sun-adapter—Belkin-artikelnummer. F1DE083)

Ondersteunde browsers

- Microsoft® Internet Explorer 6.0 en later
- Netscape® Navigator® 7.0

P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:35:03 AM

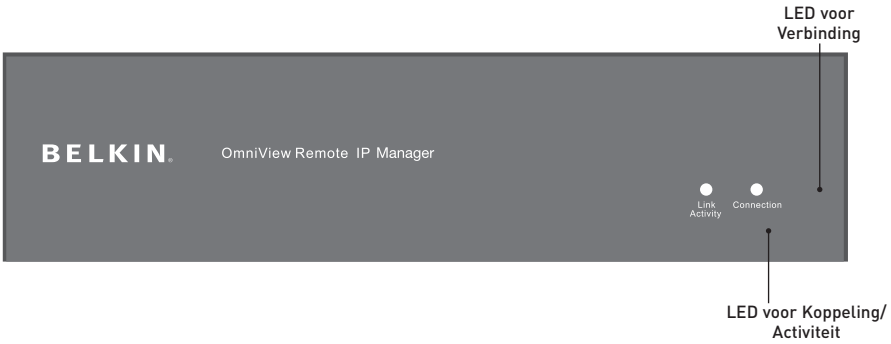
Artikelnummer:	F1DE101H
Voeding:	5V DC, 2A
Aantal ondersteunde gebruikers:	1 lokaal, 1 digitaal (1 gebruiker tegelijk)
Toetsenbordemulatie:	PS/2 en USB
Muisemulatie:	PS/2 en USB
Ondersteunde monitortypen:	CRT en LCD (met VGA-ondersteuning)
Ondersteunde resolutie:	Tot 1600x1200 bij 75 Hz
Maximale bandbreedte:	5MB
Toetsenbordingang	miniDIN6 (PS/2)
Muis-ingang:	miniDIN6 (PS/2)
Monitorpoort:	HDDB15 vrouwelijk (VGA)
CPU USB-poort:	Mini-USB
Netwerkverbinding:	RJ45
Encryptiemodi:	256-bit SSL, 128-bit, AES, DES, 3DES
authentificatie-ondersteuning:	LDAP (via lokale LDAP-client), RADIUS, AD
Ondersteunde protocollen:	SNMP v1, IPv4
Seriële apparaatpoort:	DB9
LED-indicatielampjes:	2
Behuizing:	Metaal
Afmetingen:	6,75 (B) x 1,75 (H) x 4,5 (L) in. (171 x 44 x 114mm)
Gewicht:	1,65 lbs. (0,75kg.)
Gebruikstemperatuur:	32° F tot 120° F (0° C tot 48,89° C)
Bewaartemperatuur:	-4° F tot 140° F (-20° C tot 60° C)
Vochtigheidsgraad:	5% to 80%
Garantie:	2 jaar

Let op:

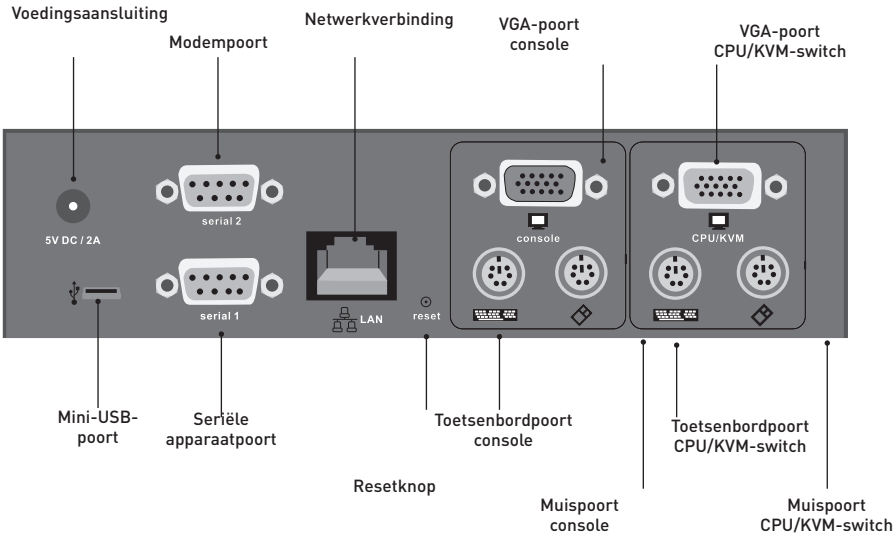
Specificaties kunnen zonder voorafgaande kennisgeving worden gewijzigd.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:35:03 AM

Voorkant van het apparaat

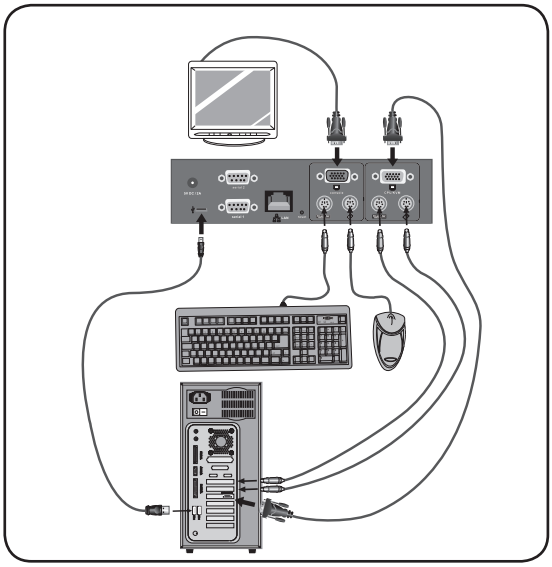


Achterkant van het apparaat

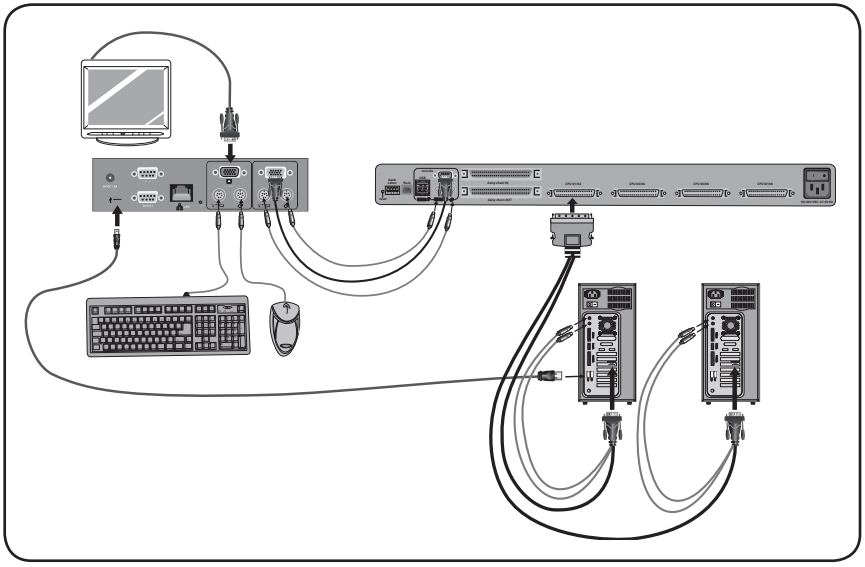


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:35:04 AM

Normale RIPM-configuratie voor computer



Normale RIPM-configuratie voor KVM-switch



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:35:07 AM

Stap 1 De RIPM in een serverrek installeren

De RIPM wordt geleverd met montagebeugels voor de installatie in een 19-inch rek.

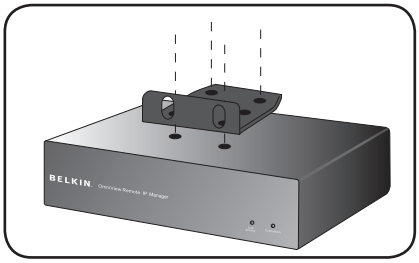


Fig. 1

1.1

Bevestig de beugel met de meegeleverde kruiskopschroeven aan de boven- of onderzijde van de RIPM.

1.2 Bevestig de RIPM in het rek. Zie **Afb. 1.**

Let op: Bevestigingsschroeven voor het rek zijn niet meegeleverd. Gebruik de schroeven die de leverancier van het rek voorschrijft.

Waarschuwing: Zorg ervoor dat de stroomvoorziening van alle betrokken computers en randapparatuur is uitgeschakeld voordat u apparaten aansluit op uw RIPM of computer(s). Als u dit nalaat is Belkin Corporation niet aansprakelijk voor de daardoor ontstane schade.

Stap 2 Uw console op de RIPM aansluiten

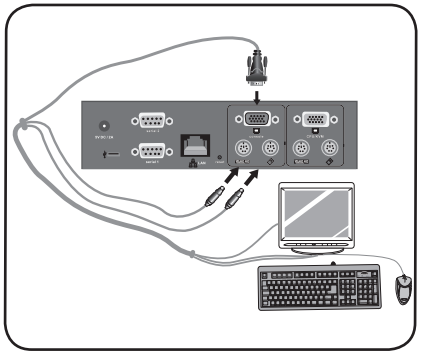


Fig. 2

2.1

Sluit uw toetsenbord en muis aan op de "Console"toetsenbord- en muispoorten van de RIPM.

2.2

Sluit uw monitor aan op de VGA-poort van de "Console" de RIPM.
Zie Afb. 2.

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:35:11 AM

Stap 3 | Optie 1: De RIPM aansluiten op een KVM-switch (Hostsysteem)

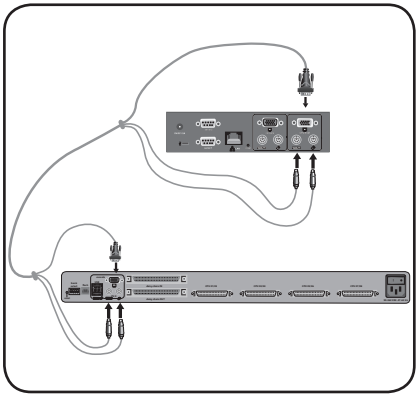


Fig. 3

3.1 Schakel de KVM-switch uit.

3.2 Gebruik de meegeleverde PS/2- en VGA-kabelset en sluit een uiteinde aan op de poorten voor “CPU/KVM switch”-monitor, toetsenbord en muis van de RIPM. Zie **afb. 3.**

3.3 Sluit het andere uiteinde aan op de monitor-, toetsenbord-, muispoorten van uw KVM-switch..

Stap 3 | Optie 2: De RIPM aansluiten op een computer (Hostsysteem)

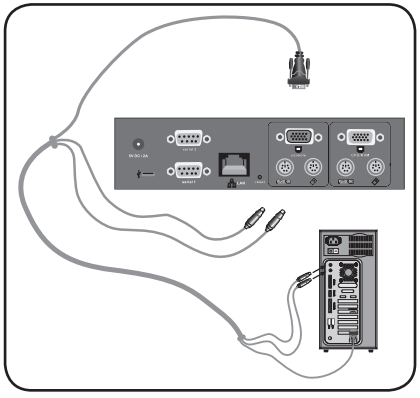


Fig. 4

3.1 Schakel de computer uit.

3.2 Gebruik de meegeleverde PS/2- en VGA-kabels en sluit een uiteinde aan op de poorten voor “CPU/KVM switch”-monitor, toetsenbord en muis van de RIPM. Zie **afb. 4.**

3.3 Sluit het andere uiteinde aan op de monitor-, toetsenbord-, muispoorten van uw computer.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:35:12 AM

Stap 4 | De mini-USB-kabel aansluiten voor ondersteuning van virtuele media

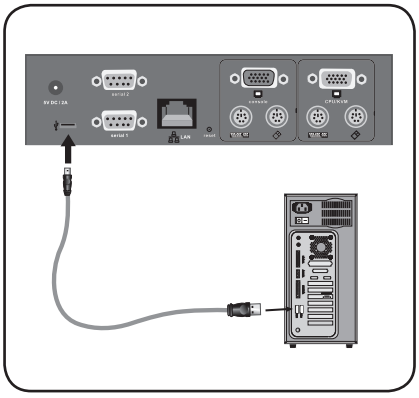


Fig. 5

4.1 Schakel de computer uit.

4.2 Sluit een uiteinde van de meegeleverde mini-USB-kabel aan op de mini-USB-poort van de RIPM en het andere uiteinde op een beschikbare USB-poort van uw computer. Zie **afb. 5.**

Opmerking: U kunt elke computer voorzien van het Windows besturingssysteem aansluiten op de RIPM voor ondersteuning van virtuele media. Hiervoor is het niet nodig dat de computer het hostsysteem is.

Let op: Als uw computer NIET is voorzien van Windows, hoeft u de hierboven beschreven installatie niet uit te voeren.

Stap 5 | De RIPM inschakelen

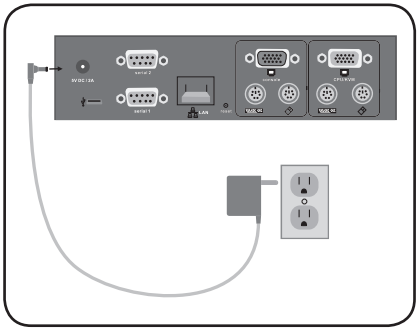


Fig 6

5.1 Sluit de meegeleverde netvoeding aan op een stopcontact.

5.2 Sluit de trommelstekker aan op de voedingsingang van de RIPM. Zie **afb. 6.**

5.3 Schakel uw KVM-switch of computer in.

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:35:14 AM

Er zijn twee manieren om uw RIPM in te stellen en te configureren. U kunt de meegeleverde installatie-cd van het apparaat gebruiken of een seriële interfacekabel op de RIPM aansluiten en de terminalsoftware (bijvoorbeeld HyperTerminal®) gebruiken.

Let op: Wij raden u aan de meegeleverde installatie-cd van het apparaat te gebruiken.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:35:15 AM

Installatie-cd van het apparaat

U kunt de software op de meegeleverde cd gebruiken om de RIPM te configureren binnen uw netwerk en externe toegang te krijgen.

1. Sluit de RIPM aan op uw computer via het lokale netwerk. Start de installatie vanaf de CD-ROM op de computer waarop de RIPM is aangesloten.
2. Volg de installatieprocedure om de RIPM te configureren. U hebt het IP-adres en gegevens over het subnet mask en gateway nodig voor toewijzing aan de RIPM. Deze gegevens kunt u opvragen bij uw netwerkbeheerder. Er verschijnt een melding zodra de configuratie is voltooid. Uw RIPM is nu geconfigureerd en de externe toegang is nu mogelijk.
3. De CD-ROM bevat ook software die nodig is voor de overdracht van bestanden tussen lokale computers en computers op afstand. Meer informatie hierover vindt u in het hoofdstuk “Virtuele media” van deze handleiding.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:35:15 AM

Er is een null-modemkabel (meegeleverd) vereist om de RIPM via de seriële interface te configureren. Sluit de null-modemkabel aan op de “Seriële 01”-poort van de RIPM en het andere uiteinde op de seriële poort van uw computer. U moet vervolgens de seriële interface aanpassen met de onderstaande parameters:

Parameter	**Waarde**
Bits/seconde	115200
Databits	8
Pariteit	neen
Stop bits	1
Flow-control	geen

Gebruik terminalsoftware (bijvoorbeeld HyperTerminal) om verbinding met de RIPM tot stand te brengen. Reset de RIPM en druk meteen op de “ESC”-toets. Er verschijnt een “=>” prompt. Voer de opdracht “config” in en druk op “ENTER”. U kunt nu de automatische IP-configuratie, het IP-adres, het subnetmasker en de standaard gateway aanpassen. Wanneer u op “ENTER” drukt zonder een waarde in te voeren,worden de instellingen niet gewijzigd. De gateway moet worden ingesteld op “0.0.0.0” (geen gateway) of elke andere waarde voor het IP-adres van de gateway. Nadat u hebt bevestigd, wordt de RIPM opnieuw opgestart met de nieuwe instellingen.

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:35:16 AM

Webinterface

De RIPM is toegankelijk via een standaard Java™-enabled webbrowser. U kunt het HTTP-protocol of een veilige, gecodeerde verbinding via HTTPS gebruiken. U hoeft enkel het ingestelde IP-adres van de RIPM in de adresbalk van uw browser in te voeren. De standaardinstellingen voor het inloggen zijn:

Parameter	Waarde
Inloggen	administrator (beheerder)
Wachtwoord	belkin

Wij raden u aan deze instellingen te wijzigen in gebruikersspecifieke waarden op de pagina Gebruikersbeheer.

Telnet

Met een standaard Telnet-client kunt u elk willekeurig apparaat openen dat via een RIPM op een van de seriële poorten van de externe IP-console is aangesloten.

De primaire interface van de RIPM is de http-interface. Als u gebruik wilt maken van het externe console-venster van uw managed hostsysteem, moet de browser zijn voorzien van een Java runtime-omgeving versie 1.1 of hoger. Als de browser geen Java ondersteunt(zoals het geval is bij een klein handheldapparaat), kunt u toch uw externe hostsysteem in stand houden met de beheersformulieren die door de browser zelf worden weergegeven.

Wij raden de volgende browsers aan voor onbeveiligde verbindingen met de RIPM:

- Microsoft Internet Explorer versie 5.0 of hoger op Windows 2000 en XP
- Netscape Navigator 7.0 op Windows 2000 en XP

Om toegang te krijgen tot het externe hostsysteem door middel van een veilig gecodeerde verbinding hebt u een browser nodig die het HTTPS-protocol ondersteunt. Een goede beveiliging is uitsluitend gewaarborgd bij het gebruik van een 128-bits sleutel.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:35:16 AM

3-1 Inloggen op de IP-manager voor beheer op afstand

Open uw webbrowser. Voer het adres van uw RIPM in dat u hebt geconfigureerd tijdens het installatieproces. U kunt hiervoor een IP-adres of een host- en domeinnaam gebruiken als u de RIPM een symbolic name in de Domain Name Server (DNS) hebt gegeven.

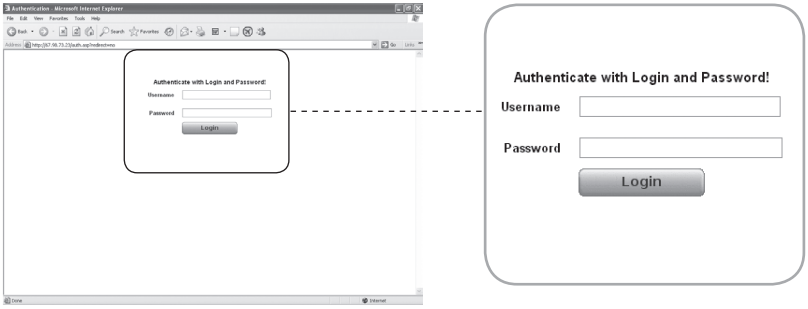
Toets bijvoorbeeld het volgende adres in op de adresregel van uw browser tijdens het maken van een onbeveiligde verbinding:

http://192.168.1.22/

Wanneer u een beveiligde verbinding maakt, voert u het volgende adres in:

http://192.168.1.22/

Hierna wordt de hieronder weergegeven RIPM-inlogpagina geopend:



De RIPM is voorzien van een ingebouwde beheerdersaccount met alle toegangsrechten om uw RIPM te beheren.

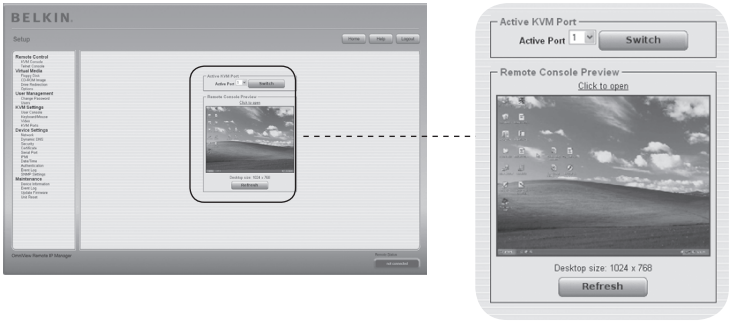
Parameter	Waarde
Inloggen	administrator (beheerder)
Wachtwoord	belkin

Opmerking: Uw webbrowser moet zo zijn ingesteld dat cookies worden geaccepteerd; zoniet, dan is inloggen niet mogelijk.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:35:16 AM

3-2 Interface voor IP-manager voor beheer op afstand

De externe console is het doorgestuurde scherm, toetsenbord en de dito muis van het externe hostsysteem waarbinnen de RIPM is geïnstalleerd. De webbrowser waarmee de RIPM wordt geopend moet een Java runtime-omgeving van versie 1.1 of hoger bieden. Wij raden u echter aan Sun JVM (Java Virtual Machine) 1.4 te installeren. De weergave van de externe console is exact hetzelfde als die van uw externe systeem. U kunt het toetsenbord en de muis op dezelfde manier gebruiken. Open de externe console door het voorbeeld op de hoofdpagina van de HTML front-end te selecteren.



Enkele van de beschikbare menu-opties zijn:

"Automatisch instellen"-knop

Druk op deze knop en wacht enkele seconden zodat de RIPM op de best mogelijke videokwaliteit kan worden ingesteld als videoweergave van slechte kwaliteit of vervormd is.

Sync-muis

Door deze optie te kiezen synchroniseert u de lokale met de externe muiscursor. Deze optie is vooral nodig wanneer u versnelde muisinstellingen op het hostsysteem gebruikt.

Video-instellingen in het menu Opties

Hiermee opent u een nieuw venster met elementen waarmee u de video-instellingen van de RIPM kunt besturen. Om de videokwaliteit te verbeteren kunt u bepaalde waarden wijzigen voor helderheid en contrast van het weergegeven beeld. Het is ook mogelijk alle videomodi of alleen de huidige modus terug te zetten naar de standaard-instellingen.

Let op: Druk eenmaal op de knop "Auto-Adjust" (Automatisch instellen) wanneer u het apparaat voor het eerst opstart en de lokale muisaanwijzer niet met de externe muisaanwijzer is gesynchroniseerd.

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:35:17 AM

Er zijn twee interfaces beschikbaar voor het verzenden van toetsenbord- en muisgegevens tussen de RIPM en de host: USB en PS/2 (apart verkrijgbaar). De correcte bediening van de externe muis hangt af van diverse instellingen. Deze instellingen worden in de volgende subhoofdstukken besproken.

USB-interface voor IP-manager voor beheer op afstand

Het is van belang dat u de juiste kabels gebruikt tussen de managed host en het managing device voor het gebruik van de USB-interface. Als de managed host bijvoorbeeld geen ondersteuning biedt voor USB-toetsenborden in de BIOS en u uitsluitend de USB-kabel hebt aangesloten, hebt u geen externe toegang met het toetsenbord tijdens het opstartproces van de host. Raadpleeg het hoofdstuk “Toetsenbord/muis” op pagina 48.

Toetsenbordinstellingen voor IP-manager voor beheer op afstand

Het toetsenbord voor de host moet correct zijn ingesteld in de RIPM om het toetsenbord correct te laten functioneren. Controleer de instellingen in de front-end van de RIPM. Raadpleeg het hoofdstuk “Toetsenbord/muis” op pagina 48.

Instellingen voor externe muis

Een bekend probleem met KVM-apparaten is de synchronisatie tussen de lokale en de externe muiscursors. In de RIPM wordt hiervoor een intelligent synchronisatie-algoritme gebruikt. Er zijn drie muismodi beschikbaar in de RIPM.

•
Automatische muissnelheid

Met de automatische muissnelheid wordt er geprobeerd de instellingen voor snelheid en versnelling van het hostsysteem automatisch te detecteren. Raadpleeg het hoofdstuk hierna voor meer informatie.

- **Vaste muissnelheid**

In deze modus worden de muisbewegingen vanaf de externe console zo geïnterpreteerd dat de beweging met één pixel leidt tot pixelbewegingen op het externe systeem. Deze parameter kunt u aanpassen met behulp van de functie Schaling. NB: deze functie werkt uitsluitend wanneer de muisversnelling op het externe systeem is uitgeschakeld.

- **Directe en indirecte muismodi**

Deze modus wordt beschreven in het hoofdstuk “Directe en indirecte muismodi” op pagina 20.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:35:17 AM

Automatische muissnelheid en muis synchroniseren

De modus voor automatische muissnelheid zorgt ervoor dat de snelheid tijdens het synchroniseren van de muis wordt gedetecteerd. Er zijn twee manieren om de lokale en externe muis opnieuw te synchroniseren als de muisbewegingen niet correct zijn.

- **Snelle synchronisatie**
  De snelle synchronisatie wordt gebruikt om een tijdelijke maar vaste verdraaiing te corrigeren. U kunt deze optie kiezen vanuit het menu Opties van de externe console. U kunt ook op de sneltoetscombinatie (als deze is gedefinieerd) voor muissynchronisatie drukken (raadpleeg het hoofdstuk “ Stuurbalk van de externe console” op pagina 23).

- **Intelligente synchronisatie**

Gebruik de intelligente synchronisatie als de snelle synchronisatie niet werkt of als de muisinstellingen op het hostsysteem zijn gewijzigd. Met deze methode worden de parameters voor de werkelijke beweging van de muisaanwijzer zodanig aangepast dat de muisaanwijzer op de juiste positie op het scherm wordt weergegeven. Deze methode neemt meer tijd in beslag dan de snelle synchronisatie en u kunt hem openen met het betreffende item in het menu Opties van de externe console. Intelligente synchronisatie vereist een correct ingesteld beeld. U kunt het beeld met de functie voor automatische beeldregeling aanpassen of in het video-instelscherm handmatig corrigeren. De vorm van de muisaanwijzer is van groot belang tijdens de detectie van de muisaanwijzer. Wij raden u aan een eenvoudige, maar veel voorkomende vorm van de muisaanwijzer te gebruiken. Detectie en synchronisatie van muisaanwijzers met animatie mislukt in de meeste gevallen. In het algemeen kunnen bewegende muisaanwijzers bijna niet worden verzonden als videoafbeelding tijdens het detectieproces van de muisaanwijzer. Het gebruik van een standaardmuisaanwijzer zorgt ervoor dat het detectieproces soepel verloopt en de synchronisatie optimaal is.

Het drukken op de “Mouse” (Muis) knop bovenaan de externe console kan, afhankelijk van de huidige status van de muissynchronisatie, verschillende resultaten hebben.Normaal gesproken opent deze knop de snelle synchronisatie, behalve in de gevallen waarbij de videomodus recentelijk is gewijzigd. Raadpleeg ook het hoofdstuk “Stuurbalk van de externe console” op pagina 23.

Opmerking: Druk eenmaal op de knop “Auto-Adjust” (Automatisch instellen) wanneer u het apparaat voor het eerst opstart en de lokale muisaanwijzer niet met de externe muisaanwijzer is gesynchroniseerd.

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:35:17 AM

Muisinstellingen voor hostsysteem

Het besturingssysteem van de host bevat diverse instellingen voor het muisstuurprogramma.

De RIPM werkt met versnelde muizen en kan lokale muisaanwijzers synchroniseren met externe muisaanwijzers. De volgende beperkingen kunnen deze synchronisatie in de weg staan:

- **Speciaal muisstuurprogramma**

Er zijn muisstuurprogramma's die de synchronisatieprocedure beïnvloeden waardoor de muisaanwijzers ontregeld worden. Zorg ervoor dat u geen muisstuurprogramma's op uw hostsysteem gebruikt die specifiek voor een bepaald type muis zijn ontwikkeld als dit gebeurt.

- **Muisinstellingen voor Windows 2003 Server/XP**
  Windows XP bevat de instelling "muisversnelling verbeteren". Zorg ervoor dat deze is uitgeschakeld.

- **Actieve desktop**
  Gebruik geen vlakke achtergrond als de "Actieve desktop" van Microsoft Windows is ingeschakeld. Gebruik in plaats daarvan een bureaublad-achtergrond (wallpaper). U kunt de Actieve Desktop ook helemaal uitschakelen.

Ga met uw muisaanwijzer naar de linkerbovenhoek van het scherm van de applet en verplaats deze heen en weer. Hierdoor zal de muis opnieuw worden gesynchroniseerd. Schakel de muisversnelling uit en herhaal deze procedure als de synchronisatie niet lukt.

- **Directe en indirecte muismodi**
  De bovenstaande informatie is van toepassing op indirecte muismodi waarbij de externe en lokale muisaanwijzers zichtbaar zijn en moeten worden gesynchroniseerd. De RIPM is voorzien van een andere modus, de directe muismodus, waarbij uitsluitend de externe muisaanwijzer zichtbaar is. Schakel deze modus in de externe console in (raadpleeg het hoofdstuk "Stuurbalk van de externe console" op pagina 23 en klik in het schermgebied. De lokale muisaanwijzer is verborgen en de externe muisaanwijzer kan rechtstreeks worden bestuurd. Om deze modus te verlaten moet u een sneltoets voor de muis bepalen in het scherm Instellingen voor externe console. Druk op deze toets om de vastgelegde lokale muisaanwijzer vrij te geven.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:35:17 AM

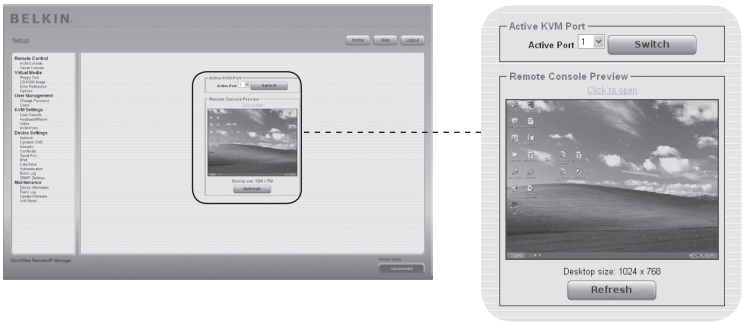
Aanbevolen muisinstellingen

Windows 2000, 2003, XP (alle versies)	In het algemeen raden wij u aan een USB-muis te gebruiken. Kies USB zonder muissynchronisatie.
Mac® OS X:	Wij raden u aan de directe muismodus te gebruiken.
Sun Solaris	Pas de muisinstellingen aan via “xset m 1” of door CDE-configuratiescherm te gebruiken om de muis in te stellen op “1:1, geen versnelling”. Als alternatief kunt u ook de directe muismodus gebruiken.
Linux	Kies allereerst de optie “Andere besturingssystemen” uit het selectievakje “Muistype”. Kies vervolgens de optie “Automatische muissnelheid”. Deze instelling is van toepassing op zowel USB- als PS/2-muizen

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:35:17 AM

Navigatie

Nadat u in de RIPM hebt ingelogd, verschijnt de hoofdpagina van de RIPM. Deze pagina bevat drie onderdelen met specifieke gegevens. Met de knoppen bovenaan het scherm kunt u binnen de front-end navigeren (raadpleeg de tabel voor meer informatie). Het kader links onderaan bevat een navigatiebalk waarmee u kunt schakelen tussen de verschillende onderdelen van de RIPM. Taakspecifieke informatie, die verschilt afhankelijk van het onderdeel dat u hebt gekozen, wordt in het kader rechts weergegeven.



Let op: Als er gedurende 30 minuten geen activiteit plaatsvindt, zal de RIPM automatisch uitloggen. Als u klikt op een van de koppelingen keert u terug naar het inlogscherm.

P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:35:18 AM

Het bovengedeelte van het scherm Externe console bevat een stuurbalk. Door de onderdelen hiervan te gebruiken, kunt u de status van de externe console bekijken en de instellingen van de lokale externe console wijzigen. Hieronder volgt een beschrijving van elke besturing.

- **"Automatisch instellen"-knop**

Druk op deze knop en wacht enkele seconden zodat de RIPM op de best mogelijke videokwaliteit kan worden ingesteld indien de videoweergave van slechte kwaliteit of vervormd is.

- **Sync-muis**

Door deze optie te kiezen synchroniseert u de lokale met de externe muiscursor. Deze optie is vooral belangrijk wanneer u versnelde muisinstellingen op het hostsysteem gebruikt. In het algemeen hoeft u de muisinstellingen niet te wijzigen.

- **Directe en indirecte muismodi**

Kies deze modus om te schakelen tussen de directe muismodus (waarbij uitsluitend de externe muisaanwijzer zichtbaar is) en de indirecte muismodus (waarbij zowel de externe als de lokale muisaanwijzers zichtbaar zijn en moeten worden gesynchroniseerd). De directe muismodus is uitsluitend beschikbaar als u Sun JVM 1.4 of hoger gebruikt.

- **Opties**

Klik op de knop "Options" (Opties) om het optiesmenu te openen.

Hieronder volgt een korte beschrijving van de beschikbare opties:

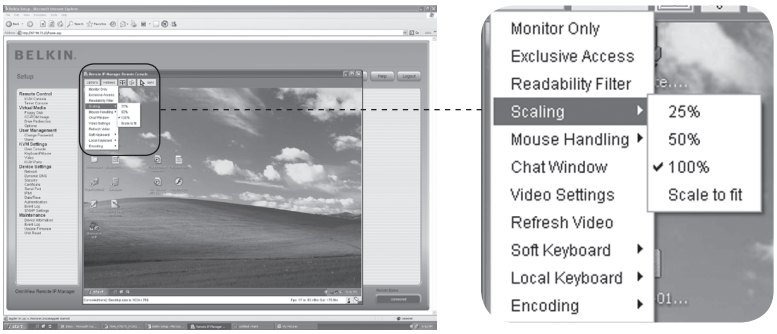
- **Uitsluitend monitor**
  Hiermee schakelt u de optie "Uitsluitend monitor" in of uit. Als deze optie is ingeschakeld, is er wel toezicht maar geen externe console-interactie mogelijk.

- **Exclusieve toegang**
  Met de juiste toegangsrechten kunt u de externe consoles van alle andere gebruikers sluiten. Niemand kan de externe console tegelijkertijd openen totdat u de exclusieve toegang uitschakelt of uitlogt.

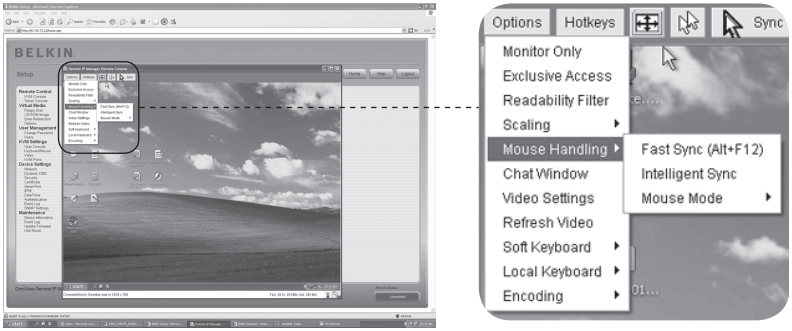
P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:35:18 AM

- **Scaling (Schaling)**

Hiermee kunt het formaat van externe console verkleinen. U kunt de muis en het toetsenbord blijven gebruiken, maar het scaling algoritme bewaart niet meer alle weergavedetails.



- **Mouse Handling (Muisbesturing)**
  In het submenu voor muisbesturing vindt u twee opties voor het synchroniseren van de lokale en externe muisaanwijzers zoals beschreven in het hoofdstuk “Muis, toetsenbord en video-configuratie”.



- **Fast Sync (snelle sync)**
  De snelle synchronisatie wordt gebruikt om een tijdelijke maar vaste verdraaiing te corrigeren.

- **Intelligente synchronisatie**
  Gebruik deze optie als de snelle synchronisatie niet werkt of als de muisinstellingen op het hostsysteem zijn gewijzigd.

Waarschuwing: Deze methode duurt langer dan de snelle synchronisatie en vereist een correct ingesteld beeld. U kunt het beeld aanpassen met de functie voor automatische beeldregeling of handmatig aanpassen in het video-instelscherm.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:35:19 AM

- **Lokale cursor**

  Deze functie biedt een lijst met beschikbare muisaanwijzersvormen voor de lokale muisaanwijzer. De geselecteerde vorm wordt voor de huidige gebruiker opgeslagen en ingeschakeld de volgende keer dat deze gebruiker de externe console opent. Het aantal beschikbare vormen is afhankelijk van de Java Virtual Machine (JVM). De versies 1.2 en hoger bieden de volledige lijst.

- **Video-instellingen**

  Hiermee opent u een scherm waarin u de video-instellingen van de RIPM kunt wijzigen. De RIPM bevat twee aparte dialoogvensters waarmee de video-instellingen kunnen worden ingesteld.

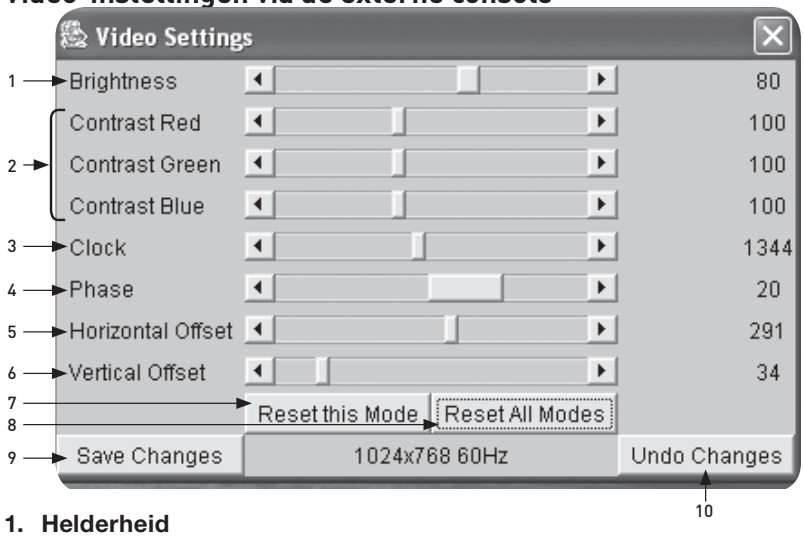
- **Video instellen via de HTML front-end**

  Selecteer deze optie om de lokale videopoort in te schakelen. Met deze optie bepaalt u of de lokale video-uitgang van de RIPM is ingeschakeld en via het binnenkomende signaal van het hostsysteem wordt doorgegeven.

Met de optie “Ruisfilter” bepaalt u op welke manier de RIPM reageert op kleine wijzigingen in het binnenkomende videosignaal. Een ruime instelling voor de filter heeft minder netwerkverkeer en een snellere videoweergave tot gevolg, maar het kan zijn dat kleine wijzigingen in delen van de display niet meteen worden herkend. Met een smalle instelling voor de filter worden alle wijzigingen meteen weergegeven, maar kan leiden tot een constante stroom netwerkverkeer, zelfs wanneer er geen wijzigingen op het beeldscherm plaatsvinden (afhankelijk van de kwaliteit van het binnenkomende videosignaal). De standaardinstelling is geschikt voor de meest gangbare omgevingen.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:35:19 AM

Video-instellingen via de externe console



1. **Helderheid**
   Hiermee stelt u de helderheid van het beeld in.
2. **Contrast**
   Hiermee stelt u de scherpte van het contrast van het beeld in.
3. **Klok**
   Hiermee bepaalt u de horizontale frequentie van een videolijn en is afhankelijk van de videomodus. Het kan zijn dat hier, afhankelijk van het type videokaart, verschillende waarden moeten worden ingevoerd. De standaardinstellingen in combinatie met de procedure voor automatische beeldregeling is geschikt voor meest gangbare configuraties. U kunt proberen om deze instelling, samen met de sample-fase, te wijzigen om een betere beeldkwaliteit te krijgen.
4. **Fase**
   Hiermee bepaalt u de fase voor videosamples die worden gebruikt om de kwaliteit van de weergave samen met de instelling voor de sampleklok te besturen.
5. **Horizontale afwijking**
   Als u deze optie selecteert, kunt u het beeld met de linkse en rechtse knoppen in horizontale richting verschuiven.
6. **Verticale afwijking**
   Als u deze optie selecteert, kunt u het beeld met de linkse en rechtse knoppen in verticale richting verschuiven.
7. **Deze modus resetten**
   Hiermee zet u de specifieke instellingen van deze modus terug naar de fabrieksinstellingen.
8. **Alle modi resetten**
   Hiermee zet u alle modus-afhankelijke instellingen terug naar de fabrieksinstellingen.
9. **Wijzigingen opslaan**
   Hiermee slaat u de wijzigingen permanent op.
10. **Wijzigingen ongedaan maken**
    Herstelt de laatste instellingen.

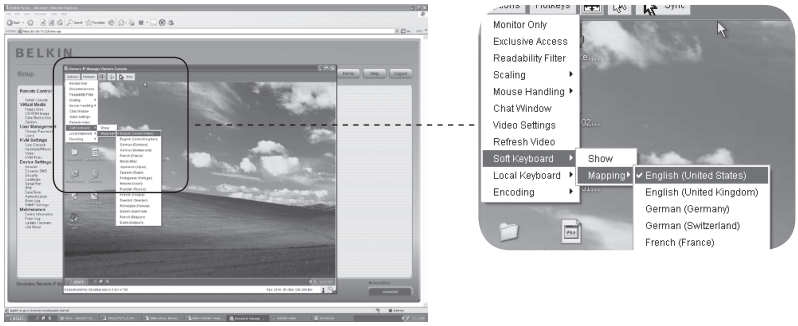
P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:35:20 AM

Volgorde voor mapping

Zacht toetsenbord
Hiermee opent u het menu voor het zachte toetsenbord.

Weergeven
Hiermee opent u het zachte toetsenbord. Het zachte toetsenbord is van belang wanneer er op uw hostsysteem een volledig andere taal en landmapping is ingesteld dan op het beheersysteem.

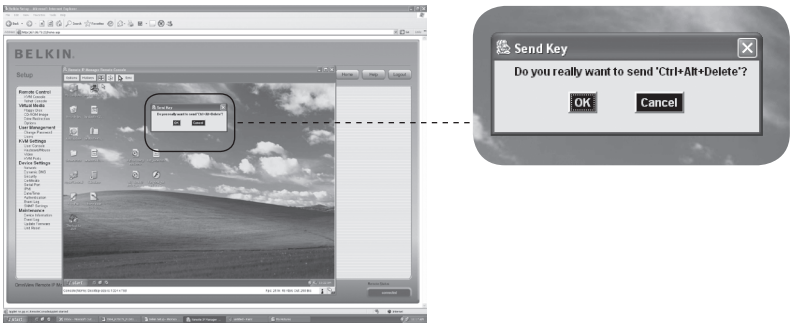
Mapping
Hiermee kunt u de juiste taal-en landmapping van het zachte toetsenbord kiezen.



P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:35:20 AM

Lokaal toetsenbord
Hiermee kunt u de taalmapping van uw browsermachine waarop de externe console-applet draait wijzigen. Normaal gesproken bepaalt deze applet automatisch de juiste waarde. Afhankelijk van uw JVM- en browserinstellingen is dit echter niet altijd mogelijk. Een goed voorbeeld hiervan is een Duits gelokaliseerd systeem waarbij een US-English toetsenbordmapping wordt gebruikt. In een dergelijk geval moet u handmatig de lokale toetsenbordinstellingen voor de juiste taal aanpassen.

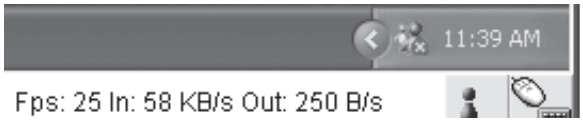
Sneltoetsen
Hiermee opent u een lijst met voorgedefinieerde sneltoetsen. Kies een invoer en de opdracht zal vervolgens naar het hostsysteem worden verzonden. U kunt een dialoogvenster voor bevestiging toevoegen die wordt weergegeven voordat de geselecteerde opdracht wordt verzonden naar de externe host. Selecteer “OK” om de opdracht uit te voeren op de externe host.



P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:35:21 AM

Op de statusregel worden zowel de externe console als de status van de verbinding weergegeven. Het externe beeldschermformaat wordt linksboven weergegeven. De waarde tussen haakjes geeft de verbinding met de externe console weer. “Norm” staat voor standaardverbinding zonder encryptie; “SSL” staat voor een beveiligde verbinding via SSL.

Zowel het inkomende (“In:”) als het uitgaande (“Out:”) netwerkverkeer wordt in kilobytes per seconde weergegeven. Een waarde tussen haakjes geeft de gecomprimeerde overdrachtsnelheid weer als gecomprimeerde codering is ingeschakeld.



De onderstaande knop geeft de toegangsinstellingen van de externe console weer.

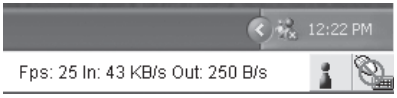
Eén of meerdere gebruikers zijn verbonden met de externe console van de RIPM.

Er is exclusieve toegang voor u ingesteld. Geen enkele andere gebruiker kan de externe host via de externe console openen, tenzij u deze optie uitschakelt.

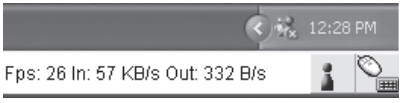
P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:35:21 AM

Een externe gebruiker heeft exclusieve toegang. U hebt geen toegang tot de externe host via de externe console, tenzij de andere gebruiker deze optie uitschakelt.

De meest rechtse knop geeft de status van de instellingen voor “Uitsluitend monitor” weer.



De optie “Uitsluitend monitor” is uitgeschakeld.



De optie “Uitsluitend monitor” is ingeschakeld.

Raadpleeg het hoofdstuk “Stuurbalk van de externe console” op pagina 23 van deze handleiding voor meer informatie over de functie Uitsluitend monitor en de instellingen voor exclusieve toegang.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:35:22 AM

Fabrieksinstellingen voor IP-manager voor beheer op afstand resetten

Volg de onderstaande procedure om de RIPM te resetten en de netwerkinstellingen terug te zetten naar de fabriekinstellingen:

1. Maak een seriële verbinding voor de initiële configuratie (HyperTerminal)

Bits per seconde:	115200
Databits:	8
Pariteit:	geen
Stop bits:	1
Flow-control:	hardware of geen

2. Druk op de resetknop die zich bevindt tussen de ingang van de gelijkstroomvoeding en de netwerkaansluiting. Laat de resetknop los en druk in het seriële terminalprogramma (HyperTerminal) onmiddellijk meerdere malen op ESC totdat de "=>"-prompt verschijnt.

Let op: Herhaal de stappen 1 en 2 als de prompt niet drie seconden nadat u de resetknop hebt losgelaten verschijnt. De RIPM detecteert de ESC-toets uitsluitend gedurende de eerste drie seconden van het opstartproces.

3. Typ "defaults" en druk op enter als er een opdrachtscherm verschijnt. De RIPM wordt opnieuw opgestart en de fabriekinstellingen worden hersteld.
4. Schakel uw server uit (de computer die lokaal aan de RIPM is verbonden).
5. Haal de stekker uit de RIPM en de poortkabels en netwerkkabel uit de "CPU/ KVM-switch".
6. Sluit de kabels opnieuw aan en start de server op.

U kunt nu uw RIPM opnieuw configureren volgens uw netwerkinstellingen via een HyperTerminal-verbinding of met behulp van de installatiesoftware.

Uitloggen op de IP-manager voor beheer op afstand

Met deze knop wordt de huidige gebruiker afgemeld en verschijnt er een nieuw aanmeldingsscherm. NB: de gebruiker wordt automatisch uitgelogd als er gedurende een halfuur geen activiteit plaatsvindt.

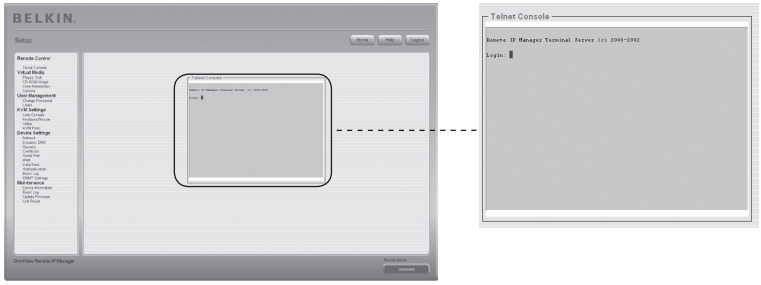
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:35:22 AM

KVM-console

Voorbeeld externe console

Klik op het invoervak van het linkermenu of op het consolepictogram rechts om de KVM-console te openen. Klik op de knop “Refresh” (Vernieuwen) om de afbeelding te vernieuwen.

Telnet-console



De RIPM-firmware is voorzien van een Telnet-gateway waarmee een gebruiker verbinding kan maken met de RIPM via een standaard Telnet-client. U kunt een terminalprogramma, zoals xterm, TeraTerm of PuTTY, gebruiken om verbinding te maken met de RIPM via het Telnet-protocol. U kunt ook de Telnet-opdracht in de opdrachtregel invoeren of het dialoogvenster “Uitvoeren” vanuit het Windows Startmenu gebruiken. Als voorbeeld kunt u de volgende lokatie invoeren:

Telnet: 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:35:23 AM

Vervang het IP-adres door het IP-adres dat tijdens de installatie aan de RIPM is toegewezen. U kunt vervolgens de gebruikersnaam- en wachtwoordgegevens invoeren om in te loggen. De referenties die voor de authentificatie moeten worden ingevoerd, zijn identiek aan de referenties van de webinterface. Dit betekent dat het gebruikersbeheer van de Telnet-interface volledig wordt bestuurd met behulp van de bijbehorende functies van de webinterface. Nadat u hebt ingelogd in de RIPM, verschijnt er een opdrachtregel en kunt u de bijbehorende beheeropdrachten invoeren. In het algemeen ondersteunt de Telnet-interface twee besturingsmodi: de opdrachtregel-modus en de terminalmodus. De opdrachtregel-modus wordt gebruikt om bepaalde parameters te besturen of weer te geven. In de terminalmodus wordt de pass-through toegang naar de seriële poort 1 ingeschakeld (als de waarden voor de seriële verbinding correct zijn ingesteld). Er is een null-modemkabel vereist om verbinding met de RIPM te maken via de seriële interface. Alle invoer wordt doorgestuurd naar het apparaat dat is aangesloten op seriële poort 1 en de antwoorden worden op de Telnet-interface weergegeven.

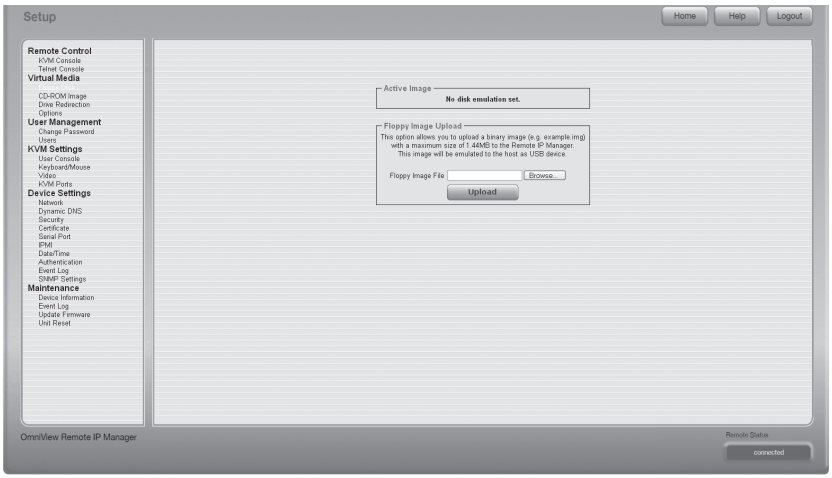
In de onderstaande lijst worden de opdrachtensyntaxis en het gebruik weergegeven.

Help	Hiermee geeft u de lijst met mogelijke opdrachten weer.
cls	Hiermee maakt u het scherm leeg.
sluiten	Sluit de huidige sessie en sluit de verbinding van de client.
versie	Hiermee geeft u informatie over de uitgave weer.
terminal	Hiermee start u een terminalmodus pass-through toegang voor de seriële poort 1. Met de sneltoetscombinatie “esc exit” schakelt u terug naar de opdrachtmodus. De opdracht is voorzien van een optionele parameter (1 of 2) om de gewenste seriële poort voor pass-through te selecteren.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:35:23 AM

Diskette



Deze functie wordt gebruikt voor het uploaden en verzenden van beeldbestanden. Met deze optie kunt u binaire afbeeldingen (bijvoorbeeld .img) van maximaal 1,44MB naar de RIPM uploaden. De afbeelding wordt geëmuleerd naar de host als USB-apparaat. Alle andere formaten moeten worden verzonden met behulp van de functie Drive Redirection. Mount deze afbeelding met behulp van een Windows share om een grotere afbeelding te gebruiken.

Een diskette-afbeelding uploaden

Stap 1: Klik op “Browse” (Bladeren) om het bestand dat u wilt uploaden te selecteren.

Stap 2: Klik op “Upload” (Uploaden) om het bestand naar de RIPM te uploaden. Er wordt een bevestiging weergegeven zodra het uploaden van het bestand naar de RIPM is voltooid.

Stap 3: Klik op “KVM-console” in het externe console-gedeelte van de RIPM-interface om toegang krijgen tot het bureaublad van de externe computer.

Stap 4: Dubbelklik op Deze computer om de betreffende map te openen.

Stap 5: Er verschijnt een tweede weergave voor het diskettestation onder Deze computer. Deze weergave wordt “3-1⁄2 Floppy (B)” genoemd. De verzonden bestanden staan in deze map.

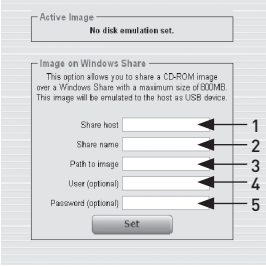
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:35:23 AM

Afbeelding op cd-rom

Afbeelding gebruiken op Windows Share (SAMBA).

Selecteer “CD-ROM” uit het
submenu om een afbeelding vanuit een Windows Share toe te voegen.

U moet de volgende gegevens opgegeven om de geselecteerde afbeelding correct
te mounten:



1. **Host delen**
   De servernaam of het IP-adres van de host. (Dit is het IP-adres dat wordt verkregen door de drive-redirection-software (zie de uitleg hieronder) uit te voeren.
2. **Naam delen**
   De naam van de gedeelde map die wordt gebruikt.
3. **Pad naar afbeelding**
   Het pad naar de afbeelding op de share.
4. **Gebruiker (optioneel)**
   Specificeer, indien nodig, de gebruikersnaam voor de share. Als deze niet worden gespecificeerd en de gastaccount is ingeschakeld, dan zullen deze gastaccount-gegevens worden gebruikt als uw login.
5. **Wachtwoord (optioneel)**
   Specificeer het wachtwoord voor de gebruikersnaam als hier om wordt gevraagd

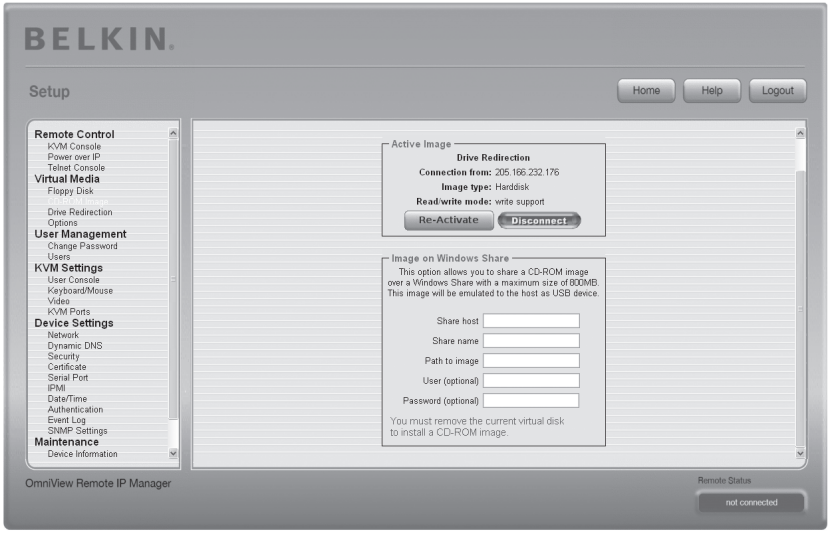
P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:35:24 AM

Cd-rom-afbeelding uploaden

Stap 1: Start de drive-redirection software.

Stap 2:

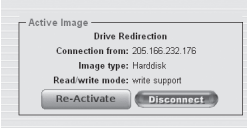
Laat het venster open en ga naar de Cd-rom-afbeelding in het onderdeel Virtuele Media van de RIPM-interface nadat de drive-redirection software verbinding heeft gemaakt.



Let op: Het IP-adres dat wordt weergegeven onder “Verbonden met” is het IP-adres dat wordt gebruikt als het hostadres van de share. Sluit de seriële kabel aan tussen de RIPM en de computer en open een hyperterminal-sessie om te controleren of het door de drive-redirection software toegewezen IP-adres correct is. Log in als “ping” en voer exact hetzelfde IP-adres in als in het veld “Share host”. De melding “<IP> is alive!” moet nu verschijnen.

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:35:24 AM

Stap 3: Klik op “Heractiveren” in het onderdeel actieve afbeelding.



Stap 4: Voer het IP-adres dat door de drive re-direction software is geleverd in het veld “Share Host “ in.

Stap 5: Voer de “Share name” en het “Pad naar afbeelding” in.

Stap 6: Klik op de knop “Set” (Instellen) om het bestand te uploaden. Het bestand wordt op de externe computer weergegeven als USB-apparaat.

De gespecificeerde afbeelding is toegankelijk vanaf de RIPM. De bovenvermelde gegevens moeten worden opgegeven in verband met de RIPM. Het is van groot belang dat u de correcte IP-adressen en apparaatnamen opgeeft. Gebeurt dit niet, dan is het mogelijk dat de RIPM de afbeelding niet kan openen en het betreffende bestand un-mounted (in de plaats hiervan verschijnt er een foutmelding). Wij raden u aan de correcte waarden te gebruiken en deze stap, indien nodig, te herhalen.

De opgegeven share moet correct zijn geconfigureerd. Hiervoor zijn er administratieve toegangsrechten vereist. Het kan voorkomen dat een normale gebruiker deze toegangsrechten niet heeft. U kunt inloggen als systeembeheerder of uw systeembeheerder vragen om u te helpen bij het uitvoeren van deze taak.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:35:24 AM

Drive Redirection (Schijf-doorsturing)

De functie drive-redirection biedt een andere manier om een virtuele schijf op de externe computer te gebruiken. U kunt met een schijf werken op uw lokale computer vanaf de externe machine door deze schijf te delen via een TCP-netwerkverbinding. U kunt opslagapparaten inclusief diskettestations en harde schijven*, cd-romspelers en verwisselbare media zoals USB-sticks doorsturen. U kunt zelfs uw externe machine zo configureren dat deze gegevens naar een lokale schijf kan schrijven.

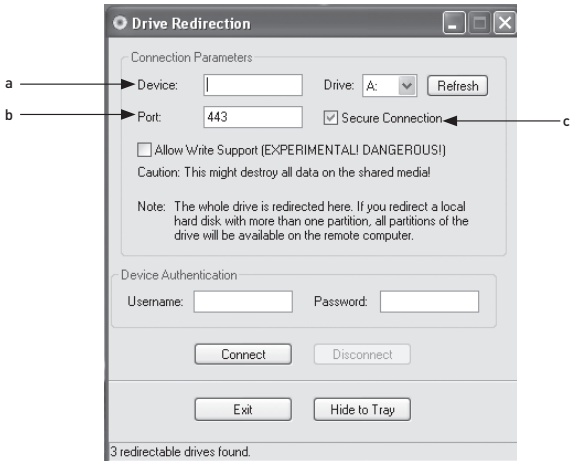
***Let op:** Wij raden u aan geen schrijfondersteuning in te schakelen tijdens het doorsturen van harde schijven en Belkin is niet verantwoordelijk voor verlies of beschadiging van gegevens tijdens dit proces.

Wees voorzichtig wanneer u deze functie gebruikt. Drive Redirection werkt op een niveau ver beneden het besturingssysteem, zodat noch het lokale, noch het externe besturingssysteem detecteert dat er een station wordt doorgestuurd. Dit kan leiden tot een inconsistente gegevenoverdracht als een van de besturingssystemen (op de lokale of externe machine) gegevens naar het apparaat schrijft. Wanneer u schrijfondersteuning hebt ingeschakeld, kan het voorkomen dat de externe computer gegevens en het bestandsysteem op het doorgestuurde apparaat beschadigt. Als het lokale besturingssysteem gegevens naar het doorgestuurde apparaat schrijft, kan het voorkomen dat het besturingssysteem op de externe host oudere gegevens bevat waardoor het besturingssysteem van de externe host ontregeld raakt. Wij raden u dus aan deze functie, vooral de functie voor schrijfondersteuning, met grote voorzichtigheid te gebruiken.

Let op: U moet de meegeleverde software voor schijf-doorsturing installeren om de functie schijf-doorsturing te kunnen gebruiken op de computer die u gebruikt om externe toegang tot de RIPM te krijgen.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:35:25 AM

1. Start de drive-redirection software.



2. Geef de parameters van de netwerkverbinding op.

a. Apparaat

Dit is het IP-adres van de RIPM waarmee u verbinding wilt maken.

b. Poort

Dit is de netwerkpoort. De RIPM gebruikt standaard de externe consolepoort (#443). U kunt deze waarde wijzigen als u de externe consolepoort in de netwerkinstellingen van uw RIPM hebt gewijzigd.

c. Veilige verbinding

Selecteer deze optie om een beveiligde verbinding via SSL in te schakelen. Dit zorgt voor een veilige verbinding, maar kan de overdrachtsnelheid vertragen.

3. Selecteer het station dat u wilt doorsturen. Alle beschikbare apparaten (stationsletters) worden weergegeven. NB: het volledige station, en niet slechts één partitie, wordt door de RIPM met de externe computer gedeeld. Als uw harde schijf meer dan één partitie bevat, worden alle stationsletters van die schijf doorgestuurd. Gebruik de knop “Refresh” (Vernieuwen) om de lijst met stationsletters te vernieuwen. Dit is met name van belang voor USB-sticks.

4. Schrijfondersteuning

Waarschuwing: Wees voorzichtig met het gebruik van deze functie. Met de functie Schrijfondersteuning kunt u met de externe computer gegevens naar uw lokale schijfstation schrijven. Als zowel het externe als het lokale systeem gelijktijdig gegevens willen schrijven naar hetzelfde apparaat, **zal het bestandsysteem op het station worden vernietigd.** Gebruik deze functie uitsluitend wanneer u er zeker van bent dat u dit veilig kunt uitvoeren.

Let op: Wij raden u aan geen schrijfondersteuning in te schakelen tijdens het doorsturen van harde schijven en Belkin is niet verantwoordelijk voor verlies of beschadiging van gegevens tijdens dit proces.

5. Het apparaat authenticeren. Om Drive Redirection te gebruiken moet u zich met een geldige gebruikersnaam en wachtwoord bij de RIPM aanmelden. Er moet toestemming worden verleend om de configuratie van de virtuele schijf te wijzigen.

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:35:25 AM

6. Schakel de Drive Redirection in door eenmaal op de knop “Connect” (Verbinden) te drukken.
Als alle instellingen correct zijn uitgevoerd, geeft de statusbalk weer dat de verbinding tot stand is gebracht en is de knop “Connect” (Verbinden) uitgeschakeld en de knop “Disconnect” (Verbinding verbreken) ingeschakeld. In geval van een storing, wordt er een foutmelding op de statusregel weergegeven.

De schijfdoorsturing-software probeert de lokale schijf te vergrendelen voordat deze wordt doorgestuurd. Hierdoor krijgt het lokale besturingssysteem geen toegang tot de schijf zolang deze wordt doorgestuurd. De poging wordt geannuleerd als er een bestand op de schijf geopend is. U krijgt een melding waarin u kunt bevestigen dat u de verbinding tot stand wilt brengen als de vergrendeling mislukt. Als u echter schrijfondersteuning hebt ingeschakeld, kan Drive Redirection ertoe leiden dat een station wordt beschadigd als dit niet is vergrendeld.

7. Gebruik de knop “Disconnect” (Verbinding verbreken) om Drive Redirection te stoppen nadat het proces is opgestart.
8. Klik op “Afsluiten” om de schijfdoorsturing af te sluiten. De verbinding zal worden verbroken voordat het programma wordt afgesloten als er een schijfdoorsturing-verbinding actief is.
9. Gebruik de knop “Hide to Tray” (Minimaliseren) om de applicatie te minimaliseren zonder deze volledig af te sluiten. Een verbinding blijft actief totdat u de applicatie afsluit. U kunt de software openen door te dubbelklikken op het pictogram in de taakbalk. Het pictogram in de taakbalk geeft ook weer of er al dan niet een verbinding is. Klik met de rechtermuisknop op het pictogram om een submenu te openen.

Opties

Drive Redirection uitschakelen
Hiermee schakelt u de Drive Redirection uit.

Alleen-lezen verbindingen forceren
Hiermee schakelt u de Drive Redirection voor schijfdoorsturing uit.

Klik op “Toepassen” om de wijzigingen te bevestigen.

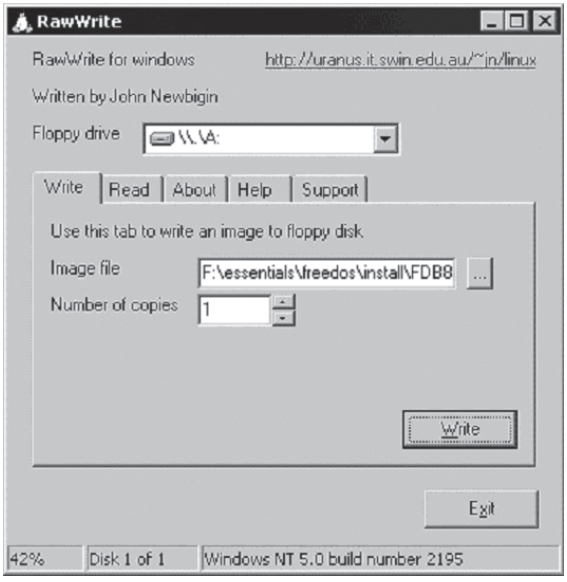
P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:35:25 AM

Images maken

Image van diskettestation

UNIX® en UNIX-achtige besturingssystemen (OS)
maken gebruik van “dd” voor het maken van een imagebestand. Dit is een van de Unix-hulpprogramma’s die zijn opgenomen binnen elk Unix-besturingssysteem (UNIX, Sun Solaris, Linux). Kopieer de inhoud van een diskette naar een bestand om een image van het diskettestation te maken. Hiervoor kunt u de volgende opdrachtregel gebruiken: dd [if=/dev/fd0] [of=/tmp/floppy.image]. Hierna leest “dd” de volledige diskette vanaf het apparaat “/dev/fd0” en bewaart de gegevens in het opgegeven uitvoerbestand “/tmp/floppy.image”. Pas de beide parameters aan uw wensen aan (invoerapparaat, enz.).

MS Windows
U kunt het hulpprogramma “RawWrite voor Windows” gebruiken.



Selecteer het tabblad “Lezen” uit het menu. Voer (of selecteer) de naam van het bestand in waar u de inhoud van de diskette naartoe wilt kopiëren. Klik op de knop “Copy” (Kopiëren) om het image-aanmaakproces te starten Raadpleeg de homepage van het “fdos project” **(http://www.fdos.org).** voor bijbehorende hulpprogramma’s.

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:35:25 AM

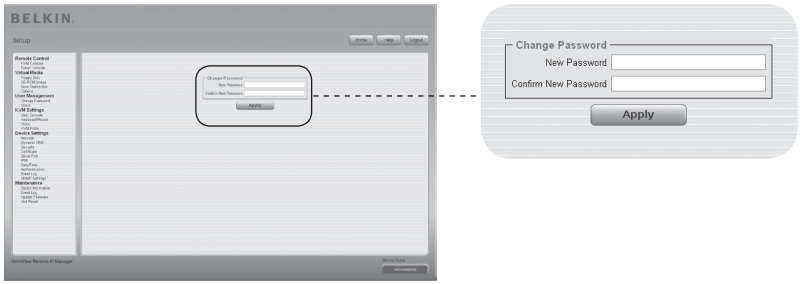
CD-ROM/ISO 9660-images

UNIX en UNIX-achtige
besturingssystemen (OS) maken gebruik van “dd” voor het maken van een imagebestand. Dit is een van de Unix-hulpprogramma’s die zijn opgenomen binnen elk Unix-besturingssysteem (UNIX, Sun Solaris, Linux). Kopieer de inhoud van de cd-rom naar een bestand om een image van de cd-rom te maken. Hiervoor kunt u de volgende opdrachtregel gebruiken: **dd [if=/dev/cdrom] [of=/tmp/cdrom.image].** Hierna leest “dd” de volledige schijf vanaf het apparaat “/dev/cdrom” en bewaart de gegevens in het opgegeven uitvoerbestand “/tmp/cdrom.image”. Pas de beide parameters aan uw wensen aan (invoerapparaat etc.).

MS Windows
U kunt uw favoriete hulpprogramma voor cd-imaging gebruiken. Kopieer de volledige inhoud van de cd in een ISO-imagebestand op uw harde schijf. Met “Nero” kiest u bijvoorbeeld “Kopiëren en backup” en gaat u naar het onderdeel “Schijf kopiëren”. Selecteer het cd-rom of dvd-station waarvan u een ISO-image wilt maken. Geef een naam op voor de ISO-image en sla de inhoud van de cd-rom op in dat bestand.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:35:25 AM

Wachtwoord wijzigen

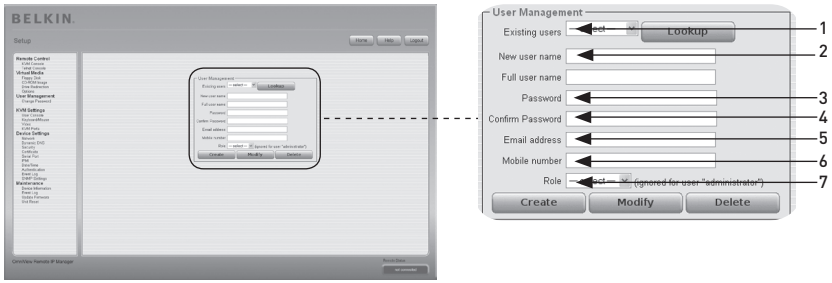


Voer in het bovenste invoerveld een nieuw wachtwoord in om uw wachtwoord te wijzigen. Voer het wachtwoord nogmaals in het veld eronder in.

Klik op “Apply” (Toepassen) om de wijzigingen door te voeren.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:35:26 AM

Gebruikers



Gebruikersbeheer

De RIPM is voorzien van een voorgeconfigureerde gebruikersaccount voor de beheerder met vooraf ingestelde toegangsrechten. Deze gebruiker heeft alle rechten om het apparaat te configureren en kan alle functies van de RIPM gebruiken. Het standaardwachtwoord voor de gebruikersaccount “beheerder” is “belkin”. Zorg dat u dit wachtwoord onmiddellijk wijzigt nadat u uw RIPM voor de eerste maal hebt geïnstalleerd en geopend. Hieronder volgt een volledige lijst van de beschikbare opties. Deze lijst kan uitsluitend worden geopend door de beheerder.

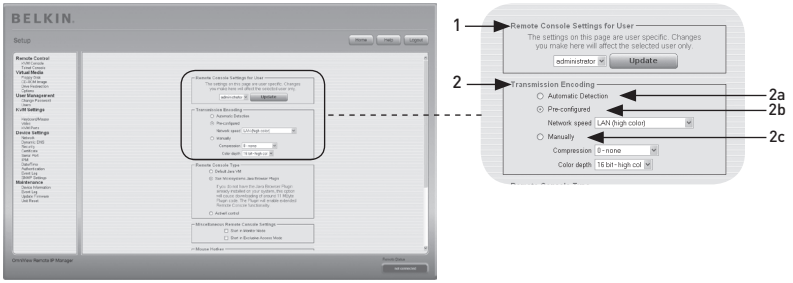
1. **Bestaande gebruikers**
   Een bestaande gebruiker selecteren en wijzigen. Klik de knop “lookup” (bekijken) om de gebruikersgegevens te bekijken nadat u de gebruiker hebt geselecteerd.
2. **Nieuwe gebruikersnaam**
   Een nieuwe gebruikersnaam voor de geselecteerde account.
3. **Wachtwoord**
   Het wachtwoord voor de inlognaam. Dit moet minstens vier tekens bevatten.
4. **Wachtwoord bevestigen**
   Bevestiging van het bovenstaande wachtwoord.
5. **E-mailadres**
   Deze functie is optioneel.
6. **Mobiele telefoonnummer**
   Deze functie is optioneel.
7. **Rol**
   Naast beheerder of gewone gebruiker, kan elke gebruiker lid zijn van een groep (dit wordt “rol” genoemd). Kies de gewenste rol uit het selectievak. Druk op de knop “Create” (Creëren) om een nieuwe gebruiker aan te maken. Met de knop “Modify” (Wijzigen) kunt u de weergegeven gebruikersinstellingen wijzigen. Druk op de knop “Delete” (Verwijderen) om een gebruiker te verwijderen.

Let op: De RIPM is voorzien van een host-onafhankelijke processor en geheugeneenheid, die beide zijn voorzien van beperkingen op het gebied van verwerkingsinstructies en beschikbaar geheugen. Wij raden u aan het aantal van 25 tegelijk aangesloten gebruikers NIET te overschrijden om een acceptabele responstijd te garanderen. Het beschikbare geheugen in de RIPM is afhankelijk van de configuratie en het gebruik van de RIPM (invoer in het logboekbestand etc.).

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:35:26 AM

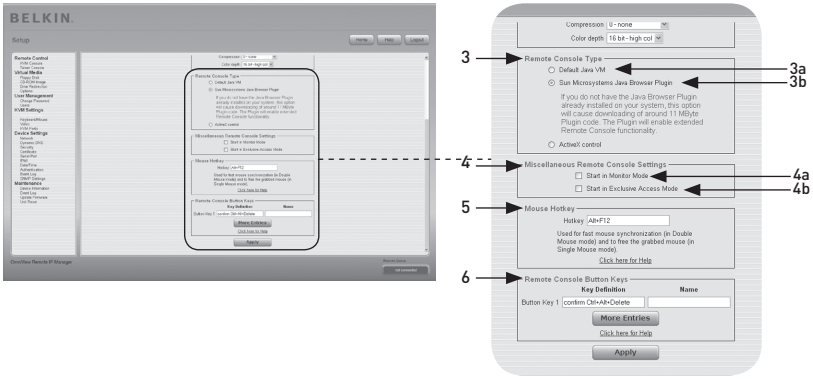
Gebruikersconsole

De volgende instellingen zijn gebruikersspecifiek. Dit betekent dat de beheerder deze instellingen voor elke afzonderlijke gebruiker kan aanpassen. De wijzigingen voor een bepaalde gebruiker hebben geen invloed op de instellingen van de andere gebruikers.



1. **Externe console instellingen voor een gebruiker**
   in dit selectievakje wordt de gebruiker-ID weergegeven waarvoor de waarden worden weergegeven en waarop de wijzigingen van toepassing zijn. Selecteer de gewenste gebruiker uit het selectievakje en druk op de knop “Update” (Bijwerken). De gebruikersinstellingen zoals hieronder weergegeven verschijnen.
   Opmerking: U kunt uitsluitend de instellingen van andere gebruikers wijzigen als u de benodigde toegangsrechten voor deze taak hebt. Voor normale gebruikers zonder de benodigde toegangsrechten is het niet mogelijk de instellingen van andere gebruikers te wijzigen.
2. **Transmissiecodering**
   Met de instelling voor transmissiecodering kunt u het algoritme voor beeldcodering wijzigen dat wordt gebruikt voor het verzenden van de videogegevens naar het scherm Externe console. Met deze instellingen kunt u de snelheid van het externe beeldscherm optimaliseren afhankelijk van het aantal gebruikers dat tegelijkertijd gebruik maakt van de bandbreedte van de lijnverbinding (Modem, ISDN, DSL, LAN, enz.).
   2a. Automatische detectie
   Het niveau van codering en compressie worden automatisch bepaald op basis van de beschikbare bandbreedte en de huidige inhoud van het videobeeld.
   2b. Voorgeconfigureerde instellingen
   De voorgeconfigureerde instellingen leveren het beste resultaat dankzij de geoptimaliseerde compressie-aanpassing en kleurdiepte voor de aangegeven snelheid van het netwerk.
   2c. Handmatige configuratie
   Hiermee kunt u afzonderlijk het compressieniveau en de kleurdiepte aanpassen. Afhankelijk van het geselecteerde compressieniveau, wordt de gegevensstroom tussen de RIPM en de externe console gecomprimeerd om bandbreedte te sparen. Omdat een hoog compressieniveau veel tijd vraagt, moet u deze niet gebruiken terwijl er meerdere gebruikers tegelijkertijd toegang hebben tot de RIPM. De standaardkleurdiepte is 16-bit (65.536 kleuren). Andere kleurdiepten zijn bedoeld voor langzamere netwerkverbindingen waardoor een snellere gegevensoverdracht mogelijk wordt. Compressieniveau 0 (geen compressie) gebruikt in zo’n geval een kleurdiepte van 16-bit. Bij een lagere bandbreedte wordt een kleurdiepte van 4-bit (16 kleuren) en 2-bit (4 grijstinten) aanbevolen voor standaard desktop-interfaces. Foto-achtige afbeeldingen worden het best weergegeven met een kleurdiepte van 4-bit. Een kleurdiepte van 1-bit (zwart/wit) wordt alleen aanbevolen voor extreem langzame netwerkverbindingen.

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:35:27 AM



3. **Type externe console**
   Geeft aan welke externe console viewer u moet gebruiken.

   3a. Standaard Java Virtual Machine (JVM)
   Deze functie gebruikt de standaard JVM van uw webbrowser; Microsoft JVM voor Internet Explorer of Sun JVM.

   3b. Plug-in voor Sun Microsystems Java Browser
   Met deze plug-in geeft u de webbrowser van uw beheerssysteem de opdracht om JVM of Sun Microsystems te gebruiken. De JVM in de browser wordt gebruikt om de code uit te voeren voor het externe console-venster dat in feite een Java applet is. Als u dit vakje voor de eerste maal op uw beheersysteem inschakelt en de betreffende Java plug-in nog niet op uw systeem is geïnstalleerd, kunt u deze automatisch downloaden en installeren. Om de installatie echter mogelijk te maken, moet u de betreffende dialoogvensters met 'ja' beantwoorden. Het downloadvolume is ongeveer 11Mbps. Het voordeel van de JVM van Sun is dat deze een stabiele en identieke Java Virtual Machine over verschillende platforms levert. De externe console-software is voor deze JVM-versie geoptimaliseerd en biedt een grotere functionaliteit.

4. **Diverse instellingen voor de externe console**

   4a. Opstarten in monitormodus
   Met deze instelling kunt u de beginwaarde voor de monitormodus selecteren. De monitormodus is standaard uitgeschakeld. Als u deze inschakelt wordt het externe console-venster in de alleen-lezenmodus opgestart.

   4b. Opstarten in de exclusieve toegangmodus
   Hiermee schakelt u de exclusieve toegangmodus in tijdens het opstarten van de externe console. Wanneer u deze modus gebruikt, worden de externe consoles van alle andere gebruikers gesloten. Geen enkele andere gebruiker kan de externe console tegelijkertijd openen totdat u de exclusieve toegang uitschakelt of uitlogt.

5. **Sneltoets voor de muis**
   Met de sneltoets voor de muis kunt u een sneltoetscombinatie bepalen om de synchronisatieprocedure voor de muis te starten (door deze combinatie in de externe console in te voeren) of de directe muismodus te verlaten.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:35:28 AM

6. Externe console Button Keys

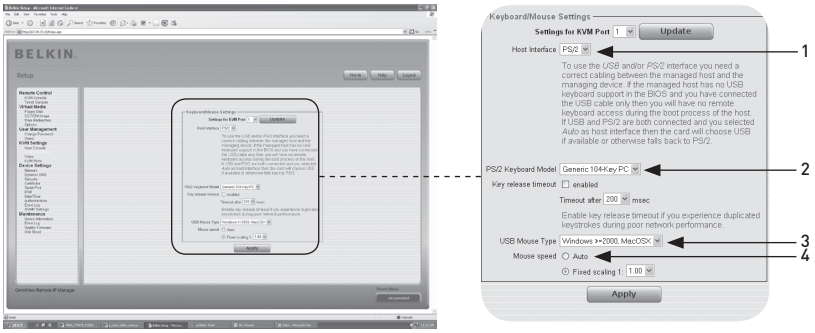
Met de button keys kunt u sneltoetsen op het externe systeem simuleren die lokaal niet kunnen worden gegenereerd. Dit kan van belang zijn als er een toets ontbreekt of het lokale besturingssysteem van de externe console onvoorwaardelijk bepaalde toetsaanslagen uitvoert. Voorbeelden hiervan zijn: “Control+Alt+Delete”, die binnen Windows en DOS altijd wordt uitgevoerd, of de sneltoetscombinatie “Control+Backspace” binnen Linux, die wordt gebruikt voor het beëindigen van de X-server. Raadpleeg de regels waarin een instelling voor een toets wordt beschreven om een nieuwe button key te definiëren of een bestaande aan te passen. In het algemeen is de syntaxis voor een nieuwe sneltoets als volgt:

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

Een term tussen haakjes is optioneel. Het sterretje aan het einde betekent dat u zo vaak als nodig andere toetsen moet toevoegen. Met de term “confirm” voegt u een dialoogvenster voor bevestiging toe die wordt weergegeven voordat de geselecteerde toetsaanslag wordt verzonden naar de externe host. De “keycode” is de toetsaanslag die wordt verzonden. U kunt meerdere toetscodes samenvoegen met een plus- of min–teken, of het “<”-teken. Toetscombinaties worden opgebouwd met het + teken; alle toetsen worden ingedrukt totdat een – teken of het einde van de combinatie verschijnt. In zo’n geval worden alle ingedrukte toetsen in omgekeerde volgorde vrijgegeven. Het min-teken bouwt dus enkelvoudige afzonderlijke toetsdrukken en vrijgaven op. Het “<”-teken geeft uitsluitend de laatste toets vrij. Met het sterretje voegt u een pauze in van 100 milliseconden. Voorbeeld: de toetsencombinatie Ctrl, Alt en F2 heeft de combinatie “Ctrl+Alt+F2” tot gevolg.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:35:28 AM

Toetsenbord/muis



1.

Hostinterface
Met de hostinterface kunt u de interface waarmee de muis is verbonden inschakelen. U kunt kiezen tussen “Auto”, voor automatische detectie, “USB”, voor een USB-muis of “PS/2”, voor een PS/2-muis.

Let op: Het is van belang dat u de juiste kabels gebruikt tussen de managed host en het managing device voor het gebruik van de USB- en/of PS/2-interface. Als de managed host geen ondersteuning biedt voor USB-toetsenborden in de BIOS en u de USB-kabel hebt aangesloten, hebt u geen externe toegang met het toetsenbord tijdens het opstartproces van de host. Als er zowel een USB als een PS/2 is aangesloten en u “Auto” selecteert als hostinterface, zal, indien beschikbaar, tijdens het opstarten USB worden geselecteerd. Als er geen USB beschikbaar is, zal PS/2 worden geselecteerd.

Er moet aan de volgende voorwaarden worden voldaan om externe toegang via een USB-toetsenbord mogelijk te maken tijdens het opstartproces van de host:

- de host-BIOS moet zijn voorzien van USB-toetsenbordondersteuning
- de USB-kabel moet zijn aangesloten of zijn geselecteerd in de optie “Hostinterface”

2. PS/2 toetsenbordmodel
Hiermee kunt u een lay-out voor het toetsenbord kiezen tussen “Generic 101-Key PC”, voor de standaardlay-out van het toetsenbord, “Generic 104-Key PC”, voor een standaardtoetsenbordlay-out, uitgebreid met 3 aanvullende Windowstoetsen, “Generic 106-Key PC”, voor een Japans toetsenbord en “Apple Macintosh”, voor het Macintosh®-toetsenbord. Selecteer de bijbehorende optie en voer de gewenste tijdwaarde in het onderstaande invoerveld in als er een time-outinstelling voor het toetsenbord is vereist.

3. USB-muistype
Hiermee schakelt u het USB-muistype in. Kies de gewenste optie in het selectievakje. Raadpleeg het hoofdstuk “Aanbevolen instellingen voor de muis” op pagina 21 van deze handleiding voor een gedetailleerde beschrijving van het muistype en de aanbevolen instellingen voor de diverse besturingssystemen.*

*Deze functie werkt uitsluitend met Windows-besturingssystemen.

P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:35:29 AM

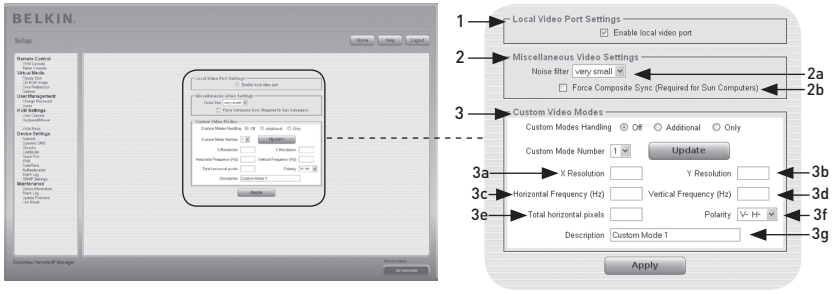
4. Muissnelheid

- **Automatische muissnelheid**
  Gebruik deze optie als de host aanvullende instellingen voor muisversnelling gebruikt. De RIPM detecteert de versnelling en snelheid van de muis tijdens de synchronisatieprocedure van de muis.
- **Directe muissnelheid**
  Gebruik deze optie om de muisbewegingen tussen de lokale en de externe muisaanwijzers direct weer te geven. U kunt ook een vaste schaling instellen waarmee het aantal pixels van de beweging van de muisaanwijzers wordt bepaald wanneer de lokale muisaanwijzer met één pixel wordt bewogen. Deze optie werkt alleen wanneer de muisinstellingen op de host lineair zijn (er geen muisversnelling wordt gebruikt).

Klik op de knop “Apply” (Toepassen) om de instellingen uit te voeren.

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:35:29 AM

Video



Klik op de knop “Apply” (Toepassen) om de instellingen (hieronder) uit te voeren.

1. **Instellingen voor lokale videopoort**

   Lokale videopoort inschakelen
   Met deze optie bewaakt u de lokale video-uitgang van de RIPM en bepaalt u of deze is ingeschakeld en via het binnenkomende signaal van het hostsysteem wordt doorgegeven.

2. **Diverse video-instellingen**

   2a. Ruisfilter
   Met deze optie bepaalt u op welke manier de RIPM reageert op kleine wijzigingen in het binnenkomende videosignaal. Een ruime instelling voor de filter heeft minder netwerkverkeer en een snellere videoweergave tot gevolg, maar het kan zijn dat kleine wijzigingen in delen van de display niet meteen worden herkend. Met een smalle instelling voor de filter worden alle wijzigingen meteen weergegeven, maar kan leiden tot een constante stroom netwerkverkeer, zelfs wanneer er geen wijzigingen op de display plaatsvinden (afhankelijk van de kwaliteit van het binnenkomende videosignaal).

   2b.

   Composietsynchronisatie forceren (vereist voor Sun Computers)
   Schakel deze optie in om de signaaloverdracht vanaf een Suncomputer te ondersteunen. Als deze functie niet is ingeschakeld, zal het beeld van de externe console niet zichtbaar zijn.

3. **Aangepaste videomodi**
   U kunt maximaal 4 aangepaste videoresoluties instellen.

   Met de optie “Aangepaste modusverwerking” kunt u aangepaste modi uitschakelen (“Off”), of een reeks standaard of exclusieve (“Only”) videoresoluties instellen. Met een andere optie (“Additional”) kunt u een speciale videomodus voor de RIPM forceren. Kies het gewenste getal uit het selectievakje en druk op de knop “Update” (Bijwerken) om de parameters van de aangepaste videomodus te wijzigen. U moet enkele aanvullende gegevens invoeren zo dat de videomodus correct kan worden herkend:

   Waarschuwing: De optie “Host Monitor Settings” (Instellingen hostmonitor) is uitsluitend bedoeld voor ervaren gebruikers. Verkeerd gebruik kan leiden tot verslechtering van de video-overdracht. Zorg ervoor dat u deze functie goed kent voordat u probeert de instellingen van de hostmonitor aan te passen.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:35:29 AM

3a. X-resolutie
Deze functie heeft betrekking op het zichtbare aantal horizontale pixels.

3b. Y-resolutie
Deze functie heeft betrekking op het zichtbare aantal verticale pixels.

3c. Horizontale frequentie (Hz)
Deze functie heeft betrekking op de horizontale (lijn)frequentie, uitgedrukt in hertz.

3d. Verticale frequentie (Hz)
Deze functie heeft betrekking op de verticale (verversings)frequentie, uitgedrukt in hertz.

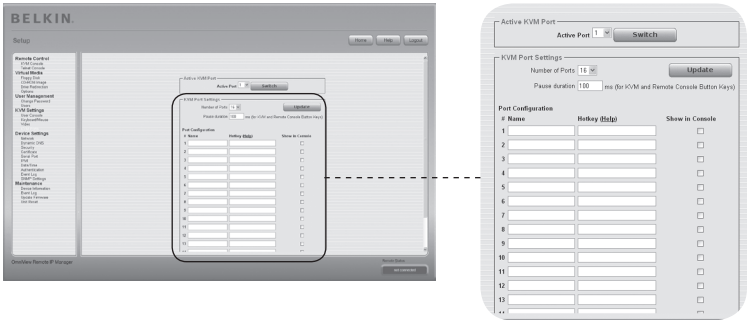
3e. Totaal aantal horizontale pixels
Deze functie heeft betrekking op het totaal aantal pixels per lijn, inclusief de onzichtbare en blanco gebieden.

3f. Polariteit
Deze functie heeft betrekking op de positieve of negatieve eigenschappen van synchronisatiesignalen. De letter V betekent verticale polariteit; de letter H betekent horizontale polariteit.

3g. Beschrijving
Hier kunt u een naam voor de modus invoeren die in de externe console wordt weergegeven wanneer de aangepaste modus wordt geactiveerd.

KVM-poorten

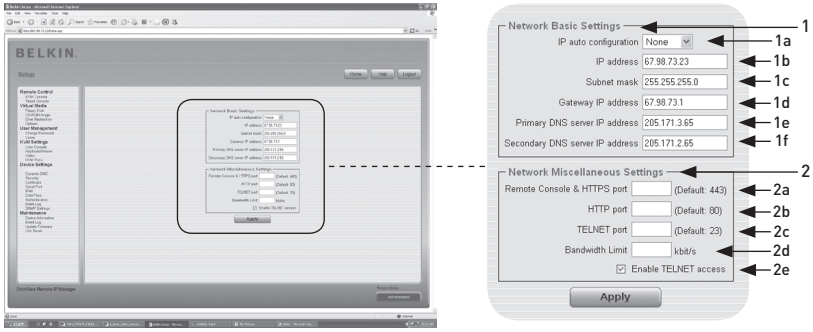
U kunt het aantal poorten selecteren dat de aangesloten kvm-switch gebruikt en aan elke poort een naam toekennen. Als u via de RIPM wilt kunnen schakelen tussen de kvm-poorten, moet u voor deze poorten bepaalde toetscombinaties definiëren.



P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:35:30 AM

Netwerk

Met behulp van het scherm “Network Settings” (Netwerkinstellingen) kunt u parameters met betrekking tot het netwerk wijzigen zoals hieronder wordt beschreven. De nieuwe
netwerkinstellingen worden meteen van kracht nadat u op Toepassen hebt gedrukt.



Waarschuwing: Het wijzigen van de netwerkinstellingen van de RIPM kan verlies van de netwerkverbinding tot gevolg hebben. Zorg ervoor dat alle waarden correct zijn zodat u de toegang tot de RIPM niet verliest als u de instellingen op afstand wijzigt.

1. **Basisinstellingen voor het netwerk**

   1a. Automatische IP-configuratie
   Met deze optie bepaalt u de locatie waarvan de RIPM de netwerkinstellingen haalt. Dit kan een DHCP- of een BOOTP-server zijn. Selecteer “DHCP” voor DHCP of “bootp” voor BOOTP. Als u “geen” kiest, wordt de automatische IP-configuratie uitgeschakeld.

   1b. Het IP-adres wordt toegewezen door uw netwerkbeheerder.

   1c. De term **“Subnet Mask” (Subnetmasker)** heeft betrekking op het net mask van het lokale netwerk, dat wordt gebruikt om het subnet te bepalen waartoe het IP-adres behoort.

   1d. Gateway IP-adres
   Stel dit IP-adres in op het IP-adres van de router van het lokale netwerk als de RIPM toegankelijk moet zijn vanaf andere netwerken dan het lokale netwerk.

   1e. Primaire DNS Server IP-adres
   Dit is het IP-adres van de primaire Domain Name Server (DNS) in puntnotatie. U kunt deze optie leeg laten, maar dan kan de RIPM geen name-resolution uitvoeren.

   1f. Secundaire DNS Server IP-adres
   Dit is het IP-adres van de secundaire Domain Name Server (DNS) in puntnotatie. Deze wordt gebruikt als er geen contact kan worden gemaakt met de primaire DNS.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:35:31 AM

2. Diverse netwerkinstellingen

2a. Externe Console en HTTPS-poort
Dit is het poortnummer waarop de externe consoleserver en HTTPS-server luisteren. Als u deze leeg laat, wordt de standaardwaarde gebruikt.

2b. HTTP-poort
Dit is het poortnummer waarop de HTTP-server van de RIPM luistert. Als u deze leeg laat, wordt de standaardwaarde gebruikt.

2c. Telnet-poort
Dit is het poortnummer waarop de telnet-poort van de RIPM luistert. Als u deze leeg laat, wordt de standaardwaarde gebruikt.

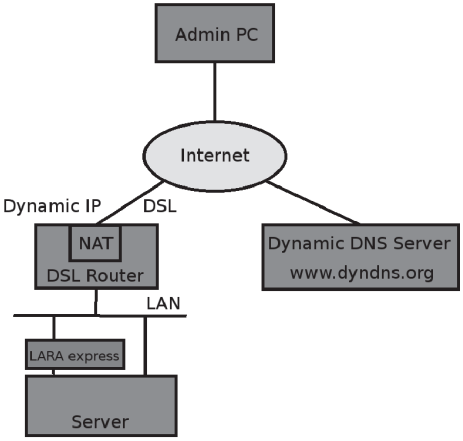
2d. Bandbreedte beperking
Deze optie heeft betrekking op het maximale netwerkverkeer dat via het Ethernet-apparaat van de RIPM mogelijk is (waarde in Kbps).

2e. Telnet-toegang inschakelen
Als u deze optie instelt, hebben gebruikers toegang tot de RIPM met behulp van de Telnet-gateway (zie hoofdstuk “Telnet-console” op pagina 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:35:31 AM

Dynamische DNS

U kunt een gratis beschikbare Dynamic DNS-service (dyndns.org) gebruiken in het volgende scenario:



Dynamische DNS-scenario

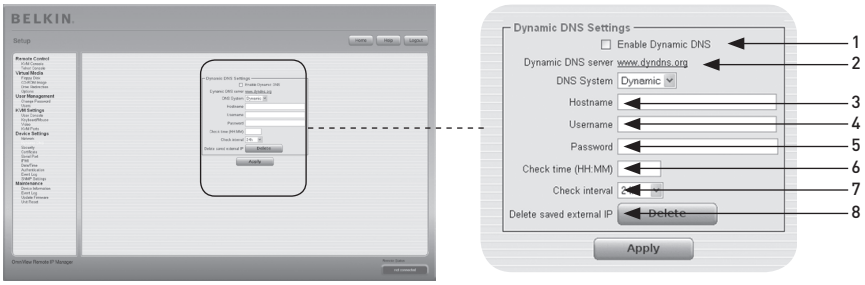
U kunt de RIPM via het IP-adres, dat dynamisch is toegewezen door uw Internetprovider, van de DSL-router bereiken. Omdat de beheerder het IP-adres dat is toegewezen door de internetprovider niet kent, wordt de RIPM in vastgestelde tussenpozen verbonden met een speciale dynamische DNS waar het IP-adres wordt geregistreerd. De beheerder heeft ook toegang tot deze server en kan hetzelfde IP-adres van de NIC ophalen. De beheerder moet een RIPM registreren en een bepaalde hostnaam toewijzen om deze DNS-service te kunnen gebruiken. Tijdens het registratieproces wordt er een gebruikersnaam en wachtwoord toegewezen. Deze accountgegevens, in combinatie met de hostnaam, is nodig om het IP-adres van de geregistreerde RIPM te bepalen.

U moet de volgende stappen uitvoeren om de dynamische DNS in te schakelen:

- Zorg ervoor dat de LAN-interface van de RIPM correct is geconfigureerd.
- Voer de instellingen van de dynamische DNS-configuratie in zoals weergegeven op pagina 55.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:35:31 AM

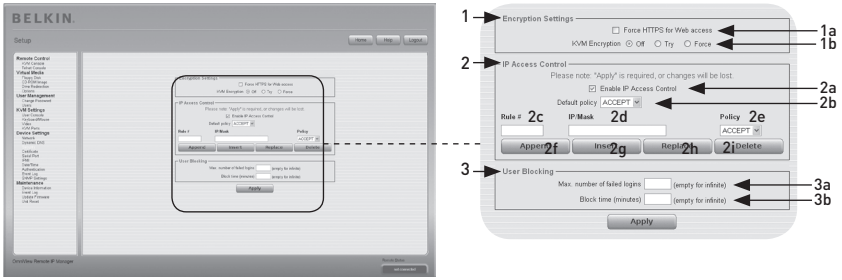
Dynamische DNS-instellingen



1. **Dynamische DNS inschakelen**
   Hiermee schakelt u de dynamische DNS-service in. Hiervoor is een geconfigureerd IP-adres van de DNS-server vereist.
2. **Dynamische DNS-server**
   De RIPM registreert zichzelf op deze locatie met regelmatige tussenpozen. Op het moment van het verschijnen van deze handleiding is de dynamische DNS ingesteld op een vaste stand omdat op dit moment uitsluitend dyndns.org wordt ondersteund.
3. **Hostnaam**
   RIPM is de hostnaam die door de dynamische DNS wordt geleverd. Gebruik de volledige naam, inclusief het domein (“testserver.dyndns.org” of “RIPM.dyndns.org”) en niet uitsluitend de werkelijke hostnaam.
4. **Gebruikersnaam**
   Tijdens de handmatige registratie bij de dynamische DNS moet u deze gebruikersnaam hebben geregistreerd.
   Let op: spaties zijn niet toegestaan binnen een gebruikersnaam.
5. **Wachtwoord**
   Tijdens de handmatige registratie bij de dynamische DNS hebt u dit wachtwoord toegewezen gekregen.
6. **Controletijd**
   De RIPM-kaart registreert zichzelf in de dynamische DNS “Controletijd”.
7. **Controle Interval**
   Dit is het interval voor rapportering aan de dynamische DNS door de RIPM.
   Let op: De RIPM is uitgerust met een eigen, real-time klok. Zorg ervoor dat de tijdinstelling van de RIPM correct is ingesteld.
8. Gebruik de handige optie “Opgeslagen externe IP verwijderen” als u uw extern opgeslagen IP-adres wil bijwerken. Druk op de knop “Delete” (Verwijderen) om het opgeslagen adres te verwijderen.

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:35:32 AM

Beveiliging



1. Encryptie instellen

1a. HTTPS forceren

Als deze optie is ingeschakeld, is de toegang tot het web front-end alleen mogelijk door middel van een HTTPS-verbinding. De RIPM zal niet “luisteren” voor binnenkomende verbindingen via de HTTP-poort. Raadpleeg het hoofdstuk “Certificatie” op pagina 58 als u uw eigen SSL-certificaat wilt maken om de RIPM te identificeren.

1b. KVM-encryptie

Met deze optie beheert u de encryptie van het RFB-protocol (Remote Frame Buffer protocol). De externe console gebruikt RFB om de schermgegevens naar de machine van de beheerder te sturen en de toetsenbord- en muisgegevens terug naar de host. Als deze functie is ingesteld op “Uit”, wordt er geen encryptie gebruikt. Als deze functie is ingesteld op “Try” (Proberen), probeert de applet een gecodeerde verbinding te maken. Als er geen verbinding kan worden gemaakt, wordt er een ongecodeerde verbinding gebruikt. Als deze functie is ingesteld op “Force” (Forceren), probeert de applet een gecodeerde verbinding te maken. Als de verbinding mislukt, wordt er een foutrapport opgesteld.

2. IP-toelatingsbeleid

In dit onderdeel worden de instellingen m.b.t. het IP-toelatingsbeleid besproken. Dit toelatingsbeleid wordt gebruikt om de toegang te beperken voor een aantal herkende clients. Deze clients worden geïdentificeerd via het IP-adres waarmee zij toegang proberen te maken.

Waarschuwing: De instellingen voor controle van IP-toegang zijn uitsluitend van toepassing op de LAN-interface.

2a. Controle van IP-toelatingsbeleid inschakelen

Hiermee schakelt u het toelatingsbeleid op basis van IP-bronadressen in.

2b. Standaardbeleid

Deze optie neemt aangekomen IP-pakketten in behandeling die aan geen van de geconfigureerde regels voldoen. Deze kunnen worden geaccepteerd of verworpen.

Waarschuwing: Als u dit instelt op “DROP” (Verwerpen) terwijl u voor “ACCEPT” (Toelaten) geen regels hebt geconfigureerd, is de toegang tot het web front-end via LAN niet mogelijk. Om de toegang opnieuw in te schakelen kunt u de beveiligingsinstellingen wijzigen via de modem of door het IP-toelatingsbeleid tijdelijk uit te schakelen via de initiële configuratieprocedure.

2c. Regelnummer

Dit moet het nummer van een regel bevatten waarop de volgende opdrachten van toepassing zijn. Negeer dit veld wanneer u een nieuwe regel toevoegt.

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:35:32 AM

2d. IP/Mask

Hiermee bepaalt u het IP-adres of de reeks IP-adressen waarvoor de regel geldt. In de onderstaande voorbeelden staat het nummer dat is gekoppeld aan een IP-adres met een a " / ", voor het aantal geldige bits dat van het gegeven IP-adres zal worden gebruikt

192.168.1.22/32 komt overeen met IP-adres 192.168.1.22

192.168.1.0/24 komt overeen met alle IP-pakketten met bronadressen van 192.168.1.0 tot 192.168.1.255

0.0.0.0/0 komt overeen met alle IP-pakketten

2e. Beleid

Met behulp van de functie Beleid bepaalt u wat er met de overeenkomende pakketten moet gebeuren. U kunt deze accepteren of verwerpen.

Waarschuwing: De volgorde van de regels is belangrijk. De regels worden in oplopende volgorde gecontroleerd totdat er een regel overeenkomt. Alle regels onder de overeenkomende regel worden genegeerd. Het standaardbeleid wordt toegepast als er geen overeenkomende regel is gevonden.

2f. Een regel toevoegen

Voer het IP/mask in en stel het beleid in. Druk vervolgens op de knop "Append" (Toevoegen).

2g. Een regel invoegen

Voer het regelnummer en IP/mask in. Stel het beleid in. Druk vervolgens op de knop "Insert" (Invoegen).

2h. Een regel vervangen

Voer het regelnummer en IP/mask in. Stel het beleid in. Druk vervolgens op de knop "Replace" (Vervangen).

2i. Een regel verwijderen

Voer het regelnummer in en druk op de knop "Delete" (Verwijderen).

3. Gebruiker blokkeren

Met de functie Gebruiker blokkeren kan de beheerder de login van een bepaalde gebruiker uitschakelen als deze gebruiker zijn/haar wachtwoord een bepaald aantal keren verkeerd heeft ingevoerd. Ook de duur van de blokkering kan worden ingesteld.

3a. Maximum aantal mislukte logins

Voer het maximum aantal mislukte logins in waarna een gebruiker moet worden geblokkeerd. Laat dit veld leeg om de functie Maximum aantal mislukte logins uit te schakelen.

3b. Blokkeertijd

Dit zijn het aantal minuten waarna de gebruiker wordt geblokkeerd als hij of zij het maximum aantal mislukte logins heeft bereikt. Laat dit veld leeg om de gebruiker te blokkeren totdat hij of zij handmatig wordt gedeblokkeerd.

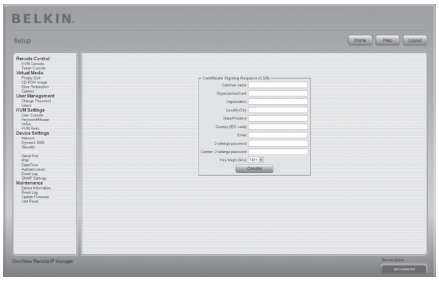
Gebruikers deblokkeren

Er zijn twee manieren om een geblokkeerde gebruiker te deblokkeren:

- Een medegebruiker kan de instellingen voor gebruikersbeheer openen (zie het hoofdstuk "Gebruikersbeheer") en voor deze gebruiker op de knop "Deblokkeren" drukken.
- Een beheerder kan de seriële console gebruiken voor de beginwaarden en inloggen als de "gedeblokkeerde" gebruiker. Het wachtwoord van de beheerder moet worden ingevoerd en er verschijnt een lijst met geblokkeerde gebruikers die kunnen worden gedeblokkeerd.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:35:33 AM

Certificaat



Certificaat instellen

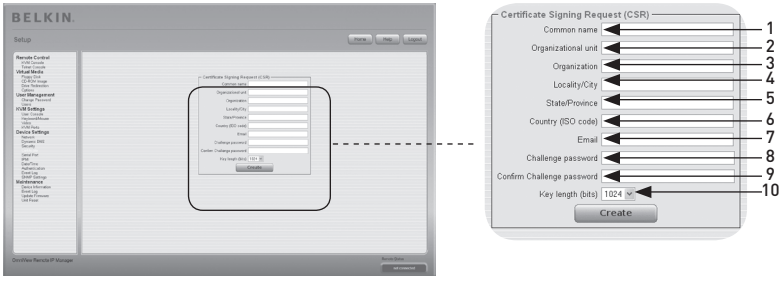
De RIPM gebruikt het SSL-protocol (Secure Socket Layer) voor al het gecodeerde netwerkverkeer tussen de RIPM en verbonden clients. Bij het maken van verbindingen moet de RIPM zijn identiteit kenbaar maken aan clients die gebruik maken van een cryptografisch certificaat. Standaard is dit certificaat en de onderliggende geheime sleutel gelijk voor alle geproduceerde RIPM's en zal niet overeenkomen met de netwerkconfiguratie die wordt toegepast op de RIPM door de gebruiker. De onderliggende geheime sleutel wordt ook gebruikt voor het beveiligen van de SSL-handshake. Het is mogelijk om een nieuw uniek 64 x.509-basiscertificaat dat specifiek is voor de RIPM te genereren en te installeren. Hierdoor kan de externe IP-console een nieuwe cryptografische sleutel en het daaraan verbonden CSR, "Certificate Signing Request" (Verzoek ondertekening certificaat) genereren dat door een officiële CA, "Certification Authority" (certificeringsinstantie) moet worden goedgekeurd. Een CA controleert uw identiteit en kent een gewaarmerkt SSL-certificaat toe. U maakt en installeert een SSL-certificaat voor de RIPM als volgt:

- Maak een SSL CSR aan met behulp van het onderstaande scherm. Vul de velden in die hieronder worden toegelicht. Hierna klikt u op de knop "Aanmaken" om het CSR te initiëren. U kunt het CSR naar uw beheersysteem downloaden met de knop "Download CSR" (Downloaden CSR).
- Verstuur het opgeslagen CSR naar een CA voor certificering. U ontvangt het nieuwe certificaat van de certificeringsinstantie.
- Upload het certificaat naar de RIPM met de knop "Create"(Creëren).

Nadat u deze drie stappen hebt voltooid, is de RIPM voorzien van een eigen certificaat waarmee de kaart door de bijbehorende clients wordt geïdentificeerd.

Waarschuwing: Als u het CSR op de RIPM vernietigt, kunt u het op geen enkele wijze herstellen! Herhaal de bovenstaande drie stappen als u het certificaat per ongeluk verwijderd.

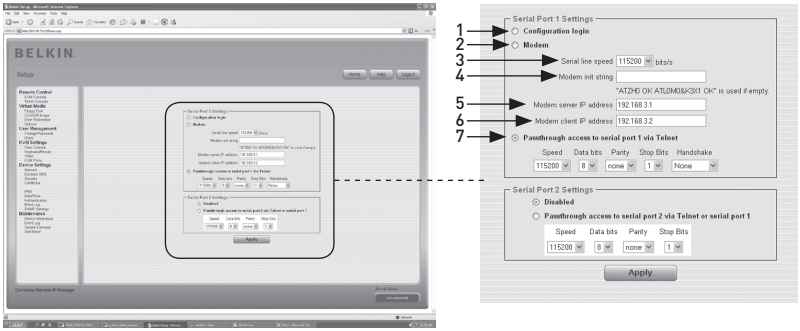
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:35:33 AM



1. **Algemene naam**
   Dit is de netwerknaam van de RIPM nadat deze in het netwerk van de gebruiker is geïnstalleerd (meestal de volledige toegekende domeinnaam). Deze is identiek aan de naam die wordt gebruikt om toegang te krijgen tot de RIPM met behulp van een webbrowser, maar zonder het voorvoegsel “http://”. Als de RIPM wordt geopend met behulp van HTTPS en de gegeven naam en de werkelijke netwerknaam verschillen, verschijnt er een pop-upvenster in de browser met een waarschuwing.
2. **Organisatie-eenheid**
   Dit veld wordt gebruikt om aan te geven tot welke afdeling binnen een organisatie de RIPM behoort.
3. **Organisatie**
   Naam van de organisatie waartoe de RIPM behoort.
4. **Plaats/Stad**
   Plaats waar de organisatie is gevestigd.
5. **Staat/Provincie**
   Staat of provincie waar de organisatie is gevestigd.
6. **Land (ISO-code)**
   Het land waar de organisatie is gevestigd (een uit twee letters bestaande ISO-code, bijv. US voor USA).
7. **Identiteitswachtwoord**
   Sommige certificeringsinstanties vereisen een identiteitswachtwoord om latere wijzigingen van het certificaat goed te keuren (bijvoorbeeld herroeping van het certificaat). Dit wachtwoord moet minstens vier tekens bevatten.
8. **Identiteitswachtwoord bevestigen**
   Bevestiging van het bovenstaande wachtwoord.
9. **E-mail**
   E-mailadres van een met de beveiliging belaste contactpersoon die voor de RIPM verantwoordelijk is.
10. **Sleutellengte**
    Dit is de lengte van de gegenereerde sleutel in bits. In de meeste gevallen is 1024 bits voldoende. Grotere sleutels kunnen bij het tot stand brengen van verbindingen een tragere reactie van de externe IP-console veroorzaken.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:35:33 AM

Seriële poort



Met de seriële instellingen van de RIPM kunt u opgeven welke apparaten met de seriële poort zijn verbonden en hoe u ze gebruikt. Er is een null-modemkabel vereist om verbinding te maken met de seriële interface.

1. **Configuratie of Console login**
   Gebruik de seriële poort niet voor speciale functies, maar uitsluitend voor de initiële configuratie.
2. **Modem**
   Naast de standaardtoegang via de ingebouwde Ethernet-adapter kan de RIPM ook via een telefoonverbinding op afstand worden geopend. De modem moet aangesloten zijn op de seriële interface van de RIPM. Het tot stand brengen van een verbinding met de externe IP-console via een telefoonlijn is niets anders dan het opbouwen van een specifieke vastelijnverbinding tussen de computer van uw consolecomputer en de RIPM. De RIPM fungeert dus als internetserviceprovider (ISP) die u kunt bellen. De verbinding komt tot stand met het Point-to-Point Protocol (PPP). Zorg ervoor dat u de consolecomputer correct configureert voordat u verbinding maakt met de RIPM. Op Windows besturingssystemen kunt u bijvoorbeeld een inbelnetwerkverbinding configureren die standaard op de juiste instellingen als PPP is ingesteld. Met het scherm modeminstellingen kunt u de toegang via een modem op afstand tot de RIPM configureren. De betekenis van elke parameter wordt hieronder beschreven. De modeminstellingen zijn onderdeel van het scherm voor seriële instellingen.
3. **Snelheid seriële lijn**
   Snelheid waarmee de RIPM met de modem communiceert. De meeste modems ondersteunen tegenwoordig de standaardsnelheid van 115200 bps. Probeer deze snelheid te verlagen als u een oudere modem gebruikt en problemen ondervindt.
4. **Initialisatiestring modem**
   Door de RIPM gebruikte initialisatiestring voor het opstarten van de modem. De standaardwaarde is geschikt voor alle huidige modems die rechtstreeks op een telefoonlijn zijn aangesloten. Als u een speciale modem hebt of een modem die verbonden is met een lokale telefoonswitch die een speciale belvolgorde vraagt om een verbinding met het openbare telefoonnet tot stand te brengen, kunt u deze instelling wijzigen door een nieuwe string in te geven. Raadpleeg de handleiding van de modem voor de AT opdrachtensyntaxis.

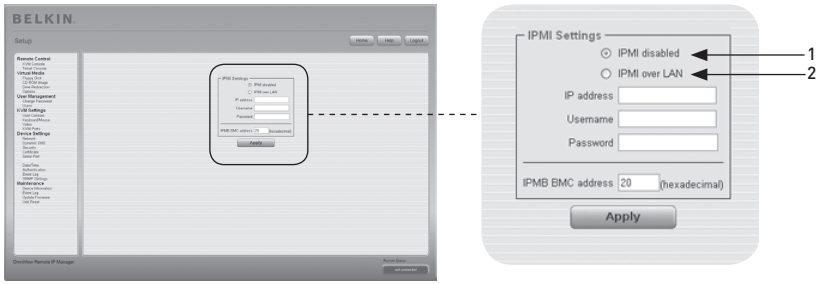
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:35:34 AM

5. **IP-adres modemserver**
   Dit IP adres wordt tijdens de PPP handshake aan de RIPM toegewezen. Omdat het een point-to-point IP-verbinding betreft, is vrijwel elk IP-adres mogelijk. Wel moet u ervoor zorgen dat dit niet interfereert met de IP-instellingen van de RIPM en de consolecomputer. Meestal is de standaardwaarde voldoende.
6. **IP-adres modemclient**
   Dit IP-adres wordt tijdens de PPP handshake aan de consolecomputer van uw RIPM toegewezen. Omdat het een point-to-point IP-verbinding betreft, is vrijwel elk IP-adres mogelijk. Wel moet u ervoor zorgen dat dit niet interfereert met de IP-instellingen van de RIPM en de consolecomputer. Meestal is de standaardwaarde voldoende.
7. **Pass-through toegang tot seriële poort via Telnet**
   Met deze optie is het mogelijk een willekeurig apparaat met de seriële poort te verbinden en deze via Telnet te openen (mits de terminal wordt ondersteund). Selecteer de betreffende opties voor de seriële poort en gebruik de Telnet-console of een standaard Telnet-client om verbinding te maken met de RIPM. Raadpleeg het hoofdstuk “Telnet-console” voor meer informatie over de Telnet-interface.

   Let op: Ga naar www.belkin.com voor een lijst met compatibele modems.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:35:34 AM

Intelligent Platform Management Interface (IPMI)



De RIPM IPMI voorzieningen bieden een manier om het systeem aan of uit te zetten of een harde reset uit te voeren. Bovendien kunt u een gebeurtenissenlogboek van het hostsysteem en de status van sommige systeemsensoren (zoals temperatuursensor) bekijken. Als uw hostsysteem IPMI ondersteunt, hebt u op de volgende manier toegang tot deze functie:

- IPMI over LAN (hiervoor is IPMI-versie 1.5 vereist)
- IPMI-instellingen

In de afbeelding hierboven worden de RIPM IPMI-instellingen weergegeven. De verschillende opties worden hieronder beschreven.

1.

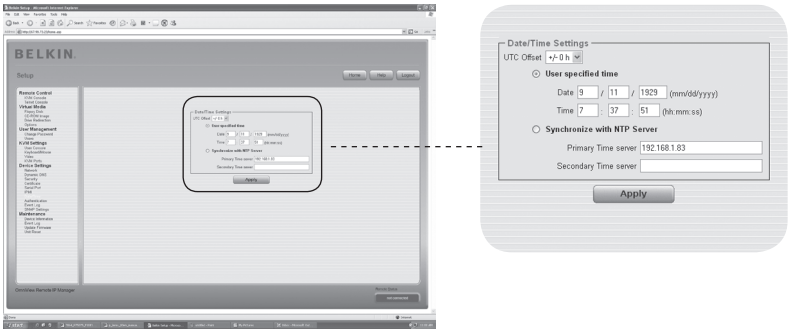
IPMI uitgeschakeld
Hiermee wordt de IPMI op de RIPM uitgeschakeld. Dit betekent dat de functies Status via IPMI en Gebeurtenissenlogboek via IPMI niet beschikbaar zijn; de functies voor stroom aan/uit en de resetfuncties maken geen gebruik van IPMI maar van ATX (Advanced Technology Extended) en de resetkabel van de RIPM is verbonden met het moederbord.

2.

IPMI over LAN
U kunt de IPMI ook via een LAN-verbinding aansluiten. Voor dit type toegang is een hostsysteem met IPMI v1.5 en een netwerkadapter side-bandverbinding aan de baseboard management controller (BMC, meestal on board) vereist. U moet het IP-adres van het bijbehorende hostsysteem en het correcte wachtwoord voor de LAN-verbinding in de IPMI-instellingen invoeren. U kunt ook toegang tot andere IPMI-systemen instellen door de bijbehorende IP-adressen in te voeren.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:35:35 AM

Datum en tijd

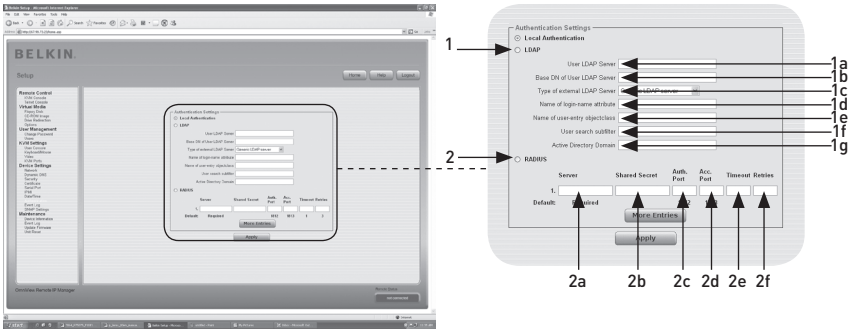


Deze link opent een pagina waar u de interne real-time klok van de RIPM kunt instellen. U kunt de klok handmatig aanpassen of een Network Time Protocol (NTP) tijdserver gebruiken. Wanneer u geen gebruik maakt van een tijdserver is de tijdinstelling niet definitief en moet u elke keer de tijd instellen wanneer de RIPM langer dan een paar minuten stroom verliest. U kunt een NTP-tijdserver gebruiken om dit te voorkomen. Met deze tijdserver kunt u de interne klok automatisch gelijkstellen met de huidige Coordinated Universal Time (CUT). Omdat de NTP-tijdserver altijd de CUT-tijd geeft, kunt u een statische verschuiving gebruiken om uw lokale tijd in te stellen.

Waarschuwing: Er bestaat momenteel nog geen manier om de zomertijd automatisch aan te passen. U moet de CUT-verschuiving tweemaal per jaar aanpassen aan de lokale tijd.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:35:35 AM

authentificatie



U kunt een lokale authentificatie gebruiken of deze gegevens bewaren in een centrale Lightweight Directory Access Protocol (LDAP) of een Remote Authentication Dial-In User Service (RADIUS) server. Voor het gebruik van LDAP of RADIUS moet u enkele gegevens in het scherm Authentificatie-instellingen invoeren. Zie hieronder voor meer informatie over de instellingen voor LDAP en RADIUS.

1. LDAP

1a. Gebruiker LDAP-server
Voer de naam of het IP-adres van de LDAP-server in die alle gebruikersinvoer bevat. Als u kiest voor een naam in plaats van een IP-adres, moet u een DNS-server in de netwerkinstellingen configureren.

1b. Basis DN van gebruiker LDAP-server
Geef de distinguished name (DN) op waar de boomdirectory in de LDAP-server van de gebruiker start.

1c. Type externe LDAP-server
Hiermee stelt u het type van de externe LDAP-server in. Dit is nodig omdat sommige servertypen een speciale verwerking vereisen. De standaardwaarden voor het LDAP-schema worden hieraan aangepast. U kunt kiezen tussen Generic LDAP Server, Novell Directory Service en Microsoft Active Directory. Kies Generic LDAP Server en stel het LDAP-schema in (zie hieronder) als u niet beschikt over Novell Directory Service of Microsoft Active Directory.

1d. Naam van de Loginnaam toewijzing
Dit is de naam van de toewijzing met de unieke loginnaam van de gebruiker. Laat dit veld leeg als u de standaardinstelling wilt gebruiken. De standaardinstelling is afhankelijk van de geselecteerde LDAP-server.

1e. Naam van gebruikersinvoer Object Class
Dit is de object class waarmee een gebruiker in de LDAP-directory wordt geïdentificeerd. Laat dit veld leeg als u de standaardinstelling wilt gebruiken. De standaardinstelling is afhankelijk van de geselecteerde LDAP-server.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:35:36 AM

1f. Subfilter zoekactie gebruikers
Hier kunt u een zoekactie naar gebruikers die bekend moeten zijn binnen de RIPM verfijnen.

1g. Active Directory-domein
Deze optie geeft het active directory-domein weer die in de Microsoft Active Directory server is geconfigureerd. Deze optie is uitsluitend geldig als u hebt gekozen voor Microsoft Active Directory LDAP-servertype.

2. Remote Authentication Dial In User Service (RADIUS)
RADIUS is een protocol dat door de werkgroep Internet Engineering Task Force (IETF) is gespecificeerd. De RADIUS-protocolsuite bestaat uit twee specificaties: Authentificatie en accountbeheer. Deze specificaties hebben als doel de authentificatie, configuratie en het accountbeheer voor dial-in services naar een onafhankelijke server te centraliseren. Het RADIUS-protocol kent verschillende implementaties, zoals gratis RADIUS, open-RADIUS of RADIUS voor UNIX-systemen. Het RADIUS-protocol is goed gespecificeerd en getest. Wij kunnen alle bovenstaande producten aanraden en in het bijzonder de gratis RADIUS implementatie.

Let op: Wij ondersteunen momenteel geen “challenge/response”. Een “Access Challenge” response wordt gezien en geëvalueerd als een “Access Reject”.

U moet inloggen om toegang te krijgen tot het externe apparaat via het RADIUS-protocol. Er wordt gevraagd naar uw gebruikersnaam en wachtwoord. De RADIUS-server leest de ingevoerde gegevens (Authentificatie) en de RIPM zoekt uw profiel op (Autorisatie). Dit profiel bevat de definities (of limieten) van uw handelingen en kan verschillen afhankelijk van uw specifieke situatie. Als er geen profiel bestaat, is toegang via RADIUS niet mogelijk. M.b.t. de externe activiteit, werkt de inlogprocedure via RADIUS hetzelfde als bij de externe console. De verbinding met de RIPM wordt onderbroken en afgesloten als er gedurende een halfuur geen activiteit plaatsvindt.

2a. Server
Voer het IP-adres van de hostnaam of de RADIUS-server in waarmee verbinding moet worden gemaakt. De DNS moet zijn geconfigureerd en ingeschakeld als u de
hostnaam gebruikt.

2b. Shared Secret
Een shared secret is een tekststring die fungeert als wachtwoord tussen de RADIUS-client en de RADIUS-server. De RIPM fungeert als een RADIUS-client. Een shared secret wordt gebruikt om te controleren of RADIUS-berichten door een RADIUS-enabled apparaat, dat met dezelfde shared secret is geconfigureerd, worden verzonden en om te controleren of de RADIUS-berichten niet worden gewijzigd tijdens de overdracht (om de integriteit van het bericht te controleren). U kunt gebruik maken van standaard alfanumerieke en speciale karakters voor de shared secret. Een shared secret kan maximaal 128 tekens bevatten in zowel kleine letters als hoofdletters (A–Z, a–z), getallen (0–9) en andere symbolen (tekens die niet zijn gedefinieerd als letters of getallen), zoals uitroeptekens (“ ! ”) of asterisken (“ * ”).

2c. Authentication Port
The port the RADIUS server listens to for authentication requests. De standaardwaarde is #1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:35:36 AM

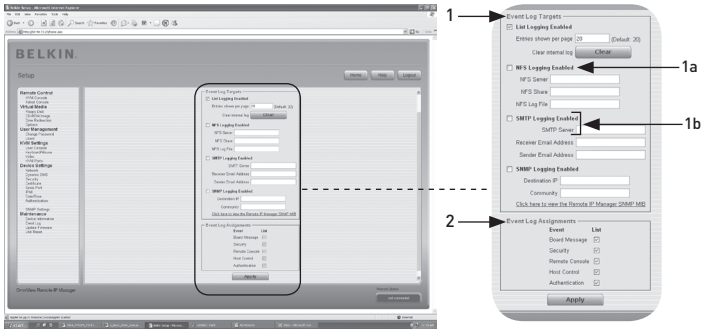
2d. Accountpoort
De poort van de RADIUS-server luistert naar accountverzoeken. De standaardwaarde is #1813.

2e. Time-out
Hiermee stelt u de time-to-live-aanvraag in seconden in. De time-to-live is de wachttijd voor het voltooien van de aanvraag. Als de aanvraag niet wordt voltooid binnen de ingestelde tijdslimiet, wordt deze geannuleerd. De standaardwaarde is één seconde.

2f. Nieuwe pogingen
Hiermee stelt u het aantal nieuwe pogingen in als een aanvraag niet kan worden voltooid. De standaardwaarde is driemaal.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:35:36 AM

Gebeurtenissenlogboek



Belangrijke gebeurtenissen zoals mislukte inlogpogingen of een update van de firmware worden opgenomen in een selectie logbestemmingen (zie Afbeelding 6-33). Elke gebeurtenis behoort tot een groep gebeurtenissen, die afzonderlijk kunnen worden geactiveerd. De normale manier om gebeurtenissen bij te houden is het gebruik van het interne logboek van de RIPM. Klik op “Event Log” (Gebeurtenissenlogboek) op de pagina Onderhoud om de lijst met gebeurtenissen te bekijken. Bij de instellingen voor het gebeurtenissenlogboek kunt u kiezen hoeveel gebeurtenissen op de pagina worden weergegeven. U kunt het logbestand ook leegmaken.

1. **Bestemmingen gebeurtenissenlogboek**
   U kunt het interne logboek van de RIPM gebruiken om gebeurtenissen bij te houden. Klik op “Event Log” (Gebeurtenissenlogboek) op de pagina “Onderhoud” om de lijst met gebeurtenissen te bekijken. Omdat het systeemgeheugen van de RIPM wordt gebruikt om alle gegevens op te slaan, is het maximum aantal gebeurtenissenlogs beperkt tot 1000 gebeurtenissen per loglijst. Bij elke invoer die het maximum overschrijdt, wordt de oudste invoer verwijderd.

Waarschuwing: Als de resetknop op de HTML front-end wordt gebruikt om de RIPM te herstarten, worden alle loggegevens permanent bewaard zodat deze beschikbaar zijn nadat de RIPM opnieuw is opgestart. Als de stroomvoorziening naar de RIPM wordt onderbroken of er een harde herstart wordt uitgevoerd, gaan alle loggegevens verloren. Gebruik één van de hieronder beschreven logmethoden om dit te voorkomen.

1a. Network File System (NFS) Logging ingeschakeld
Definieer een NFS-server waar de directories en statische links naartoe moeten worden geëxporteerd; alle loggegevens worden vervolgens in een bestand naar die locatie geschreven. U moet voor elk apparaat een unieke bestandsnaam definiëren om de loggegevens vanaf meerdere RIPM-apparaten naar één enkele NFS-share te schrijven. Wanneer u de NFS-instellingen wijzigt en op de knop “Apply” (Toepassen) drukt, wordt de NFS onmiddellijk opgebouwd. Dit betekent dat de NFS-share en de NFS-server moeten worden gevuld met geldige bronnen, anders verschijnt er een foutmelding.

Let op: In tegenstelling tot het interne logbestand van de RIPM, is de grootte van het NFS-logbestand onbeperkt. Elke loggebeurtenis wordt onderaan het bestand toegevoegd waardoor dit voortdurend groter wordt. U kunt regelmatig loggebeurtenissen binnen het bestand verwijderen of verplaatsen.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:35:37 AM

1b. SNMP-instellingen

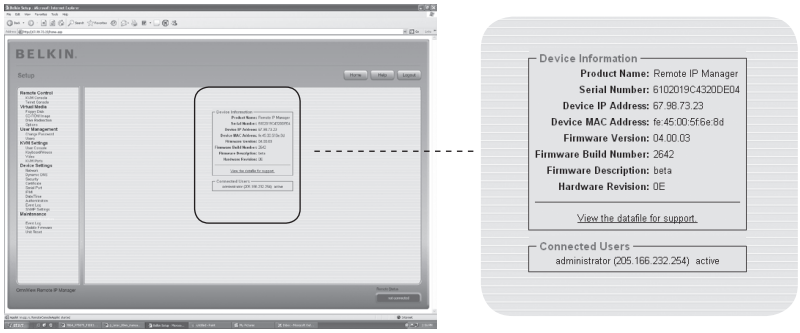
Simple Mail Transfer Protocol (SMTP) Logging ingeschakeld
Dankzij deze optie kunt u met de RIPM e-mailberichten verzenden naar een adres dat is ingevoerd in het tekstveld E-mailadres in de instellingen voor het gebeurtenissenlogboek. Deze e-mailberichten bevatten dezelfde beschrijvingstrings als het interne logbestand en het onderwerp van het bericht wordt gevuld met de groep gebeurtenissen van de betreffende loggebeurtenis. U moet een SMTP-server opgeven die bereikbaar is vanaf de RIPM en waarvoor geen authentificatie (<serverip>:<port>) nodig is om deze logbestemming te kunnen gebruiken.

SNMP Logging ingeschakeld
Als deze functie is ingeschakeld, wordt er elke keer dat er een loggebeurtenis plaatsvindt een SNMP-valkuil verzonden vanaf de RIPM naar een opgegeven IP-adres. Als de ontvanger een community-string vereist, kunt u deze in het daarvoor bestemde veld instellen. De meeste gebeurtenissen-valkuilen bevatten slechts een omschrijvende string die alle gegevens over de loggebeurtenis bevat. Authentificatie en voeding van de host zijn voorzien van een eigen valkuil die automatisch wordt aangemaakt en bestaat uit verschillende velden met gedetailleerde gegevens over de gebeurtenis. Gebruik elke willekeurige SNMP trap listener om deze SNMP-valkuil te ontvangen.

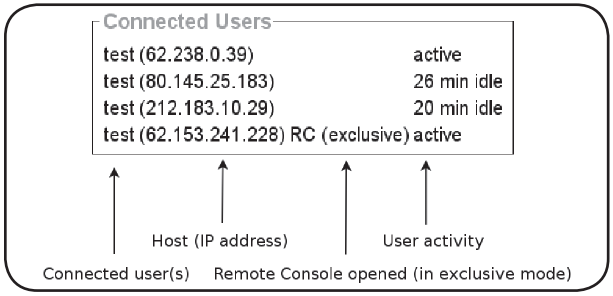
2. **Toewijzingen gebeurtenissenlogboek**
U kunt selecteren welke handelingen van de RIPM moeten worden opgeslagen in het logbestand. Selecteer het (de) gewenste selectievakje(s) en druk op “Apply” (Toepassen) om uw selectie te bevestigen.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:35:37 AM

Apparaatgegevens



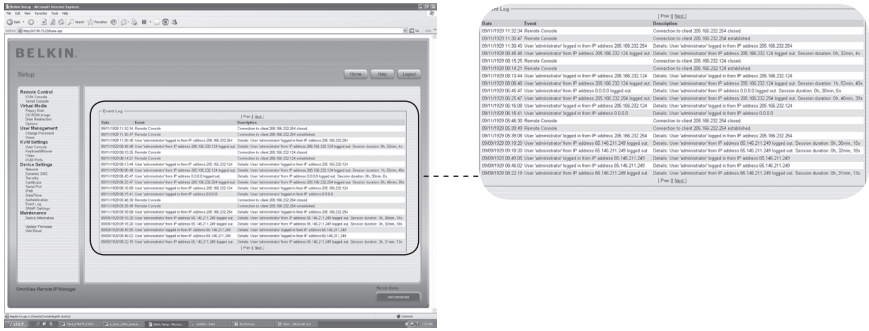
Dit hoofdstuk bevat een samenvatting van de informatie over deze RIPM en zijn huidige firmware waarmee u de RIPM kunt resetten. Met het gegevensbestand voor ondersteuning kunt u het RIPM-gegevensbestand met de specifieke gegevens voor ondersteuning downloaden. Het bestand is een eXtensible Markup Language (XML)-bestand met aangepaste gegevens voor ondersteuning (zoals het serienummer).



In de afbeelding hierboven wordt de activiteit van de RIPM weergegeven. Van links naar rechts geeft het scherm de aangesloten gebruiker(s), het IP-adres van de gebruiker van de host en de activiteitstatus van de RIPM weer. “RC” betekent dat de externe console geopend is. Als de externe console in de “exclusieve modus” is geopend, wordt de term “(exclusieve modus)” toegevoegd. Raadpleeg het hoofdstuk “Stuurbalk van de externe console” op pagina 23 van deze handleiding voor meer informatie over deze optie. De laatste kolom bevat de term “active” (actief) om aan te geven dat er een actieve gebruiker is, of de term “20 min. idle” om aan te geven dat een gebruiker gedurende een bepaalde tijd inactief is geweest.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:35:37 AM

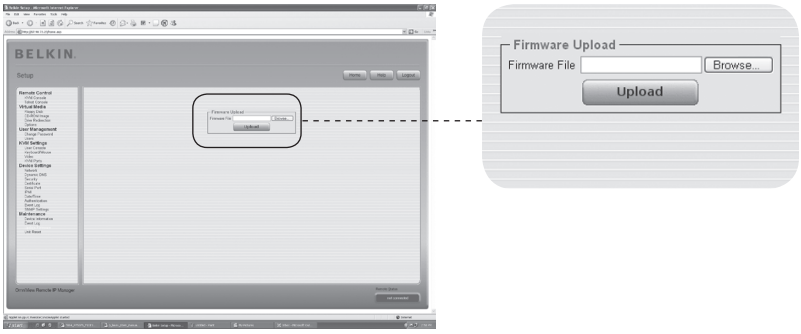
Gebeurtenissenlogboek



De lijst “Event Log” (Gebeurtenissenlogboek) bevat de gebeurtenissen die in de RIPM worden bewaard, aangevuld met de datum van de gebeurtenis, een korte beschrijving van de gebeurtenis en een IP-adres waarin de bron van de gebeurtenisaanvraag wordt weergegeven. U kunt de tekstknoppen “Prev” (Vorige) en “Next” (Volgende) gebruiken om door de gegevens te bladeren.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:35:38 AM

Firmware bijwerken



De RIPM is een volledig standalone computer die is voorzien van firmware. Deze firmware wordt geladen in het read-only memory (ROM). U kunt de firmware van de RIPM op afstand bijwerken om nieuwe of verbeterde functionaliteit of speciale functies toe te voegen. Een nieuwe update van de firmware bestaat uit een binair bestand dat u van de Belkin website kunt downloaden. U moet het bestand uitpakken als het firmwarebestand gecomprimeerd is (in geval van een zip-bestand). U kunt WinZip (te downloaden vanaf http://www.winzip.com/) gebruiken om uw firmware-updates in het Windows-besturingssysteem uit te pakken.
Let op: U moet het nieuwe, uitgepakte firmwarebestand opslaan op de computer die is verbonden met de RIPM om de firmaware bij te werken.

Het bijwerken van de firmware bestaat uit drie stappen:

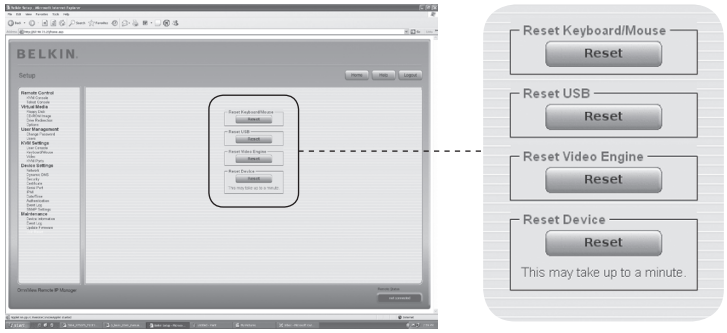
1. Het nieuwe firmwarebestand uploaden naar de RIPM. Selecteer het bestand op uw lokale systeem met behulp van de knop “Browse” (Bladeren) in het scherm “Upload Firmware” (Firmware uploaden). Klik vervolgens op “Upload” (Uploaden) om het geselecteerde bestand vanaf uw lokale systeem naar de RIPM te uploaden. Nadat het firmwarebestand is binnengehaald, controleert de RIPM automatisch de geldigheid en bevestigt dat er geen overdrachtsfouten zijn opgetreden. Als er een fout optreedt, wordt de functie “Firmware uploaden” geannuleerd en blijft de huidige firmware intact.
2. Als het uploaden met succes wordt voltooid (wat meestal het geval is), verschijnt het scherm “Update Firmware” (Firmware bijwerken) In het scherm wordt het versienummer van de huidige firmware en het versienummer van de nieuwe firmware weergegeven Klik op “Update” (Bijwerken) om de oude versie te vervangen door de nieuwe.

   Waarschuwing: Dit proces is onomkeerbaar en neemt enkele minuten in beslag. Zorg ervoor dat de stroomtoevoer naar de RIPM’s niet wordt onderbroken tijdens het bijwerken. Dit kan leiden tot instabiliteit van de RIPM.
3. Nadat de firmware is bijgewerkt, wordt de RIPM automatisch opnieuw opgestart. Na ongeveer één minuut verschijnt de inlogpagina en kunt u weer inloggen.

   Waarschuwing: Deze update van de firmware in drie stappen en de volledige consistentiecontrole maken de firmware nagenoeg volledig bestand tegen fouten. Toch is het van belang dat uitsluitend ervaren medewerkers of beheerders het bijwerken van de firmware uitvoeren. Het is van cruciaal belang dat de stroomtoevoer naar de RIPM NIET wordt onderbroken tijdens het bijwerken.

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:35:39 AM

Apparaat resetten



In dit hoofdstuk worden de methoden voor het resetten van onderdelen van het apparaat beschreven. Dit heeft betrekking op het toetsenbord en de muis, het videoscherm van de computer dat is verbonden met de RIPM en de RIPM zelf. Om de nieuwe bijgewerkte firmware te activeren moet de RIPM opnieuw worden opgestart. Tijdens dit proces worden automatisch alle huidige aansluitingen met de administratieconsole gedurende dertig seconden afgesloten. Het resetten van sub-apparaten (zoals de video-engine) neemt slechts enkele seconden in beslag en heeft geen onderbreking van de aansluitingen tot gevolg. Klik op de knop “Reset”, zoals hierboven weergegeven, om een specifieke reset van de RIPM uit te voeren.

Let op: Uitsluitend de beheerder mag de RIPM resetten.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:35:39 AM

De externe muis werkt niet of is niet synchroon.

Controleer allereerst de VGA-aansluiting. Zowel de RIPM als de lokale monitor moeten dezelfde videoresoluties ondersteunen. Zorg ervoor dat uw muisinstellingen overeenkomen met uw muismodel (PS/2 of USB). Zorg er ook voor dat het muismodel is ingesteld in de RIPM en het besturingssysteem van de host (de computer die is aangesloten op de RIPM). In sommige gevallen kunnen er tijdens het proces van de muissynchronisatie fouten optreden. Raadpleeg het onderdeel “Muis-, toetsenbord- en videoconfiguratie” in hoofdstuk 3 voor meer informatie.

De beeldkwaliteit is slecht of het beeld is korrelig.

Gebruik de menu-invoer “Resetten” om de RIPM-instellingen terug te zetten naar de standaardwaarden. Klik vervolgens op de knop “Auto-Adjust” (Automatisch instellen) om de bijbehorende video-uitgang te selecteren. Controleer of alle videokabels goed zijn aangesloten.

Het inloggen op de RIPM lukt niet.

Controleer uw gebruikersnaam en wachtwoord. De standaardgebruikersnaam is “administrator” en het standaardwachtwoord is “belkin”. Zorg ervoor dat uw webbrowser zo is ingesteld dat cookies worden geaccepteerd.

Het scherm van de externe console van de RIPM kan niet worden geopend.

Controleer of Java is geladen. Het is mogelijk dat een firewall de toegang tot de externe console onmogelijk maakt. De TCP-poorten #80 (voor HTTP) en #443 (voor HTTPS en RFB) moeten openstaan (de server waarop de firewall is geïnstalleerd moet binnenkomende TCP-verbindingen op deze poorten accepteren).

De externe console kan geen verbinding maken en er verschijnt een time-outmelding.

Controleer de hardware en netwerkinstallatie. Als er zich een proxyserver tussen de RIPM en uw host bevindt, kan het zijn dat er geen videogegevens kunnen worden verzonden via een RFB-verbinding. Sluit de RIPM rechtstreeks aan op de client. Controleer bovendien de instellingen van de RIPM en kies een andere serverpoort voor RFB-overdracht. Controleer de bijbehorende poort voor binnenkomende verbindingen als u een firewall gebruikt. U kunt deze verbindingen beperken tot de IP-adressen die door de RIPM en uw client worden gebruikt.

Er kan geen verbinding worden gemaakt met de RIPM.

Controleer uw hardware. Is de RIPM aangesloten op een netvoeding? Controleer uw netwerkconfiguratie (IP-adres, router). Verzend een “ping”-verzoek naar de RIPM om te controleren of de RIPM bereikbaar is via het netwerk.

Speciale toetsencombinaties zoals ALT+F2 en ALT+F3 worden door de console onderschept en niet naar de host doorgestuurd.

Definieer een zogenaamde “button key”. Dit kunt u doen bij de instellingen van de externe console (raadpleeg het hoofdstuk “Stuurbalk van de externe console” op pagina 23).

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:35:39 AM

De webpagina's van de RIPM worden niet correct weergegeven.

Controleer de cache-instellingen van uw browser. Verzeker u ervan dat de cache-instellingen NIET zijn ingesteld op "nooit controleren op nieuwere pagina's". Als die instelling is ingeschakeld, kan het zijn dat de pagina's van de RIPM vanuit het cache-geheugen van uw browser en niet vanuit de RIPM worden geladen en daardoor dit probleem veroorzaken.

Windows XP kan niet worden geactiveerd vanuit de standby-modus.

Dit is mogelijk een probleem binnen Windows XP. Probeer de muisaanwijzer niet te bewegen terwijl XP in de standby-modus gaat. Raadpleeg de handleiding van uw besturingssysteem voor meer informatie.

Telkens ik het dialoogvenster Externe console open, zijn de muisaanwijzers niet meer synchroon.

Schakel de instelling "Automatically move mouse pointer to the default button of dialog boxes" (Automatisch de muisaanwijzer naar de standaard knop van de dialoogvensters laten gaan) in de muisinstellingen van uw besturingssysteem uit.

Het scherm van de externe console blijft zwart

Controleer of de RIPM uitsluitend stroom krijgt via USB. Als er niet genoeg stroom wordt geleverd via USB, wordt de externe console wel geopend maar blijft het scherm zwart. Controleer de RIPM-instellingen zoals beschreven op pagina 26 van deze handleiding. Controleer of alle videokabels goed zijn aangesloten.

De videogegevens van de lokale monitor zijn omlijnd door een zwarte rand.

Dit is geen storing. De lokale monitor is geprogrammeerd in een vaste videomodus die in de video-instellingen van de RIPM kan worden geselecteerd. Raadpleeg het hoofdstuk "Stuurbalk van de externe console" op pagina 23 van deze handleiding.

Ik ben mijn wachtwoord vergeten. Hoe kan ik de RIPM terugzetten naar de fabrieksinstellingen?

Hiervoor kunt u de seriële interface gebruiken: Raadpleeg het hoofdstuk "Fabrieksinstellingen voor IP-manager voor beheer op afstand resetten" op pagina 31 van deze handleiding.

Ga naar www.belkin.com voor aanvullende probleemoplossing en een lijst met hardware die compatibel is met de RIPM.

Let op: Neem contact op met onze afdeling Technische ondersteuning via 1-800-2BELKIN, als geen van deze tips uw probleem oplost.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:35:40 AM

FCC-verklaring

Attest van gelijkvormigheid met de FCC-voorschriften voor elektromagnetische compatibiliteit.

Wij, Belkin Corporation, gevestigd te 501 West Walnut Street, Compton, CA 90220, in de Verenigde Staten van Amerika, verklaren hierbij dat wij de volledige verantwoordelijkheid aanvaarden dat het product met het artikelnummer

F1DE101H

waarop deze verklaring betrekking heeft,
voldoet aan Deel 15 van de FCC-Voorschriften. Het gebruik ervan is onderworpen aan de volgende voorwaarden: (1) dit apparaat mag geen schadelijke storingen opwekken en (2) het apparaat moet elke ontvangen storing accepteren, waaronder storingen die een ongewenste werking kunnen veroorzaken.

CE-Gelijkvormigheidsattest
"Wij, Belkin Corporation, verklaren hierbij dat wij de volle verantwoordelijkheid aanvaarden dat het product met het artikelnummer F1DE101H, waarop deze verklaring van toepassing is, voldoet aan de emissienorm EN55022 en aan de immuniteitsnormen EN55024, LVP EN61000-3-2 en EN61000-3-3."

ICES
Dit digitale apparaat uit klasse B voldoet aan de Canadese normen ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Twee jaar beperkte productgarantie van Belkin Corporation

Deze garantie dekt het volgende.
Belkin Corporation garandeert de oorspronkelijke koper van dit Belkin-product dat het product vrij is van ontwerp-, assemblage-, materiaal- en fabricagefouten.

De geldigheidsduur van de dekking
Belkin Corporation biedt twee jaar garantie voor dit product.

Hoe worden problemen opgelost?
Productgarantie
Belkin zal het product dat een defect vertoont naar eigen goeddunken kosteloos (met uitzondering van transportkosten) repareren of vervangen.

Wat valt buiten deze garantie?
Alle hierin vermelde garanties zijn niet van toepassing als het product van Belkin niet ter beschikking is gesteld op verzoek van Belkin op kosten van de koper voor onderzoek door Belkin Corporation of als Belkin Corporation besluit dat het product van Belkin verkeerd is geïnstalleerd, op enige wijze is veranderd of vervalst. De Belkin productgarantie biedt geen bescherming tegen rampen(andere dan blikseminslag), zoals overstromingen, aardbevingen, oorlog, vandalisme, diefstal, normale slijtage, erosie, depletie, veroudering, misbruik, beschadiging door netspanningsdalingen (zg. "brown-outs" en "sags"), ongeoorloofde programmering en/of wijziging van de systeemapparatuur.

Hoe wordt service verleend?
Om service voor uw Belkin-product te verkrijgen gaat u als volgt te werk:

1. Neem binnen 15 dagen na het voorval contact op met de afdeling Customer Service van Belkin Corporation te 501 W. Walnut St., Compton CA 90220, afdeling Customer Service, of bel +1 (800)-223-5546 binnen 15 dagen na het voorval. Zorg ervoor dat u de volgende gegevens bij de hand hebt:
   a. Het artikelnummer van het Belkin-product.
   b. Waar u het product hebt gekocht.
   c. Wanneer u het product hebt gekocht.
   d. Het originele aankoopbewijs.
2. De medewerker/ster van de klantenservice van Belkin instrueert u vervolgens hoe u het aankoopbewijs en het product moet verzenden en hoe de claim verder wordt afgewikkeld.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:35:40 AM

Belkin Corporation behoudt zich het recht voor het defecte Belkin-product te onderzoeken. De kosten voor verzending van het Belkin-product naar Belkin Corporation zijn volledig voor rekening van de koper. Als Belkin naar eigen bevinding tot de conclusie komt dat het onpraktisch is de beschadigde apparatuur naar Belkin Corporation te verzenden, kan Belkin naar eigen goeddunken een deskundige reparatie-inrichting aanwijzen en deze opdragen de betreffende apparatuur te inspecteren en de reparatiekosten ervan te begroten. De eventuele verzendkosten van het product naar de reparatie-inrichting en van de terugzending naar de koper en van de kostenbegroting zijn geheel voor rekening van de koper. Het beschadigde product moet voor onderzoek beschikbaar blijven totdat de claim is afgehandeld. Belkin Corporation behoudt zich bij de vereffening van claims het recht voor in de plaats te treden bij alle geldige verzekeringspolissen waarover de koper van het product zou beschikken.

De garantie en de wet.
DEZE GARANTIE OMVAT DE ENIGE GARANTIE VAN BELKIN CORPORATION EN ER ZIJN GEEN ANDERE GARANTIES, NADRUKKELIJK OF TENZIJ WETTELIJK BEPAALD IMPLICIET, MET INBEGRIP VAN IMPLICIETE GARANTIES OF VOORZIENINGEN VAN KWALITEIT, VERHANDELBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL, EN ZULKE IMPLICIETE GARANTIES, MITS VAN TOEPASSING, ZIJN WAT HUN GELDIGHEID BETREFT BEPERKT TOT DE DUUR VAN DEZE GARANTIE.

In sommige staten of landen is het niet toegestaan de duur van impliciete garanties te beperken in welk geval de bovenstaande garantiebeperkingen wellicht niet voor u gelden.

ONDER TOEPASSELIJK RECHT IS BELKIN CORPORATION NIET AANSPRAKELIJK VOOR INCIDENTELE, BIJZONDERE, DIRECTE, INDIRECTE, BIJKOMENDE OF MEERVOUDIGE SCHADE WAARONDER, MAAR NIET BEPERKT TOT, SCHADE INGEVOLGE WINSTDERVING EN/OF GEMISTE OPBRENGSTEN VOORTVLOEIEND UIT DE VERKOOP OF HET GEBRUIK VAN BELKIN-PRODUCTEN, ZELFS ALS DE BETROKKENE OP DE HOOGTE WAS VAN DE MOGELIJKHEID VAN ZULKE SCHADE.

Deze garantie verleent u specifieke wettelijke rechten en wellicht hebt u andere rechten die van staat tot staat kunnen verschillen. In sommige staten en landen is het niet toegestaan incidentele schade, gevolgschade en andere schade uit te sluiten, daarom is het mogelijk dat de bovenstaande garantiebeperkingen voor u niet gelden.

Verwijdering van afvalmateriaal door huishoudens binnen de Europese Unie:
Dit symbool op het product of de verpakking geeft aan dat het product niet mag worden verwijderd met het huishoudelijk afval. Het is uw verantwoordelijkheid uw afgedankte apparatuur af te leveren op een aangewezen inzamelpunt voor de verwerking van afval van elektrische en elektronische apparatuur. De afzonderlijke inzameling en recyclage van uw afgedankte apparatuur draagt bij tot het sparen van natuurlijke bronnen en tot het hergebruik van materiaal op een wijze die de volksgezondheid en het milieu beschermt. Voor meer informatie over waar u uw afgedankte apparatuur kunt inleveren voor recyclage kunt u contact opnemen met het gemeentehuis in uw woonplaats, de reinigingsdienst of de winkel waar u het product hebt aangekocht.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:35:40 AM

BELKIN®

OmniView®
IP-manager voor beheer op afstand

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Verenigd Koninkrijk
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Nederland
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spanje
+34 9 16 25 80 00
+34 9 02 02 00 34 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, Frankrijk
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH
Hanebergstraße 2
80637 München, Duitsland
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

© 2006 Belkin Corporation. Alle rechten voorbehouden. Alle handelsnamen zijn geregistreerde handelsmerken van de betreffende rechthebbenden. Mac OS en Macintosh zijn handelsmerken van Apple Computer, Inc., die in de Verenigde Staten en andere landen zijn gedeponeerd.

P75075ea

BELKIN®

OmniView® Remote IP Manager

Control

Controle su ordenador o un conmutador KVM mediante un buscador de Internet, desde cualquier lugar

EN
FR
DE
NL
ES
IT

Manual del usuario

F1DE101Hea

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:35:41 AM

Índice de contenidos

Índice de contenidos

1-1 Introducción y contenido del paquete

Enhorabuena y gracias por haber adquirido este Remote IP Manager (RIPM) OmniView de Belkin. Diseñado para que las empresas puedan añadir de forma sencilla la tecnología KVM a través de IP a sus configuraciones de servidores y KVM existentes, el RIPM ofrece una manera eficiente de reducir drásticamente el tiempo de inactividad de los servidores y los costes de servicio técnico. Ahora, los administradores pueden solucionar los problemas más rápidamente mediante el acceso a distancia, en cualquier momento y cualquier lugar. El RIPM se configura de forma sencilla para que funcione con su área de red local (LAN) existente, sea grande o pequeña. Consulte este Manual del usuario para conocer todos los detalles que necesitará al instalar y manejar el RIPM, y consejos expertos para resolución de averías, en el improbable caso de que apareciese un problema. Sabemos valorar su negocio y estamos convencidos de que pronto podrá apreciar por usted mismo por qué se emplean más de 1 millón de productos OmniView de Belkin en todo el mundo.


OmniView Remote IP Manager


Kit de cables para PS/2


Cable VGA


DB9 Cable null


Cable Mini-USB


Una fuente de alimentación de 5 V CC, 2 A


Soporte para montaje en bastidor con tornillos


CD con software de instalación


Manual del usuario


Guía de instalación rápida

Tarjeta de registro

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:35:44 AM

- **Acceso remoto**
  El RIPM proporciona acceso remoto a su configuración KVM y todos los servidores conectados. También puede configurarse para proporcionar acceso remoto a un servidor u ordenador individual.

- **Usuarios digitales**
  El RIPM permite a un usuario digital acceder y controlar los servidores y conmutadores KVM conectados. También permite a otros 25 usuarios más ver la imagen digital simultáneamente, para resolución de problemas colectiva.

- **Basado en un buscador de Internet**
  La interfaz del RIPM está basada en un buscador de Internet, cualquier ordenador puede acceder a él, siempre que esté conectado a la red LAN, WAN o Internet mediante una conexión estándar TCP/IP. La configuración no requiere software adicional.

- **Interfaz de fácil utilización**
  La interfaz de sencilla utilización le permite configurar y cambiar las funciones del RIPM rápida y fácilmente mediante su buscador de Internet, sin necesidad de instalar software adicional en su ordenador.

- **Acceso al nivel de la BIOS**
  El RIPM le permite acceder al sistema básico de entrada y salida (BIOS) de sus servidores para realizar ajustes y reiniciar sistemas.

- **Compatible con dispositivo Serie**
  El RIPM puede conectarse a un dispositivo Serie, como una unidad de distribución de alimentación (PDU), así puede desconectar a distancia la corriente para reiniciar sus servidores.

- **Seguridad mejorada**
  El RIPM ofrece encriptación SSL de 256 bits y protección con contraseña para varios usuarios que impide el acceso no autorizado a los servidores.

- **Medios virtuales***
  Con la capacidad virtual-media, puede transferir imágenes y archivos entre los ordenadores remotos y local, cargar software a distancia, realizar parches en el sistema operativo y las aplicaciones, y llevar a cabo pruebas de diagnóstico con un CD.

*Disponible sólo para ordenadores con Windows®.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:35:44 AM

- **Gestión de cuenta**
  El RIPM permite que el administrador cree varias cuentas de usuario y controle el acceso a los servidores.

- **Registro de sucesos**
  El Registro de sucesos captura y almacena las actividades de todos los usuarios en el RIPM.

- **Notificación por correo electrónico**
  El RIPM permite al administrador controlar la actividad de los usuarios y enviar notificaciones por correo electrónico sobre accesos, intentos de acceso no válidos, y cierres de sesión.

- **Soporte de plataforma múltiple**
  El RIPM funciona con conmutadores KVM o servidores con conexiones de consola PS/2 o USB.

- **Resolución de vídeo**
  Con un ancho de banda de 117 MHz, el RIPM es capaz de ofrecer resoluciones de vídeo de hasta 1600 x 1200 a 75 Hz.

- **Montaje en bastidor 0U**
  El RIPM es lo suficientemente pequeño para poder colocarse en su mesa de trabajo o montado en la parte trasera de su bastidor de servidores, para montarlo en un espacio de 0U.

- **Actualizaciones del firmware**
  Las actualizaciones por flash le permiten obtener las últimas actualizaciones del firmware para su RIPM. Estas actualizaciones del firmware aseguran que el RIPM es compatible con los últimos dispositivos y hardware y son gratuitas durante toda la vida útil del RIPM. Visite www.belkin.com para obtener información sobre las actualizaciones y asistencia.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:35:44 AM

Requisitos de hardware

- Remote IP Manager Serie OmniView (incluido)
- Kit de cables para PS/2 (incluido)
- Cable VGA (incluido)
- Cable Mini-USB (incluido)
- Fuente de alimentación de 5 V CC, 2 A (incluida)
- Teclado, monitor y ratón
- Conexión a la red que utilice un puerto Ethernet 10/100Base-T (RJ45)
- Cable CAT5
- Soporte para montaje en bastidor con tornillos (incluido en la caja para la opción de montaje en bastidor)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:35:44 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x y superiores;
UNIX®; Mac OS® X v10.0 y superiores (se necesita KVM);
Sun™ Solaris™ 8.x y superiores (con Adaptador Sun, número de artículo de Belkin F1DE083)

Buscadores compatibles

- Microsoft® Internet Explorer 6.0 y superiores
- Netscape® Navigator® 7.0

P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:35:44 AM

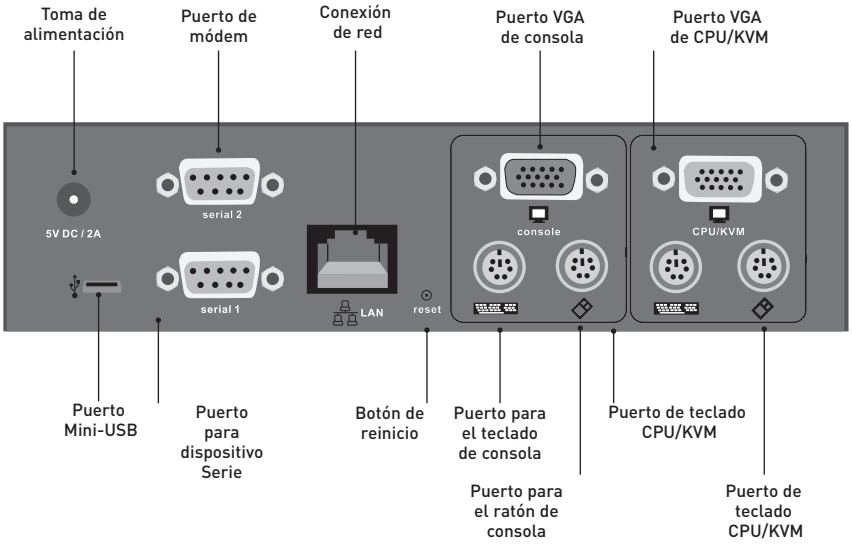
Número de artículo:	F1DE101H
Alimentación:	5V CC, 2 A
N° de usuarios admitidos:	1 local, 1 digital (1 usuario a la vez)
Emulación de teclado:	PS/2 y USB
Emulación de ratón:	PS/2 y USB
Monitores compatibles:	CRT y LCD (con soporte VGA)
Resolución válida:	Hasta 1600 x 1200 a 75 Hz
Ancho de banda remoto máximo:	5 MB
Entrada de teclado:	MiniDIN6 (PS/2)
Entrada de ratón:	MiniDIN6 (PS/2)
Puerto de monitor:	HDDB15 hembra (VGA)
Puerto USB CPU:	Mini USB
Conexión de red:	RJ45
Modos de cifrado:	SSL de 256 bits, 128 bits, AES, DES, 3DES
Soporte de autenticación:	LDAP (vía cliente LDAP local), RADIUS, AD
Soporte de protocolos:	SNMP v1, IPv4
Puerto para dispositivo Serie:	DB9
Indicadores LED:	2
Carcasa:	Metal
Dimensiones:	171 mm (ancho) x 44 mm (alto) x 114 mm (largo)
Peso:	0,75 kg
Temperatura de funcionamiento:	de 0° a 48,89° C
Temperatura de almacenamiento:	de -20° a 60° C
Humedad:	de 5% a 80%
Garantía:	2 años

Nota: Las especificaciones pueden ser objeto de modificación sin previo aviso.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:35:44 AM

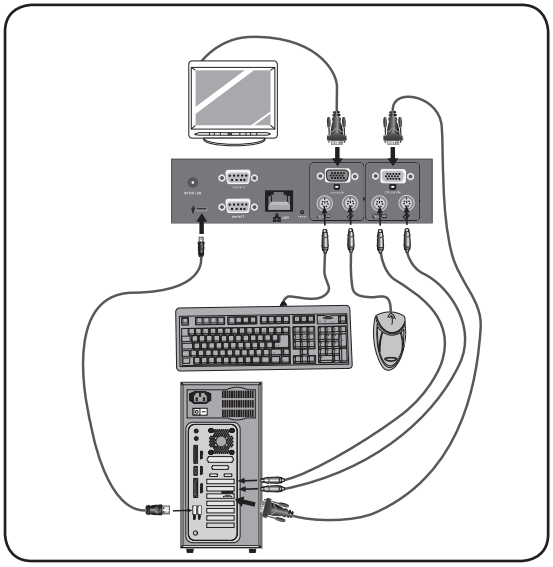
Parte delantera de la unidad

Parte posterior de la unidad

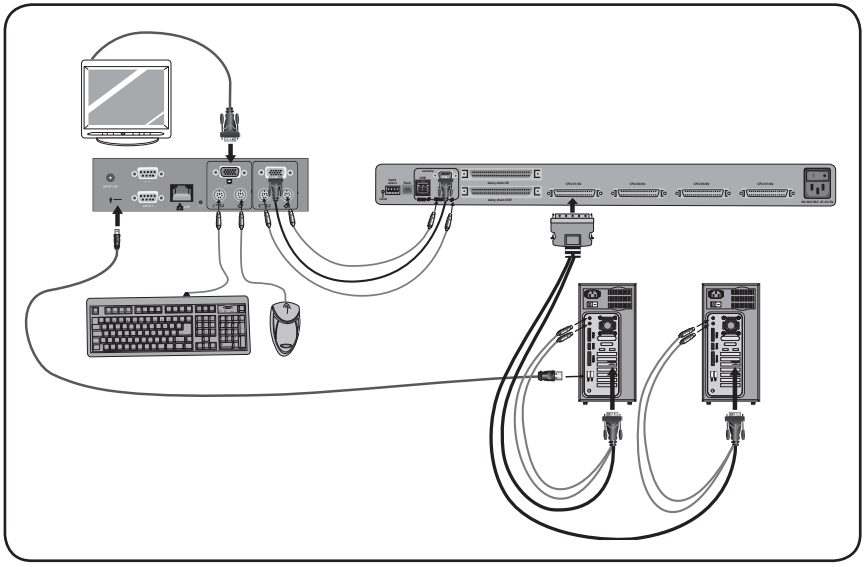


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:35:45 AM

Ejemplo de configuración del RIPM con un ordenador



Ejemplo de configuración del RIPM con un conmutador KVM



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:35:48 AM

Paso 1 | Instalación del RIPM en un bastidor para servidores

El RIPM incluye soportes de montaje para su instalación en bastidores de 19 pulgadas.

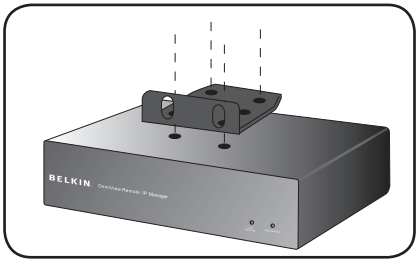


Fig. 1

1.1 Coloque el soporte incluido en la parte superior o inferior del RIPM con ayuda de los tornillos adjuntos.

1.2 Monte el RIPM en el bastidor. Vea la **Fig. 1.**

Nota: Los tornillos de montaje para el bastidor no están incluidos. Utilice los tornillos especificados por el fabricante de su bastidor.

Advertencia: Antes de intentar conectar nada al RIPM o a su ordenador u ordenadores, asegúrese de que todo su equipamiento informático y dispositivos se encuentren apagados. Si no lo hace, Belkin Corporation no se responsabilizará de los posibles daños que puedan producirse.

Paso 2 | Conecte su Consola al RIPM

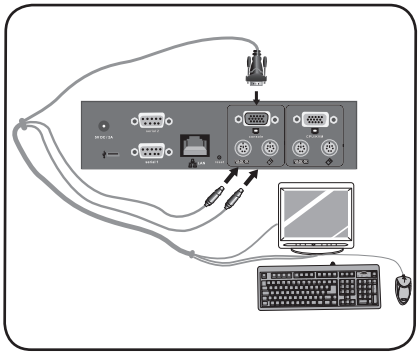


Fig. 2

2.1 Conecte su teclado y ratón a los puertos que tiene su RIPM para el ratón y el teclado de la “Consola”.

2.2 Conecte su monitor al puerto VGA para la “Consola” que tiene el RIPM. Vea la **Fig. 2.**

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:35:52 AM

Paso 3 | Opción 1: Conexión del RIPM a un conmutador KVM (sistema del equipo; equipo es el ordenador conectado al RIPM)

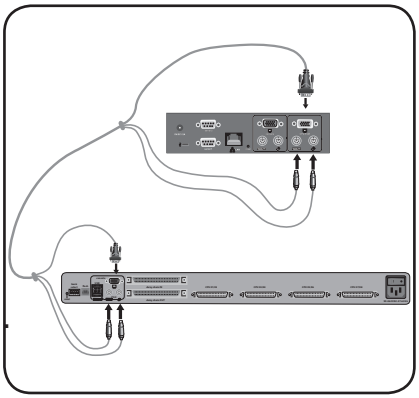


Fig. 3

3.1 Apague el conmutador KVM.

3.2 Utilizando el kit de cables VGA y PS/2 que se incluye, conecte un extremo a los puertos “CPU/KVM” para ratón, teclado y monitor que tiene el RIPM. Vea la **Fig. 3.**

3.3 Conecte el otro extremo al los puertos de ratón, teclado y monitor de su conmutador KVM.

Paso 3 | Opción 2: Conexión del RIPM a un ordenador (sistema del equipo)

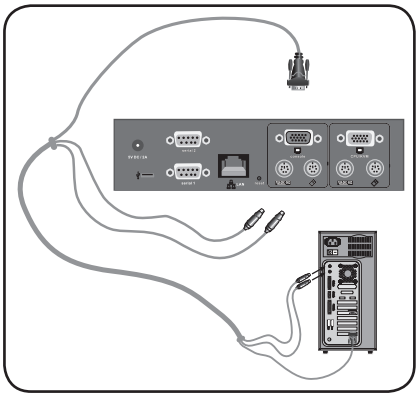


Fig. 4

3.1 Apague el ordenador.

3.2 Utilizando el kit de cables VGA y PS/2 que se incluye, conecte un extremo a los puertos “CPU/KVM” para ratón, teclado y monitor que tiene el RIPM. Vea la **Fig. 4.**

3.3 Conecte el otro extremo al los puertos de ratón, teclado y monitor de su ordenador.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:35:54 AM

Paso 4 | Conexión del Cable Mini-USB Cable para admitir medios virtuales

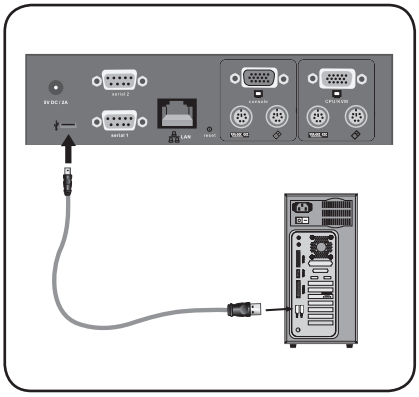


Fig. 5

4.1 Apague el ordenador.

4.2 Utilizando el cable Mini-USB que se proporciona, conecte un extremo al puerto Mini-USB del RIPM, y el otro extremo a un puerto Mini-USB disponible de su ordenador. Vea la **Fig. 5.**

Nota: Puede conectar cualquier ordenador que funcione con el sistema operativo Windows al RIPM para que admita medios virtuales, el ordenador no tiene que ser el sistema del equipo.

Nota: Si su ordenador NO funciona con Windows, no necesita realizar el paso anterior.

Paso 5 | Encendido del RIPM

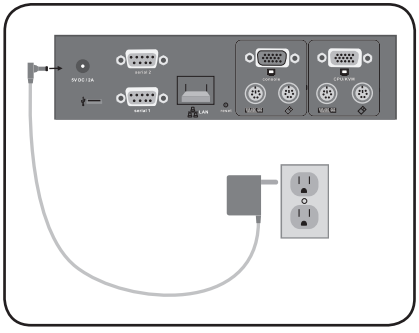


Fig 6

5.1 Conecte la fuente de alimentación que se incluye a un enchufe disponible.

5.2 Inserte el enchufe cilíndrico en la toma de alimentación del RIPM. Vea la **Fig. 6.**

5.3 Encienda su conmutador KVM o su ordenador.

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:35:56 AM

Existen dos formas de configurar el RIPM. Puede utilizar el software de configuración del dispositivo que se proporciona en el CD incluido en el paquete, o puede conectar un cable de interfaz Serie al RIPM y utilizar software de terminal (p. ej. HyperTerminal®).

Nota: Belkin recomienda que se utilice el software proporcionado de configuración del dispositivo.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:35:57 AM

Software de configuración del dispositivo

El software contenido en el CD que se incluye le ayudará a configurar el RIPM en su red para que pueda acceder a ella a distancia.

1. Conecte el RIPM a su ordenador mediante su red local. Inicie la herramienta de configuración del CD-ROM en el ordenador al que se ha conectado el RIPM.
2. Siga las instrucciones del asistente para configurar el RIPM. Necesitará tener la dirección IP, máscara de subred e información de pasarela que se asignará al RIPM. Puede que necesite obtener esta información de su administrador de red. Cuando la configuración se haya completado, recibirá una notificación de que se ha realizado con éxito. Su RIPM está ahora configurado y puede accederse a él.
3. Este CD-ROM también contiene el software necesario para transferir archivos entre los ordenadores remoto y local. Esto se explicará con más detalles en la sección “Medios virtuales” de este Manual del usuario.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:35:57 AM

Para configurar el RIPM mediante la interfaz Serie, se necesita un cable de módem null (incluido). Conecte el cable de módem null al puerto “serial 1” del RIPM y el otro extremo al puerto Serie del ordenador. La interfaz Serie necesita ajustarse con los parámetros que se muestran a continuación:

Parámetro	**Valor**
Bits/segundo	115200
Bits de datos	8
Paridad	No
Bits de parada	1
Control del flujo	Ninguno

Utilice un programa de software de terminal (p. ej. HyperTerminal) para conectar el RIPM. Reinicie el RIPM y pulse inmediatamente la tecla “ESC”. Aparecerá un mensaje “=>”. Escriba el comando “config” y pulse la tecla “INTRO”. Se le pedirá que ajuste la configuración automática IP, la dirección IP, la máscara de red y la pasarela predeterminada. Si pulsa la tecla “INTRO” sin introducir valores, no se cambian los ajustes. El valor de pasarela se debe fijar en “0.0.0.0” (si no hay pasarela) o cualquier otro valor para la dirección IP de la pasarela. Después de la confirmación, el RIPM lleva a cabo un reinicio utilizando los nuevos valores que se han fijado.

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:35:57 AM

Interfaz de web

Se puede acceder al RIPM utilizando un buscador de web estándar con Java™. Puede utilizar el protocolo HTTP o una conexión segura con cifrado mediante HTTPS. Simplemente introduzca la dirección IP del RIPM en su buscador de web. Los ajustes de acceso iniciales son:

Parámetro	Valor
Nombre de acceso	administrator
Contraseña	belkin

Se recomienda encarecidamente que cambie estos ajustes por valores únicos del usuario, esto se puede realizar en la página de Gestión del usuario (“User Management”).

Telnet

Es posible emplear un cliente Telnet estándar para acceder a un dispositivo cualquiera conectado a uno de los puertos Serie del RIPM a través de un modo de terminal.

La interfaz primaria del RIPM es la interfaz HTTP. Para utilizar la ventana de consola remota del sistema del equipo gestionado por usted, el buscador deberá incluir un entorno de ejecución Java versión 1.1 o superior. Si el buscador empleado no dispone de soporte Java (como en un dispositivo de bolsillo), también puede mantener su sistema de equipo remoto utilizando las formas de administración que muestra el propio navegador.

Para una conexión sin seguridad garantizada al RIPM, le podemos recomendar los buscadores siguientes:

- Microsoft Internet Explorer versión 5.0 o superior en Windows 2000 y XP
- Netscape Navigator 7.0 en Windows 2000 y XP

Para poder acceder al sistema de equipo remoto utilizando una conexión con cifrado segura, necesitará un navegador compatible con el protocolo HTTPS. Únicamente será posible garantizar una seguridad elevada si emplea una clave de 128 bits de longitud.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:35:57 AM

Abra su navegador de Internet. Escriba la dirección de su RIPM que ha configurado durante el proceso de instalación. Para esto, puede utilizar una dirección IP o un equipo y nombre de dominio, en caso de que haya dado a su RIPM un nombre simbólico en el DNS (Servidor de nombres de dominio).

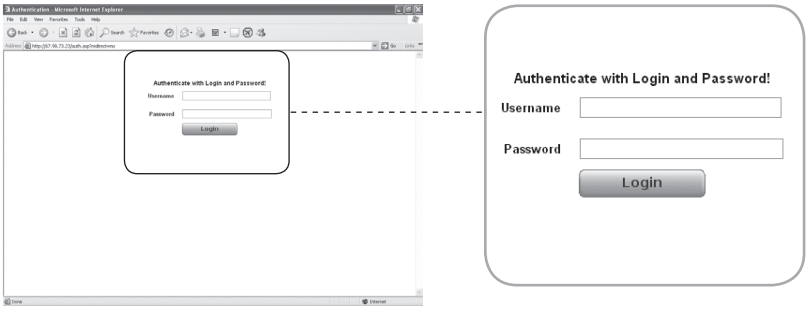
Por ejemplo, introduzca lo siguiente en la barra de dirección de su buscador de Internet web cuando establezca una conexión sin seguridad:

http://192.168.1.22/

Cuando utilice una conexión segura, escriba:

http://192.168.1.22/

Esto le conducirá a la página de acceso del RIPM, que se muestra a continuación:



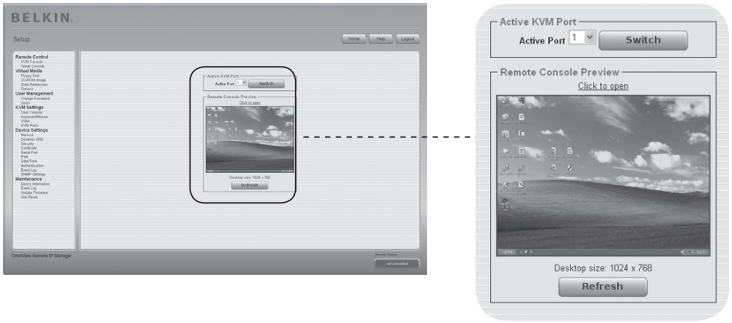
El RIPM dispone de una cuenta de administrador incorporada que tiene todos los permisos para administrar su RIPM:

Parámetro	Valor
Nombre de acceso	administrator
Contraseña	belkin

Nota: Su buscador de Internet debe aceptar cookies, de lo contrario, el acceso no será posible.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:35:58 AM

La Consola remota son la pantalla, teclado y ratón redirigidos del sistema de equipo remoto en el que se ha instalado el RIPM. El buscador de Internet utilizado para el acceso al RIPM deberá ofrecer un entorno de ejecución Java versión 1.1 o superior. Sin embargo, se recomienda encarecidamente que instale Sun JVM (Java Virtual Machine) 1.4. La Consola remota se comportará exactamente del mismo modo que si estuviese sentado directamente frente a la pantalla de su sistema remoto, puede utilizar el teclado y el ratón con normalidad. Abra la Consola remota seleccionando la imagen de vista previa de la portada HTML.



Algunas de las opciones de menú disponibles incluyen:

Botón de regulación automática

Si la imagen mostrada es de mala calidad o está distorsionada de alguna forma, pulse este botón y espere unos segundos mientras que el RIPM se regula para obtener la mejor calidad de imagen posible.

Sincronización del ratón

Seleccione esta opción para sincronizar el cursor del ratón local con el del ratón remoto. Esto es especialmente necesario cuando se utilizan ajustes de ratón más rápidos en el sistema del equipo.

Ajustes de vídeo en el menú de opciones

Esta opción abre una nueva ventana con elementos que permiten controlar los ajustes de vídeo del RIPM. Podrá modificar algunos valores, por ejemplo, los relacionados con el brillo y el contraste de la imagen mostrada, para mejorar la calidad de la misma. Asimismo, es posible retornar a los ajustes por defecto para todos los modos de vídeo o sólo para el modo actual.

Nota: La primera vez que se inicia el sistema, el puntero del ratón local no está sincronizado con el puntero del ratón remoto, pulse el botón de regulación automática una vez.

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:35:58 AM

Entre el RIPM y el equipo, existen dos interfaces disponibles para transmitir los datos del ratón y el teclado: USB y PS/2 (disponibles por separado). El funcionamiento correcto del ratón remoto depende de varios ajustes, que se describirán en los apartados siguientes.

Interfaz USB del Remote IP Manager

Para utilizar la interfaz USB, necesita usar el cableado correcto entre el equipo que se gestiona y el dispositivo de gestión. Por ejemplo, si el equipo que se gestiona no tiene soporte para teclado USB en la BIOS y únicamente ha conectado el cable USB, entonces no tendrá acceso al teclado remoto durante el proceso de arranque del equipo. Consulte la sección “Teclado/ratón” en la página 48.

Ajustes de teclado para el Remote IP Manager

Los ajustes del RIPM para el tipo de teclado del equipo deben ser correctos para lograr que el teclado remotos funcione adecuadamente. Controle los ajustes en la portada del RIPM. Consulte la sección “Teclado/ratón” en la página 48.

Ajustes de ratón remoto

Un problema común en los dispositivos KVM es la sincronización entre los cursores de los ratones local y remoto. El RIPM aborda esta circunstancia con un algoritmo de sincronización inteligente. Hay tres modos de ratón disponibles en el RIPM.

- **Velocidad de ratón automática**
  La velocidad de ratón automática intenta detectar los ajustes de aceleración y velocidad del sistema del equipo automáticamente. Consulte la sección siguiente para una explicación más detallada.

- **Velocidad de ratón fija**

Este modo traslada los movimientos del ratón de la Consola remota de forma que un movimiento de un píxel conducirá al movimiento de un píxel en el sistema remoto. Este parámetro se puede ajustar a escala. Se debe tener en cuenta que esto funciona únicamente cuando la aceleración del ratón está desactivada en el sistema remoto.

- **Modos de ratón sencillo y doble**
  Este modo se describe en la sección “Modos de ratón sencillo y doble” en la página 20.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:35:58 AM

Sincronización de ratón y velocidad de ratón automática

El modo de velocidad de ratón automática realiza la detección de la velocidad durante la sincronización del ratón. Cuando el ratón no se mueve correctamente, existen dos formas de volver a sincronizar el ratón local y el remoto:

- **Sincronización rápida**
  La sincronización rápida se emplea para corregir una divergencia temporal pero fija. Seleccione esta opción del menú de opciones de la Consola remota. Si se ha definido, también puede
  pulsar la secuencia de teclas de acceso directo para sincronizar el ratón (consulte la sección “Barra de control de
  Consola remota” en la página 23).

- **Sincronización inteligente**
  Si la sincronización rápida no funciona, o si han sido modificados los ajustes del ratón en el sistema del equipo, utilice la sincronización inteligente. Este método ajusta los parámetros para el movimiento real de puntero del ratón de forma que el puntero del ratón aparece en la posición correcta de la pantalla. Este método precisa algo más de tiempo que la sincronización rápida y puede ser iniciado a través del elemento correspondiente del menú de opciones de la Consola remota. La sincronización inteligente necesita una imagen correctamente regulada. Utilice la función de regulación automática o la corrección manual en el panel de ajustes de vídeo para ajustar la imagen. La forma del puntero del ratón tiene una influencia importante en la detección del puntero. Belkin recomienda que utilice una forma de puntero sencilla y común. En la mayoría de los casos, la detección y sincronización fallan con formas de puntero animadas. En general, las formas de puntero que cambian durante el proceso de detección del puntero son prácticamente imposibles de detectar en la imagen de vídeo transferida. Si utiliza un puntero de ratón corriente, se asegura de que el proceso de detección será bastante sencillo y la sincronización será óptima.

  El botón del “Ratón” de la parte superior de la Consola remota puede comportarse de manera diferente, dependiendo del estado actual de sincronización del ratón. Normalmente, al pulsar este botón, se realiza una sincronización rápida, excepto en situaciones en las que se acaba de cambiar la modalidad de vídeo. Consulte también la sección “Barra de control de Consola remota” en la página 23.

Nota: En el primer inicio del sistema, si el puntero del ratón local no está sincronizado con el puntero del ratón remoto, pulse el botón de regulación automática una vez.

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:35:59 AM

Ajustes de ratón del sistema del equipo

El sistema operativo del equipo dispone de diversos ajustes del controlador del ratón.

Aunque el RIPM funciona con ratones acelerados y es capaz de sincronizar el puntero del ratón local con el del remoto, las condiciones siguientes pueden impedir que la sincronización funcione correctamente:

- **Controlador especial de ratón**
  Existen controladores de ratón que influyen en el proceso de sincronización, provocando que los punteros de los ratones se desincronicen. Si esto sucede, asegúrese de que no esté empleando un controlador de ratón específico de un vendedor en su sistema del equipo.

- **Ajustes de ratón Windows 2003 Server/XP**
  Windows XP tiene un ajuste denominado “mejorar la aceleración del ratón”, que debe desactivarse.

- **Escritorio activo**
  Si está activada la función de Microsoft Windows “Escritorio activo”, no utilice un fondo de escritorio plano. En lugar de eso, utilice un fondo de pantalla con imágenes. Como alternativa, puede desactivar totalmente el Escritorio activo.

  Desplácese con el puntero del ratón hacia la esquina superior izquierda de la pantalla del Applet (aplicación Java) y muévalo ligeramente hacia delante y hacia atrás. Esto volverá a sincronizar el ratón. Si la resincronización falla, desactive la aceleración del ratón y repita el proceso.

- **Modos de ratón sencillo y doble**
  La información anterior se aplica a la modalidad de ratón doble cuando los punteros de los ratones local y remoto pueden verse y necesitan ser sincronizados. El RIPM dispone de otra modalidad, el modo de ratón único, en el que solo puede verse el puntero del ratón remoto. Active este modo en la Consola remota (consulte la sección “Barra de control de Consola remota” en la página 23) y haga clic en el área de la ventana. El puntero del ratón remoto se ocultará, y se podrá controlar el remoto directamente. Para salir de este modo, es necesario definir una tecla de acceso directo para el ratón en el panel de ajustes de la Consola remota. Pulse esta tecla para mostrar el puntero del ratón local oculto.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:35:59 AM

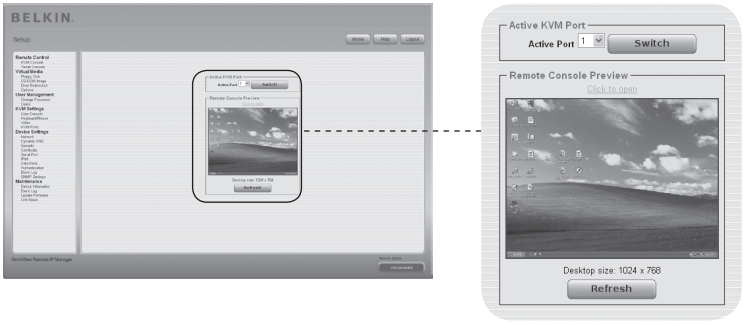
Ajustes de ratón recomendados

Windows 2000, 2003, XP (todas las versiones)	En general, Belkin recomienda el uso de un ratón a través de USB. Elija USB sin sincronización de ratón.
Mac OS X	Belkin recomienda utilizar la modalidad de ratón único.
Sun Solaris	Ajuste la configuración del ratón mediante “xset m 1” o utilizando el Panel de control CDE para ajustar el ratón sin aceleración en “1:1, no acceleration”. Como alternativa, también puede utilizar el modo de ratón único.
Linux	Primero, elija la opción de otros sistemas operativos “Other Operating Systems” del cuadro de selección de tipo de ratón “Mouse Type”. En segundo lugar, elija la opción de velocidad de ratón automática “Auto Mouse Speed”. Esto se aplica a ratones tanto USB como PS/2.

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:35:59 AM

Navegación

Una vez que haya accedido correctamente al RIPM, aparece la pantalla principal del RIPM. Esta página consta de tres partes y cada una de ellas contiene información específica. Los botones de la parte superior le permiten navegar en la portada (consulte la Tabla para más detalles). El marco inferior izquierdo contiene una barra de navegación que le permite cambiar entre las distintas secciones del RIPM. La información específica de la tarea, que depende de la sección que haya seleccionado antes, se muestra en el interior del marco derecho.



Nota: Si no existe actividad durante 30 minutos, el RIPM cerrará su sesión automáticamente. Al hacer clic en uno de los enlaces, se dirigirá de nuevo a la pantalla de acceso.

P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:36:00 AM

La parte superior de la ventana de la Consola remota contiene una barra de control. Utilizando sus elementos, puede ver el estado de la Consola remota y modificar los ajustes de la Consola remota local. A continuación, se describen los controles.

- **Botón de regulación automática**

Si la imagen mostrada es de mala calidad o está distorsionada de alguna forma, pulse este botón y espere unos segundos mientras que el RIPM se regula para obtener la mejor calidad de imagen posible.

- **Sincronización del ratón**

Seleccione esta opción para sincronizar el cursor del ratón local con el del ratón remoto. Esto es especialmente importante cuando se utilizan ajustes de ratón más rápidos en el sistema del equipo. En general, no es necesario modificar los ajustes de ratón.

- **Modos de ratón sencillo y doble**

Elija esta modalidad para cambiar entre el modo de ratón único (en el que solo puede verse el puntero del ratón remoto) y la modalidad de ratón doble (cuando los punteros de los ratones local y remoto pueden verse y necesitan ser sincronizados). El modo de ratón único está disponible sólo si utiliza Sun JVM 1.4 o superior.

- **Opciones**

Para abrir el menú de opciones, haga clic en el botón de opciones “Options”.

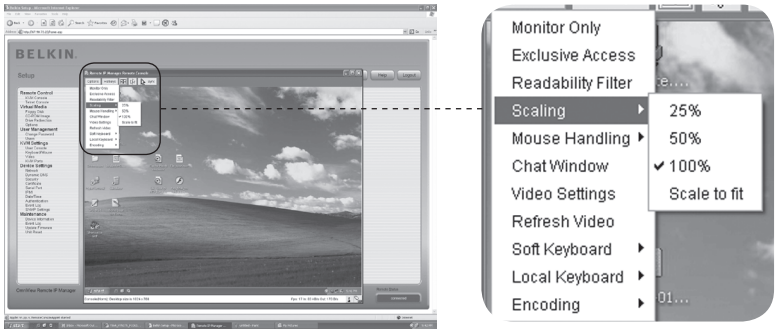
A continuación se ofrece una breve descripción de las opciones:

- **Monitor Only (sólo supervisión)**
  Activa o desactiva el filtro “Monitor Only”, únicamente supervisión. Si el filtro está activado, no es posible la interacción con la Consola remota, pero sí es posible supervisar el sistema.

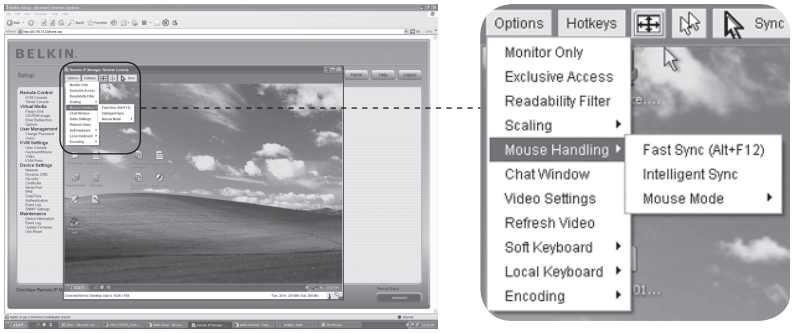
- **Exclusive Access (acceso exclusivo)**
  Con los permisos adecuados, puede hacer que todas las Consolas remotas de todos los otros usuarios se cierren. Nadie podrá abrir la Consola remota al mismo tiempo otra vez hasta que no desactive el acceso exclusivo o cierre la sesión.

P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:36:00 AM

- **Scaling (escala)**
  Le permite reducir la escala de la Consola remota. Podrá seguir utilizando el ratón y el teclado, sin embargo, el algoritmo de escala no conservará todos los detalles de la imagen.



- **Mouse Handling (manejo del ratón)**
  El submenú para el manejo del ratón ofrece dos opciones para sincronizar los punteros de los ratones local y remoto, como se explica en la sección “Configuración de vídeo, teclado y ratón”.



- **Fast Sync (sincronización rápida)**
  La sincronización rápida se emplea para corregir una divergencia temporal pero fija.

- **Intelligent Sync (sincronización inteligente)**
  Utilice esta opción si la sincronización rápida no funciona, o si han sido modificados los ajustes del ratón en el sistema del equipo.

  Advertencia: Este método precisa algo más de tiempo que la sincronización rápida y se necesita una imagen correctamente regulada. Para ajustar la imagen, utilice la función de regulación automática o la corrección manual en el panel de ajustes de vídeo.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:36:01 AM

- **Cursor local**

  Ofrece una lista con distintos tipos de formas de cursor para elegir el puntero del ratón local. La forma seleccionada por el usuario actual se guardará y se activará la próxima vez que este usuario abra la Consola remota. El número de punteros disponibles depende de la versión de JVM (Java Virtual Machine), las versiones 1.2 y superiores ofrecen la lista completa.

- **Ajustes de vídeo**

  Abre un panel para modificar los ajustes de vídeo del RIPM. El RIPM dispone de dos cuadros de diálogo diferentes que influyen en los ajustes de vídeo.

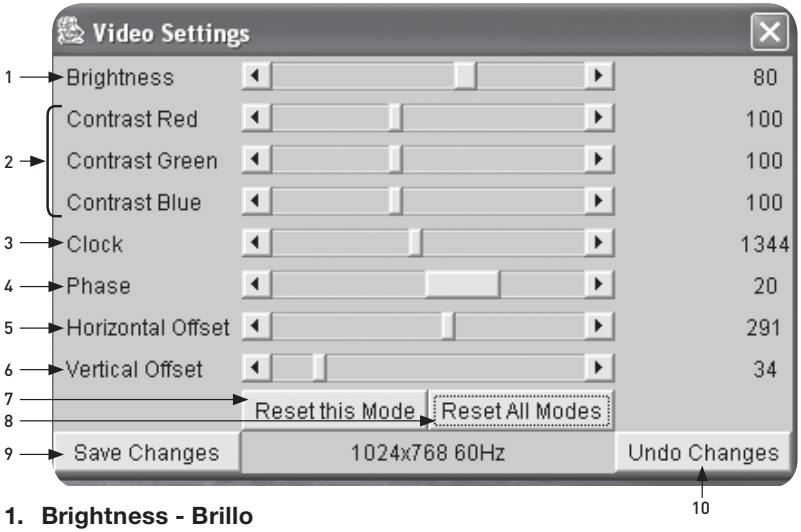
- **Ajustes de vídeo a través de la portada HTML**

  Seleccione esta opción para activar el puerto de vídeo local. Esta opción determina si la salida de vídeo local del RIPM está activa y pasando a través de la señal entrante desde el sistema del equipo.

  La opción de “Noise Filter” (filtro de ruido) define cómo reacciona el RIPM a pequeños cambios en la señal de entrada de vídeo. Un ajuste de mayor filtro necesita menor tráfico de red y contribuye a una mayor rapidez del vídeo, pero los pequeños cambios pueden que no se reconozcan de inmediato en algunas regiones. Un filtro más estricto indica todos los cambios instantáneamente pero puede provocar una cantidad constante de tráfico de red, incluso cuando el contenido de la pantalla no está cambiando realmente (dependiendo de la calidad de la señal de entrada de vídeo). El ajuste predeterminado es adecuado para la mayoría de las situaciones.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:36:01 AM

Ajustes de vídeo a través de la Consola remota



1. **Brightness - Brillo**
   Controla el brillo de la imagen.
2. **Contrast - Contraste**
   Controla la definición del contraste de la imagen.
3. **Clock - Reloj**
   Define la frecuencia horizontal para una línea de vídeo y depende de la modalidad de vídeo. Los distintos tipos de tarjetas de vídeo pueden requerir valores diferentes. Los ajustes predeterminados, junto con el procedimiento de ajuste automático debería ser adecuado para todas las configuraciones más comunes. Para lograr una mejor calidad de imagen, puede intentar cambiar este ajuste junto con la fase de muestreo.
4. **Phase - Fase**
   Define la fase del muestro de vídeo, utilizado para controlar la calidad de imagen junto con el ajuste del reloj de muestreo.
5. **Horizontal Offset - Compensación horizontal**
   Le permite utilizar los botones de la parte izquierda y derecha para desplazar la imagen en sentido horizontal mientras se mantenga seleccionada esta opción.
6. **Vertical Offset - Compensación vertical**
   Le permite utilizar los botones de la parte izquierda y derecha para desplazar la imagen en sentido vertical mientras se mantenga seleccionada esta opción.
7. **Reset this Mode - Reiniciar esta modalidad**
   Reinicia los ajustes de esta modalidad específica, estableciendo los ajustes de fábrica.
8. **Reset all Modes - Reiniciar todas las modalidades**
   Reinicia todos los ajustes, estableciendo los ajustes predeterminados de fábrica.
9. **Save Changes - Guardar cambios**
   Guarda los cambios de forma permanente.
10. **Undo Changes - Deshacer cambios**
    Restablece los últimos ajustes.

P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:36:02 AM

Secuencia de asignación

Soft Keyboard - Teclado virtual
Abre el menú para el teclado virtual.

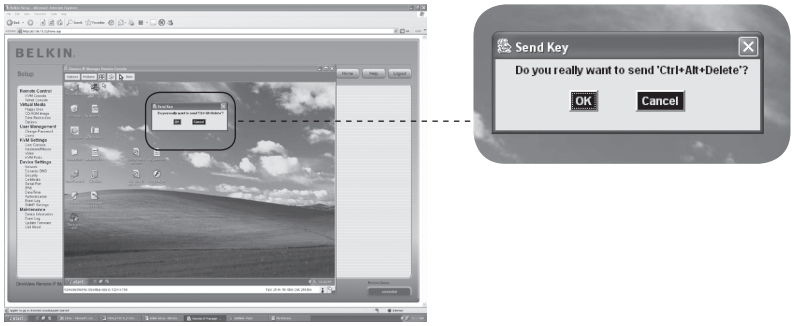
Show - Mostrar
Abre la ventana del teclado virtual. El teclado virtual es necesario en caso de que su sistema del equipo funcione con asignación de país e idioma completamente diferentes a los de su máquina de administración.

Mapping - Asignación
Se utiliza para elegir la asignación de país e idioma adecuados para el teclado virtual.

P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:36:02 AM

Teclado local
Se utiliza para cambiar la asignación de idioma de su máquina buscadora en la que se ejecuta el Applet de la Consola remota. Normalmente, el Applet determina automáticamente el valor correcto. Sin embargo, dependiendo de los ajustes de su servidor y de su versión de JVM, esto no siempre es posible. Un ejemplo es un sistema situado en Alemania que utiliza asignación de teclado inglés de los EE.UU. En este caso, debe ajustar manualmente el ajuste del teclado local para seleccionar el lenguaje correcto.

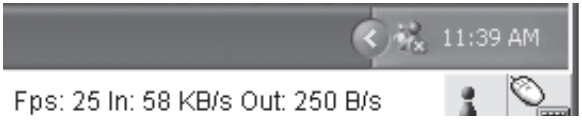
Teclas de acceso directo
Abre una lista de teclas de acceso directo predefinidas. Elija una entrada y el comando se enviará al sistema del equipo. Puede añadir un cuadro de diálogo de confirmación que aparecerá antes de que el comando seleccionado se envíe al equipo remoto. Seleccione “OK” para llevar a cabo el comando en el equipo remoto.



P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:36:03 AM

La línea de estado muestra tanto el estado de la Consola remota como el estado de conexión. El tamaño de la pantalla remota se indica a la izquierda. El valor entre paréntesis describe la conexión a la Consola remota. “Norm” significa una conexión estándar sin cifrado; “SSL” indica una conexión segura en la que se utiliza el protocolo SSL.

Tanto el tráfico de red entrante (“In:”) como el de salida (“Out:”) se indican en kilobytes por segundo. Si se activa la codificación comprimida, un valor entre paréntesis indica la tasa de transferencia comprimida.



El siguiente botón muestra los ajustes de acceso de la Consola remota.

Uno o más usuarios están conectados a la Consola remota del RIPM.

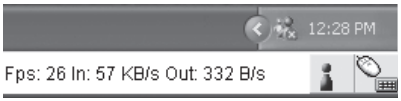
Su acceso se ha establecido como exclusivo. Cualquier otro usuario no podrá acceder al equipo remoto mediante la Consola remota a menos que desactive esta opción.

P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:36:04 AM

Un usuario remoto tiene acceso exclusivo. Cualquier otro usuario no podrá acceder al equipo remoto mediante la Consola remota a menos que desactive esta opción.

El botón exterior derecho muestra el estado de los ajustes de supervisión sin interacción “Monitor Only”.

La opción “Monitor Only” está desactivada.



La opción “Monitor Only” está activada.

Para más información sobre los ajustes de acceso exclusivo y sólo supervisión, consulte la sección “Barra de control de consola remota” en la sección 23 de este Manual del usuario.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:36:04 AM

Reajuste del Remote IP Manager a los ajustes de fábrica

Para reiniciar el RIPM y cambiar los ajustes de red restableciendo los ajustes de fábrica:

1. Haga una conexión Serie para la configuración inicial (HyperTerminal)

Bits por segundo:	115200
Bits de datos:	8
Paridad:	Ninguno
Bits de parada:	1
Control del flujo:	hardware o ninguno

2. Pulse el botón de reinicio, situado entre la toma de corriente CC y la toma de red. Suelte el botón de reinicio e inmediatamente pulse la tecla ESC en el programa terminal Serie (HyperTerminal) varias veces hasta que aparezca la ventana "=>".

   Nota: Si la ventana no aparece en los primeros tres segundos después de soltar el botón de reinicio, repita los Pasos 1 y 2. El RIPM detectará la tecla ESC sólo durante los tres primeros segundos del proceso de inicio.

3. Cuando aparezca, escriba "defaults" y pulse la tecla intro. El RIPM entonces se reiniciará y se restablecerán los ajustes de fábrica.
4. Apague su servidor (el ordenador al que está conectado localmente el RIPM).
5. Desconecte el suministro eléctrico del RIPM así como los cables del puerto "CPU/KVM" y el cable de red.
6. Vuelva a conectar los cables y encienda su servidor.

Ahora puede volver a configurar el RIPM a los ajustes de red mediante un conexión HyperTerminal, o utilizando el software de configuración.

Cerrar sesión del Remote IP Manager

Este botón "Logout" cierra la sesión del usuario actual y presenta una nueva pantalla de acceso. Tenga en cuenta que la sesión se cerrará de manera automática si no existe actividad durante media hora.

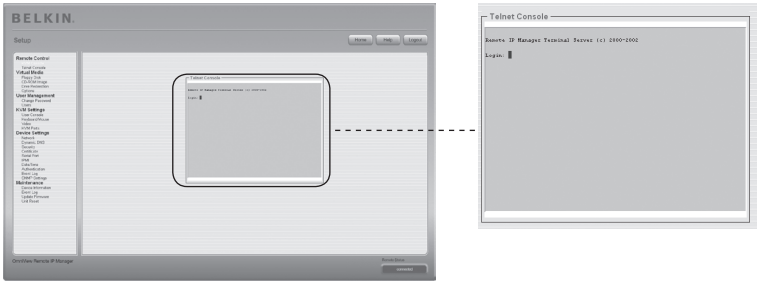
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:36:04 AM

Consola KVM

Vista previa de la Consola remota

Para abrir la consola KVM, haga clic en la entrada del menú a la izquierda, o en la imagen de la consola a la derecha. Para actualizar la imagen, haga clic en el botón “Refresh” (Actualizar).

Consola Telnet



El firmware del RIPM dispone de un acceso Telnet que permite al usuario conectarse al RIPM mediante un cliente Telnet estándar. Para conectarse al RIPM mediante el protocolo Telnet, debe utilizar un programa de terminal como xterm, TeraTerm, o PuTTY. Como alternativa, puede introducir el comando Telnet en la línea para comandos o utilizar el cuadro de “Ejecutar” desde el menú de Inicio de Windows. Por ejemplo, puede escribir la siguiente secuencia:

Telnet: 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:36:05 AM

Sustituya la dirección IP con la que se asignó al RIPM durante la instalación. A continuación, se le pedirá la información del nombre de usuario y la contraseña para acceder al dispositivo. Los credenciales necesarios que deben introducirse para la autenticación son idénticos a los de la interfaz de web. Esto significa que la gestión del usuario de la interfaz Telnet está totalmente controlada con las funciones adecuadas de la interfaz de web. Una vez que haya accedido correctamente al RIPM, aparecerá un línea para comandos y puede introducir los comandos de gestión correspondientes. En general, la interfaz Telnet tiene dos modos de funcionamiento: el modo de línea para comandos y el modo de terminal. El modo de línea para comandos se utiliza para controlar o supervisar algunos parámetros. En el modo de terminal, el acceso de transferencia al puerto Serie 1 está activado (si los ajustes Serie se han realizado correctamente). Para acceder al RIPM mediante la interfaz Serie, se necesita un cable de módem null. Todas las entradas son redirigidas al dispositivo en el puerto Serie 1, y sus respuestas se muestran en la interfaz Telnet.

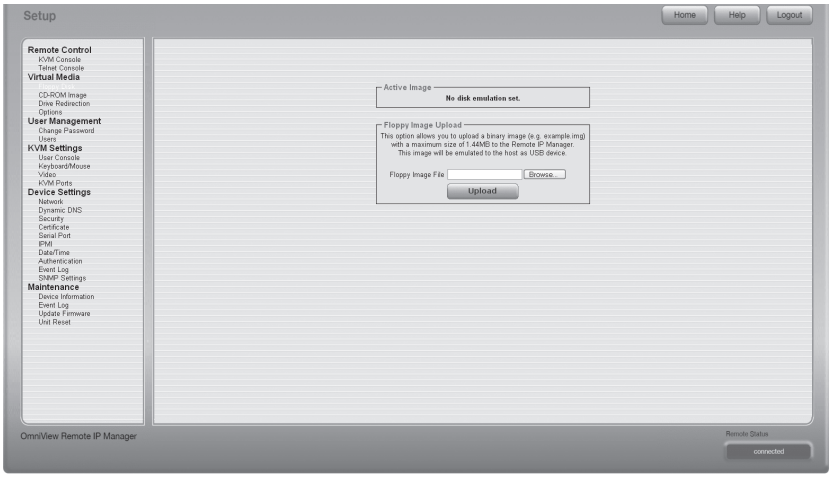
La siguiente lista muestra los comandos y sus funciones.

Help	Muestra la lista de posibles comandos.
cls	Borra la pantalla.
quit	Cierra la sesión actual y se desconecta del cliente.
version	Muestra la información sobre la publicación.
terminal	Inicia el modo de transferencia de terminal para el puerto 1. La secuencia “esc exit” hace regresar al modo para comandos. El comando tiene un parámetro opcional (1 ó 2) para seleccionar el puerto Serie que se prefiera para el acceso de transferencia.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:36:05 AM

Disquete



Esta función está destinada a cargar y transferir archivos de imagen (compilación de toda la información de un disco físico en un solo archivo). Esta opción le permite cargar una imagen en modo binario (ejemplo.img) con un tamaño máximo de 1,44 MB al RIPM. Esta imagen o copia del dispositivo será emulada en el equipo como un dispositivo USB. El resto de formatos deben transferirse utilizando la función de redirección de unidad. Para utilizar una imagen de mayor tamaño, monte esta imagen utilizando la opción Compartir Windows.

Carga de la imagen de un disquete

Paso 1: Haga clic en “Browse” (Examinar) para especificar qué archivo va a transferirse.

Paso 2: Haga clic en “Upload” (Cargar) para cargar el archivo en el RIPM. Recibirá un mensaje de confirmación de que el archivo se ha cargado correctamente en el RIPM.

Paso 3: Haga clic en “KVM Console” (Consola KVM) en la sección Consola remota de la interfaz del RIPM para acceder al escritorio del ordenador remoto.

Paso 4: Haga doble clic en el icono de Mi PC para abrir esta carpeta.

Paso 5: Aparecerá una segunda entrada para la unidad de disquete en la lista de Mi PC. Esta entrada se denomina “3-1⁄2 Floppy (B)”. Aquí puede acceder a los archivos que ha transferido.

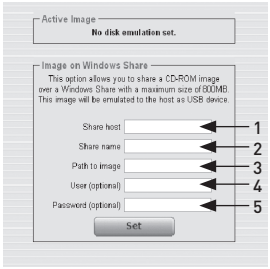
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:36:06 AM

Imagen de un CD-ROM

Utilice Imagen en Compartir Windows (Samba).

Para incluir una imagen de Compartir Windows, seleccione “CD-ROM” en el submenú.

Debe proporcionar la información siguiente para montar correctamente la imagen seleccionada:



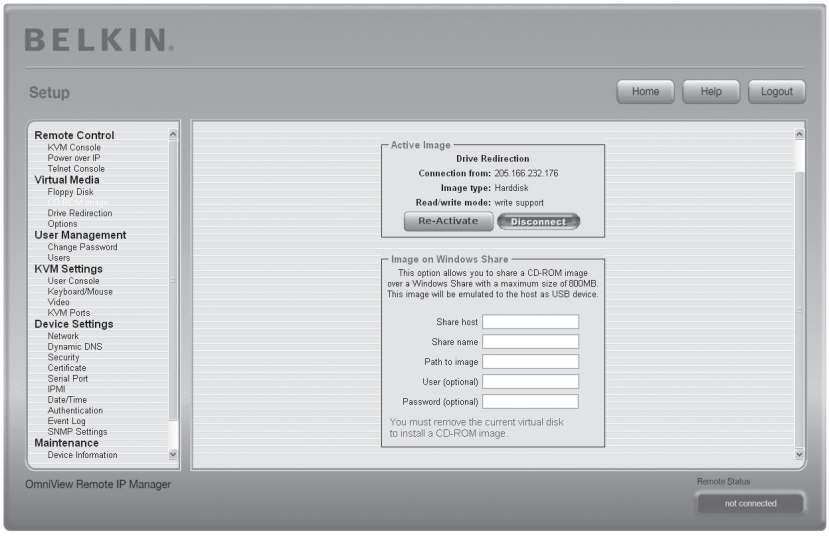
1. **Share Host - Compartir equipo**
   El nombre del servidor o su dirección IP. (Esta dirección IP se obtiene ejecutando el software de redirección de la unidad, como se explica a continuación.)
2. **Share Name - Nombre compartido**
   El nombre de la carpeta compartida que se va a utilizar.
3. **Path to image - Ruta a la imagen**
   La ubicación del archivo de imagen que se comparte.
4. **User (Optional) - Usuario (opcional)**
   Si es necesario, especifique el nombre de usuario para compartir. Si no se especifica y existe una cuenta de invitado activada, esta información de cuanta de invitado se utilizará como su nombre de acceso.
5. **Password (Optional) - Contraseña (opcional)**
   Si se le pide que proporcione una contraseña, escriba la contraseña del nombre de usuario que utilizó.

P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:36:06 AM

Cargar la imagen de un CD-ROM

Paso 1: Abra y ejecute el software de redirección de unidad.

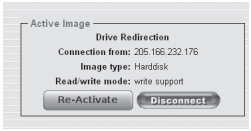
Paso 2: Cuando el software de redirección de unidad se ha conectado, deje esta ventana abierta y vaya a la imagen del CD-ROM en la sección Medios virtuales de la interfaz del RIPM.



Nota: La dirección IP que aparece tras “Connection From” (Conexión desde) es la dirección IP que se utilizó como dirección del equipo para compartir. Para verificar que la dirección IP asignada por el software de redirección de unidad es correcta, conecte el cable Serie entre el RIPM y el ordenador y abra una sesión de HyperTerminal. Acceda como “ping” y escriba la dirección IP exactamente como en el campo “Share host” (Compartir equipo). Debería recibir la respuesta “<IP> is alive!” (IP activa)

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:36:07 AM

Paso 3: Clic “Re-Activate” (Reactivar) en la sección Active Image (Imagen activa).



Paso 4: Introduzca en el campo “Share Host “ (Compartir equipo) la dirección IP proporcionada por el software de redirección de unidad.

Paso 5: Introduzca en “Share name” el nombre de la carpeta que se va a compartir y en “Path to Image” la ubicación de la imagen.

Paso 6: Para cargar el archivo, haga clic en el botón “Set”. El archivo se mostrará como un dispositivo USB en el ordenador remoto.

El archivo de la imagen especificado debe poder ser accesible desde el RIPM. La información anterior debe proporcionarse desde el punto de vista del RIPM. Es importante especificar las direcciones IP correctas y los nombres de dispositivos. De lo contrario, el RIPM no podrá acceder correctamente al archivo de imagen mencionado y dejará el archivo sin montar (aparece un mensaje de error). Belkin recomienda que utilice los valores correctos y que repita este paso, si fuese necesario.

La configuración para compartir se debe realizar correctamente Además es necesario tener permisos de administrador. Como usuario normal, puede que no tenga estos permisos. Debe acceder como administrador del sistema o pedirle ayuda al administrador de su sistema para que lleve a cabo esta tarea.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:36:07 AM

Redirección de unidad

La función de redirección de unidad ofrece otro modo de usar una unidad de disco virtual en el ordenador remoto. Puede trabajar con una unidad de su ordenador local desde la máquina remota compartiendo la unidad mediante una conexión de red TCP. Los dispositivos de almacenamiento como disquetes y discos duros*, CD-ROM, y dispositivos extraíbles como memorias USB, se pueden redirigir. Incluso puede configurar su ordenador remoto para poder grabar datos en un disco local.

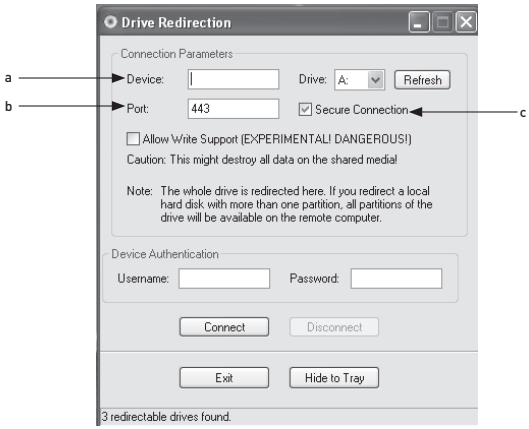
***Nota:** Belkin no recomienda activar la función de escribir datos cuando se redirigen discos duros y no se hace responsable de las pérdidas o corrupción de datos durante este proceso.

Le rogamos que actúe con precaución cuando utilice esta función. La redirección de unidad función a un nivel que se encuentra muy por debajo del sistema operativo, por lo que no el sistema operativo remoto ni el local pueden detectar que en un momento dado se está redirigiendo una unidad. Esto puede causar inconsistencia de datos cuando uno de los sistemas operativos (ya sea en el ordenador local o el equipo remoto) escribe datos en el dispositivo. Con la capacidad de escribir datos activada, el ordenador remoto puede dañar los datos y el sistema de archivos del dispositivo redirigido. Por otra parte, si el sistema operativo local escribe datos en el dispositivo redirigido, caché de la unidad en el sistema operativo del equipo remoto podría contener datos antiguos, causando confusión en el sistema operativo del equipo remoto. Por lo tanto recomendamos que se utilice con mucho cuidado la redirección de unidad, especialmente la función que permite escribir datos.

Nota: Para poder utilizar la función de redirección de unidad, debe instalar el software de redirección de unidad, que se incluye con este producto, en el ordenador que está utilizando para acceder al RIPM a distancia.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:36:07 AM

1. **Abra la aplicación de redirección de unidad.**



2. **Especifique los parámetros de la conexión de red.**
   a. Device - Dispositivo
   Esta es la dirección IP del RIPM al que quiere conectarse.
   b. Por - Puerto
   Este es el puerto de red. De forma predeterminada, el RIPM utiliza el puerto de la consola remota (n° 443). Puede que tenga que cambiar este valor si ha cambiado el puerto de la consola remota en los ajustes de red de su RIPM.
   c. Secure Connection - Conexión Segura
   Marque este recuadro para establecer una conexión segura mediante SSL. Esto aumentará al máximo la seguridad, sin embargo, puede reducir la velocidad de conexión.
3. **Seleccione la unidad que quiere redirigir.** Se muestran todos los dispositivos disponibles (las letras de las unidades). Tenga en cuenta que el RIPM comparte con el ordenador remoto la unidad entera, no solo una partición. Si tiene un disco duro con más de una partición todas las letras de las unidades que pertenezcan al disco duro se redirigirán. Utilice el botón "Refresh" para actualizar la lista de letras de las unidades, especialmente en caso de que se utilice una unidad de almacenamiento USB.
4. **Capacidad de escribir**
   Advertencia: Utilice esta función con precaución. La capacidad de escribir permite al ordenador remoto escribir en su unidad local. Si los dos sistemas local y remoto intentan simultáneamente escribir datos en el mismo dispositivo, **el sistema de archivos de la unidad se destruirá.** Le rogamos que utilice esta función solamente si tiene absoluta certeza de que puede hacerlo de forma segura.
   Nota: Belkin no recomienda activar la función de grabar datos cuando se redirigen discos duros y no se hace responsable de las pérdidas o corrupción de datos durante este proceso.
5. **Autenticar el dispositivo.** Para utilizar la redirección de unidad, debe identificarse en el RIPM utilizando un nombre de usuario y contraseña válidos. Necesitará permiso para cambiar la configuración de disco virtual.

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:36:07 AM

6. **Establezca la redirección de unidad pulsando el botón “Connect” (Conectar) una vez.**
   Si todos los ajustes son correctos, la barra de estado indica que la conexión se ha realizado, el botón “Connect” (Conectar) está desactivado, y el botón “Disconnect” (Desconectar) se activa. En caso de error, la barra de estado muestra el mensaje de error.

   El software de redirección de unidad intenta bloquear la unidad local antes de que sea redirigida. Esto impide que el sistema operativo local acceda a la unidad mientras se redirige. El intento fallará si cualquier archivo de la unidad se encuentra abierto. En caso de que haya un fallo de bloqueo, se le pedirá que confirme si desea establecer la conexión. Sin embargo, recuerde que si la capacidad de escribir está activada, la redirección de unidad podría dañar una unidad que no ha sido bloqueada.
7. Utilice el botón “Disconnect” (Desconectar) para detener una redirección de unidad después de que el proceso haya comenzado.
8. Haga clic en “Exit” (Salir) para cerrar el programa de redirección de unidad. Si está activa una conexión de redirección de unidad, la conexión se cerrará antes de que la aplicación termine.
9. Utilice el botón “Hide to Tray” (Ocultar de la bandeja) para minimizar la aplicación sin terminarla completamente. Una conexión activa permanecerá hasta que cierre la aplicación. Puede acceder al software haciendo doble clic en su icono de la bandeja. El icono de la bandeja también indica si se ha establecido o no una conexión. Haga clic con el botón derecho para acceder al submenú.

Opciones

Disable Drive Redirection - Desactivar la redirección de unidad
Esto desconecta la redirección de unidad.

Force Read-Only Connections - Obligar a que las conexiones sean solo de lectura
Esto desconecta la capacidad de escribir de la redirección de unidad.

Haga clic en “Apply” (Aplicar) para enviar sus cambios.

P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:36:08 AM

Creación de una imagen

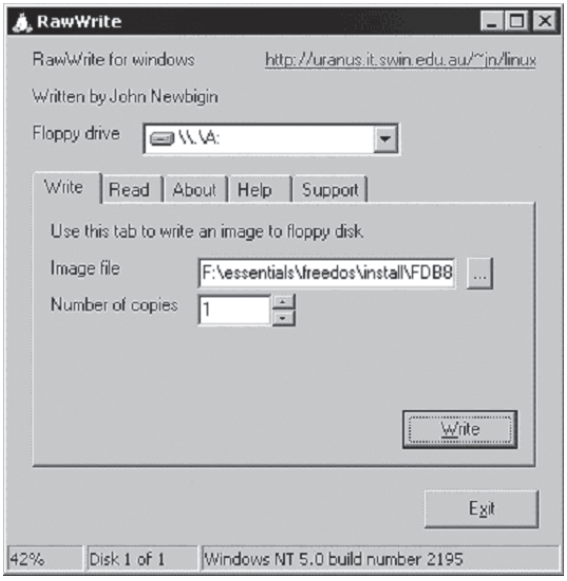
Imágenes de disquete

Sistemas operativos UNIX® y semejantes a UNIX

Para crear el archivo de una imagen, utilice “dd”. Esta una de las utilidades originales de UNIX y se incluye en todos los sistemas operativos semejantes a UNIX (UNIX, Sun Solaris, Linux). Para crear el archivo de imagen de un disquete, copie el contenido del disquete en un archivo. Puede utilizar el siguiente comando: dd [if=/dev/fd0] [of=/tmp/floppy.image]. En este caso, “dd” lee el disco entero del dispositivo “/dev/fd0” y guarda el resultado en el archivo específico de salida “/tmp/floppy.image”. Ajuste ambos parámetros exactamente a sus necesidades (dispositivo de entrada, etc.).

MS Windows

Puede utilizar la herramienta “RawWrite para Windows”.



Seleccione la pestaña “Read” (Leer) del menú. Introduzca (o elija) el nombre del archivo en el que quiere guardar el contenido del disquete. Haga clic en el botón “Copy” para iniciar el proceso de creación de imágenes. Para herramientas similares, consulte la página web del “Proyecto fdos” **(http://www.fdos.org).**

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:36:08 AM

Imágenes de CD-ROM/ISO 9660

Sistemas operativos UNIX y semejantes

Para crear un archivo de imagen, utilice “dd”. Esta una de las utilidades originales de UNIX y se incluye en todos los sistemas operativos semejantes a UNIX (UNIX, Sun Solaris, Linux). Para crear el archivo de imagen de un CD-ROM, copie el contenido del CD-ROM en un archivo. Puede utilizar el siguiente comando:

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

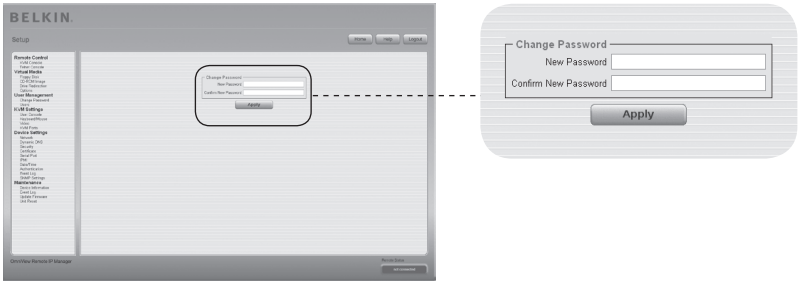
En este caso, “dd” lee el disco entero del dispositivo “/dev/cdrom” y guarda el resultado en el archivo específico de salida “/tmp/cdrom.image”. Ajuste ambos parámetros exactamente a sus necesidades (dispositivo de entrada, etc.).

MS Windows

Para crear el archivo de imagen, utilice la herramienta de imagen de CD. Copie en su disco duro todo el contenido del CD en un solo archivo de imagen ISO. Por ejemplo, con “Nero”, elija “Copy and Backup”, y diríjase a la sección “Copy Disc”. Seleccione la unidad de CD-ROM o DVD en la que se encuentra el disco del que desea crear una imagen ISO. Especifica el nombre del archivo de la imagen ISO y guarde el contenido del CD-ROM en ese archivo.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:36:08 AM

Cambio de contraseña

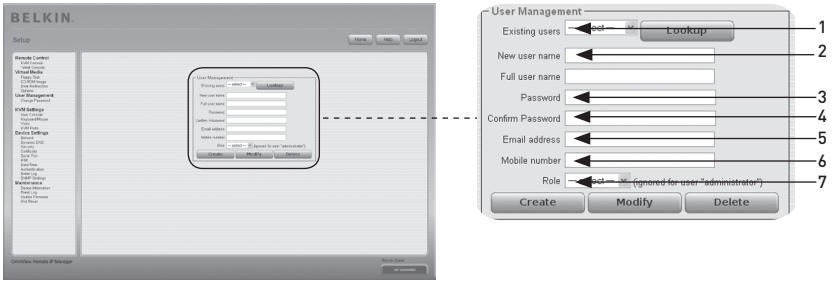


Para cambiar su contraseña, escriba la nueva contraseña en el cuadro superior. Repita la contraseña en el cuadro de debajo.

Haga clic en “Apply” (Aplicar) para enviar sus cambios.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:36:09 AM

Usuarios



Gestión de usuario

El RIPM dispone de una cuenta de usuario preconfigurada para el administrador que tiene permisos fijos. Este usuario tiene todos los derechos posibles para configurar el dispositivo y utilizar todas las funciones que ofrece el RIPM. Cuando se entrega, la cuenta tiene como nombre de usuario “administrator” y la contraseña es “belkin”. Asegúrese de cambiar la contraseña inmediatamente después de haber instalado su RIPM y haber accedido por primera vez. A continuación se muestra una lista completa de las opciones disponibles. Esta lista solo puede verla el administrador.

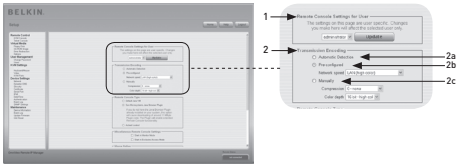
1. **Existing Users - Usuarios existentes**
   Seleccione un usuario existente para modificarlo. Una vez que ha sido seleccionado un usuario, haga clic en el botón de “lookup” (consultar) para ver la información de usuario.
2. **New Username - Nuevo nombre de usuario**
   El nuevo nombre de usuario para la cuenta seleccionada.
3. **Password - Contraseña**
   La contraseña del nombre de usuario. Deberá contener al menos cuatro caracteres.
4. **Confirm Password - Confirmar contraseña**
   Confirmación de la contraseña anterior.
5. **Email Address - Dirección de correo electrónico**
   Este campo es opcional.
6. **Mobile Number - Número de móvil**
   Este campo también es opcional.
7. **Role - Grupo de usuarios**
   Además de ser administrador o usuario normal, cada usuario puede pertenecer a un grupo (en inglés “role”). Elija en el cuadro de selección el grupo de usuarios que prefiera.
   Para crear un nuevo usuario, pulse el botón “Create” (Crear). El botón “Modify” (Modificar) cambia los ajustes del usuario mostrados. Para borrar un usuario, pulse el botón “Delete” (Borrar).

   Nota: El RIPM dispone de una unidad de memoria y un procesador independientes del equipo, ambos con limitaciones en cuanto a procesamiento de instrucciones y capacidad de memoria. Para garantizar que el tiempo de respuesta sea aceptable, Belkin recomienda NO supere el número total de 25 usuarios conectados simultáneamente al RIPM. El espacio de memoria disponible en el RIPM depende de la configuración y el uso del RIPM (entradas de archivos de registro, etc.).

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:36:09 AM

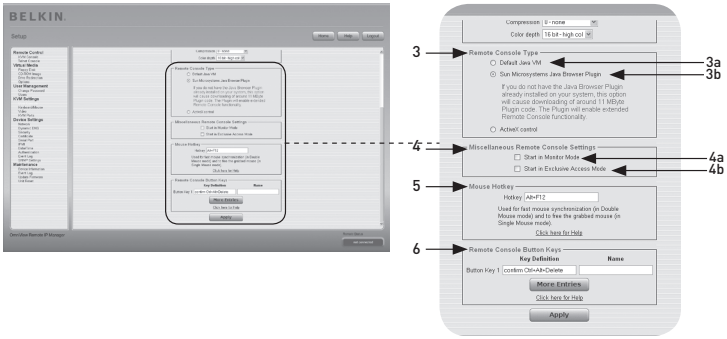
Consola de usuario

Los siguientes ajustes son específicos para cada usuario. Esto significa que el administrador puede personalizar estos ajustes para cada usuario por separado. Si cambia los ajustes para un usuario, esto no afectará a los ajustes para los otros usuarios.



1. **Remote Console Settings for User - Ajustes de Consola remota para usuario**
   Este cuadro de selección muestra la identificación del usuario al que corresponden los valores que se muestran y al que afectarán los cambios. Seleccione el usuario deseado en el cuadro de selección y pulse el botón "Update" (Actualizar). Al hacerlo se mostrarán los ajustes de usuario que se indican a continuación.
   Nota: Podrá realizar cambios en los ajustes de otros usuarios solamente si tiene los derechos de acceso necesarios para esta tarea. Esto no es posible para un usuario normal sin los permisos requeridos para cambiar los ajustes para cualquiera de los otros usuarios.
2. **Transmission Encoding - Codificación de la transmisión**
   El ajuste de codificación de la transmisión "Transmission Encoding" le permite modificar el algoritmo de codificación de imagen empleado para transmitir los datos de vídeo a la ventana de la Consola remota. Con estos ajustes es posible mejorar la velocidad de la pantalla remota dependiendo del número de usuarios que haya trabajando simultáneamente y del ancho de banda de la línea de conexión (módem, ISDN, DSL, LAN, etc.).
   2a. Automatic Detection - Detección automática
   El nivel de compresión y la codificación se determinan automáticamente según el ancho de banda disponible y el contenido actual de la imagen de vídeo.
   2b. Pre-Configured Settings - Ajustes preconfigurados
   Los ajustes preconfigurados proporcionan el mejor resultado debido a que se han optimizado el ajuste de compresión y la resolución del color para la velocidad de red indicada.
   2c. Manual Configuration - Configuración manual
   Le permite ajustar la tasa de compresión y la resolución del color individualmente. Dependiendo de la tasa de compresión seleccionada, la transferencia de datos entre el RIPM y la Consola remota se realizará comprimida para ahorrar ancho de banda. Debido a que las tasas de compresión elevadas requieren mucho tiempo, no deben utilizarse cuando existen varios usuarios accediendo al RIPM simultáneamente. La resolución de color estándar es de 16 bits (65536 colores). El resto de resoluciones de color están dirigidas a conexiones de red más lentas, para lograr una transmisión de datos más rápida. Además, el nivel de compresión 0 (sin compresión) utiliza solo la resolución de color de 16 bits. Con menores anchos de banda, sólo se recomiendan 4 bits (16 colores) y 2 bites (escalas de cuatro grises) para la interfaz de escritorio normal. Las imágenes similares a las fotografías obtendrán mejores resultados con una resolución de color de 4 bits. La resolución de un bit (blanco y negro) solo debe utilizarse para conexiones de red extremadamente lentas.

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:36:10 AM



3. Remote Console Type - Tipo de Consola remota
Especifica qué visualizador de Consola remota se utilizará.

3a. Default Java Virtual Machine (JVM) - Máquina virtual Java (JVM) predeterminada
Esta función utiliza la JVM predeterminada de su buscador de Internet, bien la JVM de Microsoft para el Internet Explorer o la JVM de Sun.

3b. Sun Microsystems Java Browser Plug-In - Plug-in para buscador Java de Sun Microsystems
Este plug-in o componente adicional indica al buscador de Internet de su sistema de administración que utilice la JVM de Sun Microsystems. La JVM en el buscador se emplea para ejecutar el código para la ventana de la Consola remota, que es en realidad un Applet de Java. Si marca este recuadro por primera vez en su sistema de administración y el plug-in de Java apropiado aún no se encuentra instalado en su sistema, se descargará e instalará automáticamente. Sin embargo, para hacer posible la instalación, deberá hacer clic en “Yes” (Sí) en el cuadro de diálogo correspondiente. El volumen de la descarga es de aproximadamente 11 Mbps. La ventaja de descargar la JVM de Sun es que proporciona una JVM estable e idéntica para diferentes plataformas. El software de la Consola remota está optimizado para esta versión de JVM y ofrece una amplia gama de funciones cuando se ejecuta en ella.

4. Miscellaneous Remote Console Settings - Ajustes diversos de Consola remota

4a. Start in Monitor Mode - Empezar en modo de control
Este ajuste le permite seleccionar el valor inicial para el modo de control. De forma predeterminada, el modo de control está desactivado. Si lo activa, la ventana de la Consola remota se iniciará en la modalidad de solo lectura.

4b. Start in Exclusive-Access Mode - Empezar en modo de acceso exclusivo
Activa el modo de acceso exclusivo cuando se inicia la Consola remota. Al utilizar esta modalidad se obliga a cerrar las Consolas remotas de todos los otros usuarios. Ningún otro usuario podrá volver a abrir la Consola remota simultáneamente hasta que desactive esta opción o cierre su sesión.

5. Mouse Hot Key - Tecla de acceso de ratón
La tecla de acceso directo de ratón le permite asignar una combinación de teclas de acceso directo para iniciar el proceso de sincronización del ratón (introduciendo la combinación de teclas en la Consola remota) o para salir del modo de ratón único.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:36:11 AM

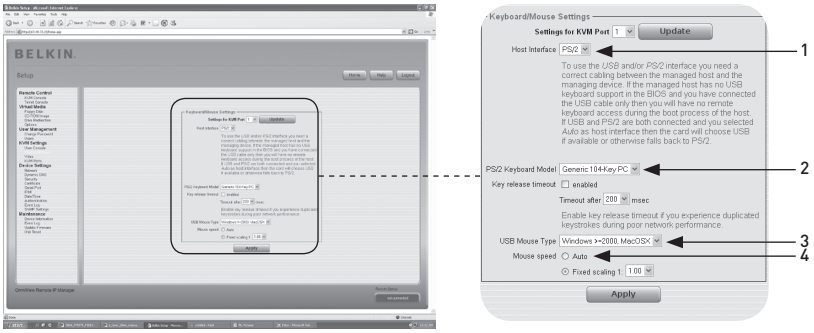
6. **Remote Console Button Keys - Teclas de botón de Consola remota**
   Las teclas de botón permiten simular pulsaciones del teclado en el sistema remoto que no se pueden realizar en el equipo local. Puede ser necesario si faltan teclas o si en el sistema operativo local de la Consola remota existe alguna combinación de teclas que ya está ocupada. Ejemplos frecuentes son las combinaciones “Control+Alt+Supr” en Windows y DOS, que siempre tienen ya su función, o la secuencia de teclas “Control+Tecla de retroceso” en Linux, que se puede utilizar para apagar el servidor X. Para definir una tecla de botón nueva, o para ajustar un existente, consulte las reglas que describen el ajuste de una tecla. En general, la sintaxis para una tecla es la siguiente:

   [confirm] <código de tecla>[+|-|<[*]<código de tecla>]*

   El término entre paréntesis es opcional. El asterisco al final significa que debe añadir más teclas, tantas como sea necesario en su caso. El término “confirm” añade un ventana de diálogo de confirmación que aparecerá antes de que la pulsación de teclas se pueda enviar al equipo remoto. El “código de tecla” es la tecla que se enviará. Los códigos con varias teclas pueden ser encadenados con un signo más, menos o un “<”. El signo más crea combinaciones de teclas, todas las teclas deben permanecer pulsadas hasta un signo menos o al final de la combinación. En este caso, todas las teclas deben soltarse en orden inverso al de pulsado. Por el contrario, el signo menos hace que las teclas se pulsen y suelten de forma única, por separado. El signo “<” hace que se suelte solo la última tecla. El asterisco introduce una pausa con duración de 100 milisegundos. Por ejemplo, la combinación de teclas Ctrl, Alt, y F2 se representa mediante la secuencia “Ctrl+Alt+F2”.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:36:11 AM

Teclado/ratón



1. **Host Interface - Interfaz del equipo**
   La interfaz de equipo activa la interfaz a la que está conectado el ratón. Puede elegir “Auto” para la detección automática, “USB” para un ratón USB, o “PS/2” para un ratón PS/2.

   Nota: Para utilizar la interfaz USB o la PS/2, necesita usar el cableado correcto entre el equipo que se gestiona y el dispositivo de gestión. Por ejemplo, si el equipo que se gestiona no tiene soporte para teclado USB en la BIOS y únicamente ha conectado el cable USB, entonces no tendrá acceso al teclado remoto durante el proceso de arranque del equipo. Si están conectados USB y PS/2 y selecciona “Auto” como interfaz del equipo, se seleccionará USB en el arranque si está disponible. Si USB no está disponible, se seleccionará “PS/2”

   Para tener acceso al teclado USB remoto durante el proceso de arranque del equipo, se deben cumplir las siguientes condiciones:

   - la BIOS del equipo debe permitir la utilización de un teclado USB
   - el cable USB debe conectarse o seleccionarse en la opción “Host Interface” (Interfaz del equipo).

2. **PS/2 Keyboard Model - Modelo de teclado PS/2**
   Le permite elegir una configuración de teclado entre “Generic 101-Key PC” para un teclado estándar, “Generic 104-Key PC” para un teclado estándar ampliado con tres teclas de Windows adicionales, “Generic 106-Key PC” para un teclado japonés, y “Apple Macintosh” para el teclado ordenador Macintosh®. Si necesita un tiempo límite de inactividad para el teclado, seleccione la opción apropiada y ajuste el valor de tiempo en el cuadro inferior.

3. **USB Mouse Type - Tipo de ratón USB**
   Activa el tipo de ratón USB. Elija la opción adecuada del cuadro de selección. Para ver una descripción detallada del tipo de ratón y las opciones recomendadas para los diferentes sistemas operativos, consulte la sección “Ajustes de ratón recomendados” en la página 21 de este Manual del usuario.*

*Esta opción solo funciona con el sistema operativo Windows.

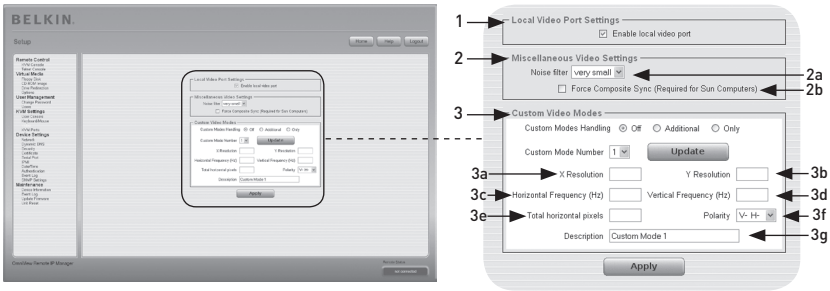
P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:36:11 AM

4. **Mouse Speed - Velocidad de ratón**
   - **Auto Mouse Speed - Velocidad de ratón automática**
     Utilice esta opción si los ajustes de ratón del equipo utilizan un ajuste de aceleración adicional. El RIPM detecta la aceleración y velocidad del ratón durante el proceso de sincronización del ratón.
   - **Fixed Mouse Speed - Velocidad de ratón fija**
     Utilice esta opción para un traslado directo de los movimientos del ratón entre el puntero remoto y el local. También puede establecer una escala fija que determine la cantidad de píxeles que se mueve el puntero del ratón remoto cuando el puntero del ratón local se mueve un píxel. Esta opción solo funciona cuando los ajustes de ratón en el equipo son uniformes, es decir, cuando no existe aceleración de ratón.

   Para fijar las opciones, haga clic en el botón “Apply” (Aplicar).

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:36:12 AM

Vídeo



Para fijar las opciones (descritas a continuación), haga clic en el botón “Apply” (Aplicar).

1. **Local Video Port Settings - Ajustes del puerto de vídeo local**
   Enable Local Video Port - Activar el puerto de vídeo local
   Esta opción controla la salida de vídeo local del RIPM, e indica si está activo y transmitiendo la señal de entrada del sistema del equipo.
2. **Miscellaneous Video Settings - Ajustes diversos de vídeo**
   2a. Noise Filter - Filtro de ruido
   Esta opción define cómo reacciona el RIPM a los pequeños cambios en la señal de entrada de vídeo. Un ajuste de mayor filtro necesita menor tráfico de red y contribuye a una mayor rapidez del vídeo, pero los pequeños cambios pueden que no se reconozcan de inmediato en algunas regiones. Un filtro más estricto indica todos los cambios instantáneamente pero puede provocar una cantidad constante de tráfico de red, incluso cuando el contenido de la pantalla no está cambiando realmente (dependiendo de la calidad de la señal de entrada de vídeo).
   2b. Force Composite Sync (Required for Sun Computers) - Obligar a que se sincronice el sistema de vídeo compuesto (necesario para ordenadores Sun)
   Para hacer posible la transmisión de la señal desde una máquina Sun, active esta opción. Si esta función no está activada, no podrá mostrarse la imagen de la Consola remota.
3. **Custom Video Modes -Modos de vídeo personalizados**
   El número máximo de resoluciones de vídeo que se pueden personalizar es cuatro.
   La opción “Custom Modes Handling” (Gestión de modos personalizados) le permite desactivar los modos personalizados (“Off”), o establecer resoluciones generales o individuales (“Only”). Una opción final (“Additional”, Adicional) le permite fijar una modalidad de vídeo especial para el RIPM. Para cambiar los parámetros de la modalidad de vídeo personalizado, elija el número correcto del cuadro de selección y pulse el botón “Update” (Actualizar). Se le pedirá que proporcione información adicional para que pueda reconocerse correctamente la modalidad de vídeo:
   Advertencia: La opción “Host Monitor Settings” (Ajustes de monitor del equipo) solo es para usuarios avanzados. Si se utiliza incorrectamente puede afectar al rendimiento de la transmisión de vídeo. Debe estar seguro de que comprende totalmente esta función antes de intentar ajustar los ajustes de monitos del equipo.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:36:12 AM

3a. X Resolution - Resolución en el eje X
Corresponde al número visible de píxeles horizontales.

3b. Y Resolution - Resolución en el eje Y
Corresponde al número visible de píxeles verticales.

3c. Horizontal Frequency (Hz) - Frecuencia horizontal (Hz)
Corresponde a la frecuencia horizontal (línea) en hercios.

3d. Vertical Frequency (Hz) - Frecuencia vertical (Hz)
Corresponde a la frecuencia vertical (actualización) en hercios.

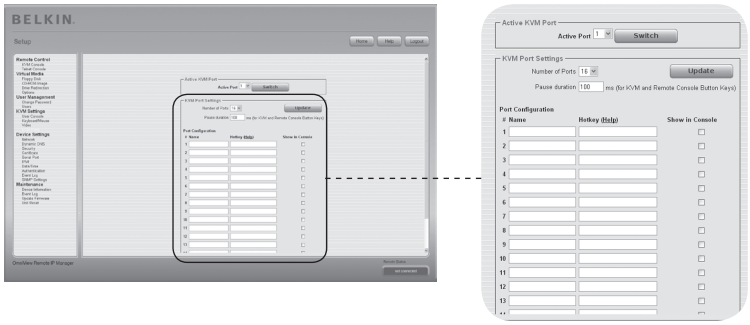
3e. Total horizontal pixels - Total de píxeles horizontales
Corresponde al número total de píxeles por línea, incluidas las zonas en blanco y no visibles.

3f. Polarity - Polaridad
Corresponde a la característica negativa o positiva de las señales de sincronización. V indica polaridad vertical; H indica polaridad horizontal.

3g. Description - Descripción
Aquí puede escribir el nombre de la modalidad, que aparecerá en la Consola remota si el modo personalizado está activado.

Puertos KVM

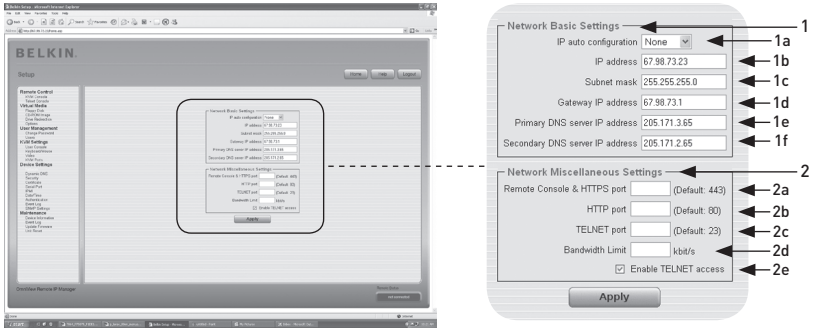
Es posible seleccionar el número de puertos utilizados por el conmutador KVM conectado y puede asignar un nombre a cada puerto. Con el fin de permitir la conmutación de puertos KVM a través del RIPM, será preciso definir para los mismos las combinaciones de teclas.



P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:36:13 AM

Red

El panel de ajustes de red “Network Settings” (se muestra a continuación) le permite cambiar los parámetros relacionados con la red, como se explica más adelante. Cuando se haya aplicado, los nuevos ajustes de red se harán efectivos inmediatamente.



Advertencia: Al cambiar los ajustes de red del RIPM se podría perder la conexión con la red. Si modifica los ajustes a distancia, asegúrese de que todos los valores sean correctos para poder seguir accediendo al RIPM.

1. **Basic Network Settings - Ajustes de red básicos**
   - **1a. IP Auto Configuration - Configuración automática de IP**
     Con esta opción, puede definir una ubicación desde la que el RIPM toma sus ajustes de red, bien un servidor DHCP o BOOTP. Para DHCP, seleccione “DHCP”; para BOOTP, seleccione “bootp”. Si puede elegir “none”, la configuración automática de IP está desactivada.
   - **1b. La dirección IP** la asigna su administrador de red.
   - **1c.** El término **“Subnet Mask” (Máscara de subred)** se refiere a la máscara de red de la red local, que se utilice para determinar a quien pertenece la dirección de IP.
   - **1d. Gateway IP Address - Dirección IP de pasarela**
     Si el RIPM debe ser accesible desde otras redes distintas a la red local, establezca esta dirección IP para la dirección IP del router de la red local.
   - **1e. Primary DNS Server IP Address - Dirección IP del servidor DNS primario**
     Esta es la dirección IP del Servidor de nombres de dominio (DNS) primario en notación de puntos. Puede dejar esta opción en blanco, sin embargo, si lo hace, el RIPM no podrá ofrecer la resolución correspondiente.
   - **1f. Secondary DNS Server IP Address - Dirección IP de servidor DNS secundario**
     Este término se refiere a la dirección IP del Servidor de nombres de dominio (DNS) secundario en notación de puntos. Se utilizará en caso de que no se pueda establecer contacto con el Servidor de nombres de dominio (DNS) primario.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:36:14 AM

2. Network Miscellaneous Settings - Ajustes diversos de red

2a. Remote Console and HTTPS Port - Consola remota y puerto HTTPS
Este es el número de puerto al que están vinculados el servidor de la Consola remota del RIPM y el servidor HTTPS. Si se deja en blanco, se utilizará el valor predeterminado.

2b. HTTP Port - Puerto HTTP
Este es el número de puerto con el que se comunica el servidor HTTP del RIPM. Si se deja en blanco, se utilizará el valor predeterminado.

2c. Telnet Port - Puerto Telnet
Este es el número de puerto con el que se comunica el servidor Telnet del RIPM. Si se deja en blanco, se utilizará el valor predeterminado.

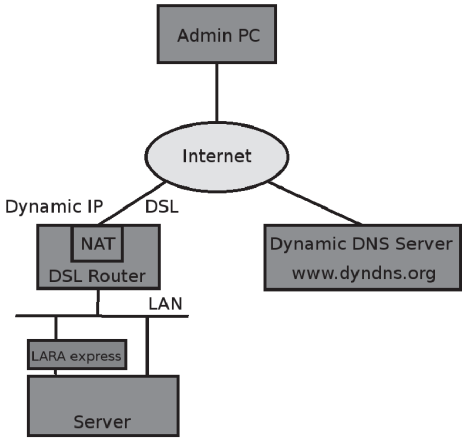
2d. Bandwidth Limit - Límite de ancho de banda
Esta opción se refiere al tráfico de red máximo generado a través del dispositivo de Ethernet del RIPM (valor en Kbps).

2e. Enable Telnet Access - Activar el acceso a Telnet
Establezca esta opción para permitir a los usuarios que accedan al RIPM utilizando Telnet (consulte la sección “Consola Telnet” en la página 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:36:14 AM

DNS dinámico

Se puede utilizar un servicio disponible gratuito se servidor DNS dinámico (dyndns.org) en el siguiente entorno:



Entorno DNS dinámico

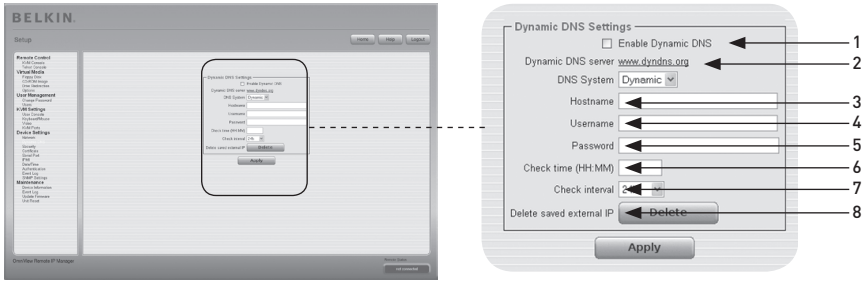
Puede acceder al RIPM mediante la dirección IP del router DSL, que la asigna dinámicamente el proveedor. Como el administrador no conoce la dirección IP asignada por el proveedor, el RIPM se conecta a un DNS dinámico especia en intervalos regulares y registra su dirección IP allí. El administrador también puede contactar con este servidor y tomar la misma dirección IP que pertenece al NIC. El administrador debe registrar el RIPM para utilizar el servicio con el DNS dinámico y asignarle un nombre de equipo determinado. Se asignarán un nombre de usuario y contraseña durante el proceso de registro. Esta información de cuenta junto con el nombre del equipo es necesaria para determinar la dirección IP del RIPM registrado.

Debe llevar a cabo los pasos siguientes para activar el DNS dinámico:

- Asegúrese de que la interfaz LAN del RIPM está correctamente configurada.
- Introduzca los datos en el cuadro de configuración de ajustes de DNS dinámico como se indica en la página 55.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:36:14 AM

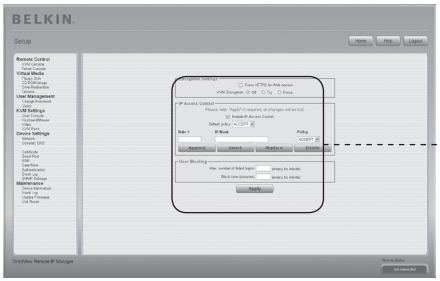
Dynamic DNS Settings - Ajustes de DNS dinámico



1. **Enable Dynamic DNS - Activar DNS dinámico**
   Activa el servicio de DNS dinámico. Esto requiere una dirección IP de servidor DNS configuradas.
2. **Dynamic DNS Server - Servidor DNS dinámico**
   El RIPM se registra en intervalos regulares en esta ubicación. En el momento de la publicación de este Manual del usuario, el DNS dinámico es un ajuste fijo ya que en la actualidad solo admite dyndns.org.
3. **Host Name - Nombre del equipo**
   RIPM es el nombre del equipo que proporciona el DNS dinámico. Utilice el nombre entero, incluido el dominio, p. ej. “testserver.dyndns.org” (o “RIPM. dyndns.org”), y no solo el nombre del equipo propiamente dicho.
4. **Username - Nombre de usuario**
   Durante su registro manual con el DNS dinámico, debe haber registrado este número de usuario.
   Nota: No se pueden incluir espacios en el nombre de usuario.
5. **Password - Contraseña**
   Durante su registro manual con el DNS dinámico, debe haber designado esta contraseña.
6. **Check Time - Momento de comprobación**
   La tarjeta del RIPM se registra en el DNS dinámico en el momento que fije para la comprobación, “Check Time”.
7. **Check Interval - Intervalo de comprobación**
   Es el intervalo para los envíos de informes del RIPM al DNS dinámico.
   Nota: El RIPM tiene su propio reloj independiente. Compruebe que la hora del RIPM está ajustada correctamente.
8. Utilice la práctica opción **“Delete saved external IP” - Borrar IP externas guardadas** si quiere actualizar sus direcciones IP guardadas externamente. Para borrar la dirección guardada, pulse el botón “Delete” (Borrar).

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:36:15 AM

Seguridad



1. **Encryption Settings - Ajustes de cifrado**
   - **1a. Force HTTPS - HTTPS obligatorio**
     Cuando se encuentra activada esta opción, el acceso a la portada de web sólo será posible utilizando una conexión HTTPS. El RIPM no se "comunicará" mediante el puerto HTTP con las conexiones entrantes. En caso de que quiera crear su propio certificado SSL que puede utilizarse para identificar el RIPM, consulte la sección "Certificado" en la página 58.
   - **1b. KVM Encryption - Cifrado de KVM**
     Esta opción controla el cifrado del protocolo RFB (Remote Frame Buffer). La Consola remota utiliza el protocolo RFB para transmitir los datos de la pantalla a la máquina del administrador, y enviar los datos del ratón y el teclado al equipo. Si se selecciona "Off", no se utilizará cifrado. Si selecciona "Try" (Intentar), el Applet tratará de realizar una conexión con cifrado. Si la conexión no puede establecerse, se utilizará en su lugar una conexión sin cifrado. Si selecciona "Force" (Obligar), el Applet tratará de realizar una conexión con cifrado. Si la conexión falla, el sistema genera un informe de error.
2. **IP-Access Control - Control de acceso IP**
   Esta sección explica los ajustes referentes al control de acceso IP. Se utiliza para limitar el acceso a un número de determinados clientes. Estos clientes se identificarán mediante las direcciones IP desde las cuales están intentando realizar las conexiones.
   Advertencia: Los ajustes de control de acceso IP se aplican solo a la interfaz LAN.
   - **2a. Enable IP-Access Control - Activar el control de acceso IP**
     Activa el control de acceso basado en las direcciones IP de origen.
   - **2b. Default Policy - Política por defecto**
     Esta opción controla qué hace cuando llegan paquetes IP que no coinciden con las reglas establecidas. Pueden aceptarse o rechazarse.
     Advertencia: Si establece está opción en "DROP" (Eliminar) y no tiene reglas configuradas con "ACCEPT" (Aceptar) , el acceso a la portada web a través de la LAN será imposible. Para activar de nuevo el acceso, puede modificar los ajustes de seguridad a través del módem o desactivando temporalmente el control de acceso IP con el procedimiento de configuración inicial
   - **2c. Rule Number - Número de regla**
     Aquí debe incluirse el número de una norma para la cual se aplicarán las siguientes instrucciones. En caso de que esté añadiendo una nueva regla, omita rellenar este campo.

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:36:15 AM

2d. IP/Mask - Máscara/IP
Especifica la dirección IP o el intervalo de dirección IP para el cual se aplica la regla. En los siguientes ejemplos, el número encadenado a una dirección IP por medio de un " / " representa el número de bits válidos de la dirección IP proporcionada que se utilizará:

192.168.1.22/32 se corresponde con la dirección IP 192.168.1.22
192.168.1.0/24 se corresponde con todos los paquetes IP con direcciones de origen desde 192.168.1.0 hasta 192.168.1.255
0.0.0.0/0 no se corresponde con ningún paquete IP

2e. Policy - Política
La política determina qué hacer con los paquetes que coinciden. Pueden aceptarse o rechazarse.

Advertencia: El orden de las reglas es importante. La reglas se comprueban en orden ascendente hasta que una regla coincide. Se hará caso omiso de todas las reglas siguientes que coincidan. La política por defecto se aplica si no se ha encontrado correspondencia.

2f Appending a Rule- Añadido de una regla
Introduzca la máscara/IP y establezca la política. Finalmente, pulse el botón "Append" (Añadir).

2g. Inserting a Rule - Introducción de una regla
Introduzca el número de la regla y la máscara/IP. Establezca la política. Finalmente, pulse el botón "Insert" (Introducir).

2h. Replacing a Rule - Sustitución de una regla
Introduzca el número de la regla y la máscara/IP. Establezca la política. Finalmente, pulse el botón "Replace" (Sustituir).

2i. Deleting a Rule - Borrado de una regla
Introduzca el número de la regla y pulse el botón "Delete" (Borrar).

3. User Blocking - Bloqueo de usuario
El mecanismo de bloqueo del usuario permite al administrador desactivar el acceso de un usuario determinado si su contraseña se ha introducido incorrectamente un cierto número de veces. La duración del bloqueo también se puede configurar.

3a. Maximum Number of Failed Logins - Número máximo de accesos fallidos
Introduzca el número máximo de accesos fallidos después de los cuales se bloquea al usuario. Deje este campo en blanco para desactivar la función de bloqueo de usuario.

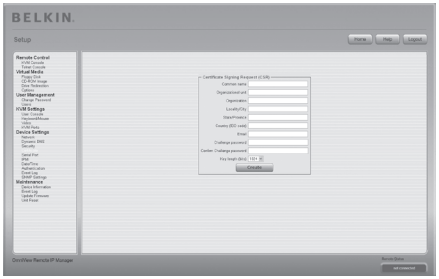
3b. Block Time - Duración de bloqueo
El número de minutos que se bloquea al usuario después de que haya excedido el número máximo de intentos de acceso fallidos. Deje este campo en blanco para bloquear al usuario hasta que se quiera desbloquear manualmente.

Unblocking Users - Desbloqueo de usuario
Existen dos posibilidades para desbloquear a un usuario bloqueado:

- Un usuario con los permisos necesarios puede dirigirse a los ajustes de gestión de usuario (consulte la sección "Gestión de usuario") y pulsar el botó "Unblock" (Desbloquear) para cancelar el bloqueo al usuario.
- Un administrador puede utilizar la consola serie para la configuración inicial y acceder como el usuario "unblock". El RIPM pedirá la contraseña del administrador y mostrará una lista de los usuarios bloqueados que pueden desbloquearse.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:36:16 AM

Certificado



Ajustes de certificado

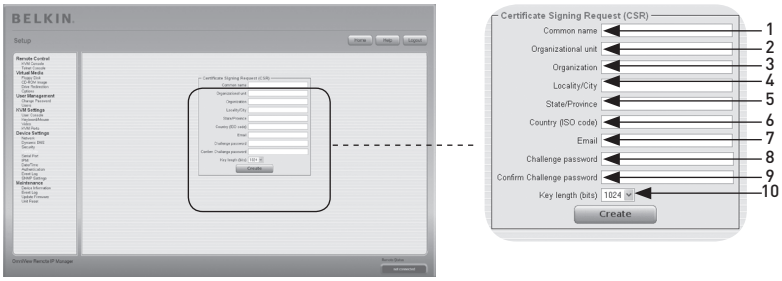
El RIPM emplea el protocolo SSL para todo el tráfico de red cifrado entre el propio RIPM y un cliente conectado. Durante el establecimiento de la conexión, el RIPM deberá revelar su identidad a un cliente empleando un certificado criptográfico. Antes de la entrega, este certificado y la clave secreta subyacente serán idénticos para todos los RIPM fabricados y no corresponderá con la configuración de red que el usuario aplicará al RIPM. La clave secreta subyacente del certificado también se utiliza para la seguridad en el establecimiento de comunicación SSL. Es posible generar e instalar un certificado nuevo X.509 codificado en base 64 que sea exclusivo para un RIPM en particular. Para ello, el RIPM puede generar una nueva clave criptográfica y el CSR (Certificate Signing Request) que necesita ser certificado por una autoridad de certificación (CA). Una CA o autoridad de certificación verifica que usted es quien dice ser y firma y emite un certificado SSL para usted. Para crear e instalar un certificado SSL para el RIPM, haga lo siguiente:

- Cree una CSR SSL utilizando el panel que se muestra en la siguiente ilustración. Necesita rellenar un varios campos, cada uno de los cuales se explica a continuación. Una vez realizado esto, haga clic en el botón “Create” (Crear), esto iniciará la solicitud de firma de certificado CSR. La CSR puede ser descargada en su equipo de administración utilizando el botón “Download CSR” (Descargar CSR).
- Envíe la CSR guardad a una CA para su certificación. Obtendrá el nuevo certificado de la CA.
- Cargue el certificado en el RIPM utilizando el botón “Create” (Crear).

Despuéde de haber completado estos tres pasos, el RIPM tendrá su propio certificado que identificará a la tarjeta para sus clientes.

Advertencia: Si destruye la CSR del RIPM, no habrá forma de recuperarla. Si la borra por error, repita los tres pasos descritos anteriormente.

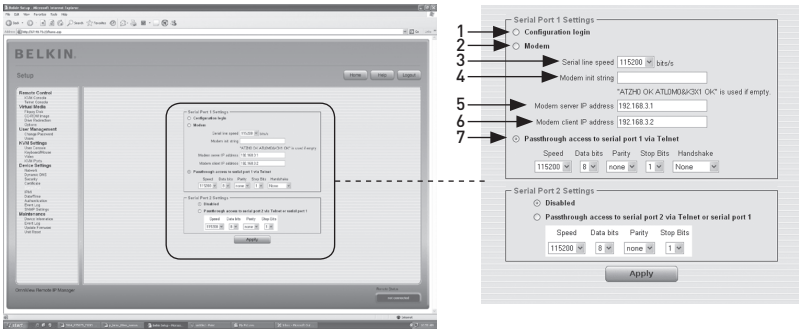
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:36:17 AM



1. **Common Name - Nombre común**
   Este es el nombre de red del RIPM una vez instalado en la red del usuario (normalmente el nombre de dominio correcto completo). Es idéntico al nombre que se ha utilizado para acceder al RIPM con un buscador de Internet pero sin el prefijo “http://”. Si se accede al RIPM utilizando HTTPS y el nombre que se da aquí y el nombre de la red son distintos, aparecerá en el buscador una advertencia de seguridad.
2. **Organizational Unit - Unidad organizativa**
   En este campo se especifica a qué departamento de la organización pertenece el RIPM.
3. **Organization - Organización**
   El nombre de la organización a la que pertenece RIPM.
4. **Locality/City - Localidad/Ciudad**
   La ciudad en la que se encuentra la organización.
5. **State/Province - Estado/Provincia**
   El estado o provincia donde se encuentra la organización.
6. **Country (ISO Code) - País (Código ISO)**
   El país en el que se encuentra la organización (en código ISO de 2 letras, p. ej. ES para España).
7. **Challenge Password - Contraseña para cambios**
   Algunas autoridades de certificación requieren una contraseña adicional para autorizar posteriores modificaciones en el certificado (p. ej. la revocación del certificado). La longitud mínima de esta contraseña es de cuatro caracteres.
8. **Confirm Challenge Password - Confirmar la contraseña para cambios**
   Es necesario que vuelva a introducir la contraseña para cambios.
9. **Email - Correo electrónico**
   Se refiere a la dirección de correo electrónico de una persona de contacto que es la responsable del RIPM y su seguridad.
10. **Key Length - Longitud de la clave**
    Esta es la longitud en bits de la clave generada. En la mayoría de los casos , es suficiente con 1.024 bits. Las claves más largas pueden provocar que aumente el tiempo de respuesta del RIPM durante el establecimiento de la conexión.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:36:17 AM

Puerto Serie



Los ajustes Serie del RIPM le permiten especificar qué dispositivo está conectados al puerto Serie y cómo utilizarlo. Para acceder a la interfaz Serie, se necesita un cable de módem null.

1. **Configuration Login - Acceso de configuración**
   No utilice el puerto Serie para ninguna función especial, utilícelo solo para la configuración inicial.
2. **Modem - Módem**
   El RIPM ofrece acceso remoto utilizando una línea de teléfono además del acceso estándar a través del adaptador de Ethernet incorporado. El módem necesita conectarse a la interfaz Serie del RIPM. Conectarse al RIPM utilizando una línea de teléfono únicamente supone el establecimiento de una conexión punto a punto exclusiva de su ordenador al RIPM. En otras palabras, el RIPM actúa como una proveedor de servicios de Internet (ISP) al que se puede acceder mediante la línea de teléfono. La conexión se establece utilizando el protocolo punto a punto (PPP). Antes de conectarse al RIPM, asegúrese de haber configurado el ordenador correctamente. Por ejemplo, en los sistemas operativos Windows, puede configurar una conexión de red telefónica que utilice de forma predeterminada los ajustes correctos (como PPP). El panel de ajustes del módem le permite configurar el acceso a distancia al RIPM utilizando un módem. El significado de cada parámetro se describe a continuación. Los ajustes del módem son parte del panel de ajustes Serie.
3. **Serial-Line Speed - Velocidad de línea Serie**
   La velocidad a la que el RIPM está comunicándose con el módem. La mayoría de los módems disponibles en la actualidad admiten el valor predeterminado de 115.200 bps. Si está utilizando un módem antiguo y aparecen problemas, pruebe a bajar esta velocidad.
4. **Modem Init String - Secuencia de inicio de módem**
   La secuencia de inicialización empleada por el RIPM para inicializar el módem. El valor predeterminado funcionará con todos los módems estándares directamente conectados a la línea de teléfono. Si dispone de un módem especial o si su módem está conectado a un conmutador de teléfono local que requiera una secuencia de marcado especial para establecer una conexión con la red de teléfono pública, podrá modificar este ajuste utilizando una nueva secuencia. Consulte en el manual de su módem la sección sobre los comandos AT.

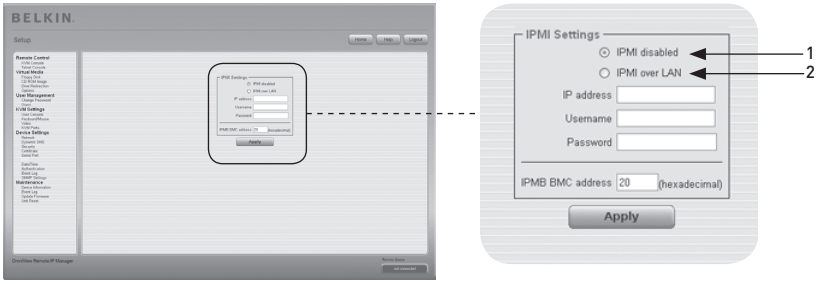
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:36:18 AM

5. **Modem Server IP Address - Dirección IP del servidor del módem**
   Esta dirección IP se asignará al propio RIPM durante el establecimiento de comunicación PPP. Debido a que se trata de una conexión IP punto a punto, es posible asignar prácticamente cualquier dirección IP, pero deberá asegurarse de que no interfiera con los ajustes IP del RIPM y de su ordenador de consola. El valor predeterminado funcionará en la mayoría de los casos.
6. **Modem Client IP Address - Dirección IP de cliente del módem**
   Esta dirección IP se asignará al ordenador de su consola durante el establecimiento de comunicación PPP. Debido a que se trata de una conexión IP punto a punto, es posible asignar prácticamente cualquier dirección IP, pero deberá asegurarse de la IP asignada que no interfiera con los ajustes IP del RIPM y de su ordenador de consola. El valor predeterminado funcionará en la mayoría de los casos.
7. **Pass-Through Access to Serial Port via Telnet - Acceso de paso al puerto Serie a través de Telnet**
   Utilizando esta opción es posible conectar un dispositivo cualquiera al puerto Serie y acceder al mismo (suponiendo que proporcione soporte a la terminal) a través de Telnet. Seleccione las opciones apropiadas para el puerto serie y emplee la consola Telnet o un cliente Telnet estándar para conectar con el RIPM. Para obtener más información sobre la interfaz Telnet, consulte la sección “Consola Telnet”.

   Nota: Puede consultar una lista de módems compatibles en www.belkin.com.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:36:18 AM

IPMI (Interfaz de gestión de plataforma inteligente)



Las funciones IPMI del RIPM ofrecen una manera adicional de conectar o desconectar el sistema o para forzar un reinicio. Además, estas funciones le permiten consultar el registro de sucesos del sistema del equipo y el estado de algunos sensores del sistema (p. ej., de temperatura). Si su equipo admite IPMI, puede acceder a esta interfaz de una de las siguientes maneras:

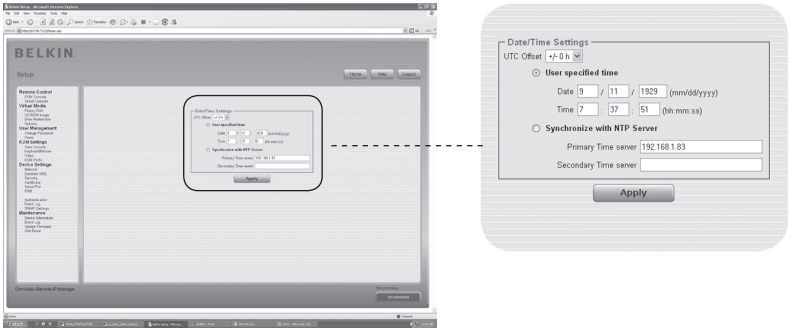
- IPMI a través de LAN (se requiere IPMI v1.5)
- Ajustes IPMI

La ilustración anterior muestra el panel de ajustes IPMI del RIPM. Sus opciones se explican a continuación.

1. **IPMI Disabled - IPMI desactivada**
   Desactiva la interfaz IPMI del RIPM. Esto significa que el Estado mediante IPMI y el Registro de sucesos mediante IPMI no están disponibles; las funciones de conexión/desconexión y de reinicio no utiliza IPMI en lugar de la ATX (Advanced Technology Extended), y el cable de reinicio está conectado del RIPM a la placa base.
2. **IPMI over LAN - IPMI mediante LAN**
   También puede conectar IPMI a través de una conexión LAN. El prerrequisito para este tipo de acceso es un sistema en el equipo con IPMI v1.5 y un adaptador de red con conexión de banda lateral al controlador de gestión de placa (BMC) (en la mayoría de los casos en la placa). En los ajustes IPMI, debe introducir la dirección IP de este equipo y la contraseña correcta para la conexión LAN. También puede acceder a otros sistemas IPMI introduciendo sus direcciones IP respectivas.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:36:19 AM

Fecha y hora

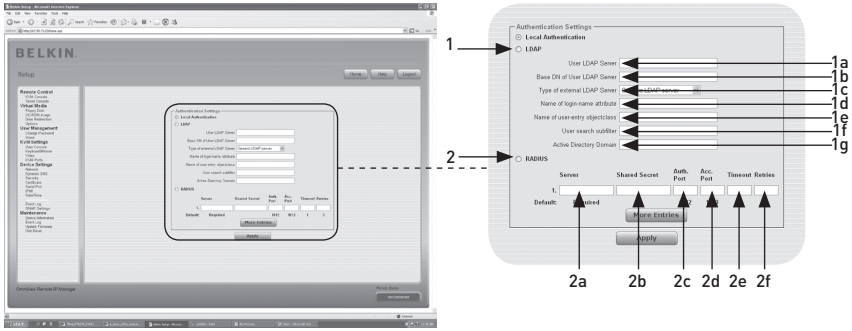


Este enlace se refiere a una página en la que se puede ajustar la hora del reloj del RIPM. Puede ajustar el reloj manualmente o utilizar un servidor de protocolo horario de red (NTP). Sin un servidor horario, su ajuste de hora no quedará de forma permanente, así que tendrá que ajustar la hora cada vez que el RIPM no reciba corriente durante más de unos pocos minutos. Para evitar esto, puede utilizar un servidor horario NTP, que ajusta el reloj interno de forma automática con el tiempo universal coordinado o CUT (Coordinated Universal Time). Debido a que la hora del servidor NTP corresponde siempre con el CUT, existe un ajuste que le permite establecer una diferencia fija para obtener su hora local.

Advertencia: Por el momento no existe un modo automático de ajustar la hora al horario de verano. Debe ajustar el diferencia con la hora CUT dos veces al año, según cambie la hora en su país.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:36:19 AM

Autenticación



El RIPM le permite utilizar su autenticación local o guardar la información en un LDAP (Protocolo ligero de acceso a directorios) o en un servidor RADIUS (Remote Authentication Dial-In User Service). Para LDAP o RADIUS, debe especificar cierta información en el panel de ajustes de autenticación. A continuación se ofrece más información sobre los ajustes LDAP y RADIUS.

1. LDAP

1a. User LDAP Server - Servidor LDAP de usuarios
Introduzca el nombre o dirección IP del servidor LDAP que contiene todas las entradas de los usuarios. Si elige un nombre en lugar de una dirección IP, necesitará configurar un servidor DNS en los ajustes de red.

1b. Base DN of User LDAP Server - DN base de servidor LDAP de usarios
Especifique el nombre correspondiente (DN) donde el árbol de directorio comienza en el servidor LDAP de usuarios.

1c Type of External LDAP Server - Tipo de Servidor externo LDAP
Establece el tipo de servidor LDAP externo. Esto es necesario porque algunos servidores necesitan un tratamiento especial. Además, los valores predeterminados para el esquema LDAP se ajustan correctamente. Puede elegir entre un servidor LDAP genérico, un Servicio de Directorio de Novell, y un Directorio Activo de Microsoft. Si no tiene un Servicio de Directorio de Novell ni un Directorio Activo de Microsoft, entonces elija un servidor LDAP genérico y modifique el esquema LDAP (vea a continuación).

1d. Name of Login-Name Attribute - Nombre de acceso - Nombre de atributo
Este es el nombre del atributo que contiene el nombre de acceso exclusivo de un usuario. Para utilizar el valor predeterminado, deje este espacio en blanco. El valor predeterminado depende del tipo de servidor LDAP seleccionado.

1e. Name of User-Entry Object Class - Nombre de usuario-Entrada de clase de objeto
Esta es la clase de objeto que identifica a un usuario en el directorio LDAP. Para utilizar el valor predeterminado, deje este espacio en blanco. El valor predeterminado depende del tipo de servidor LDAP seleccionado.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:36:20 AM

1f. User Search Sub-Filter - Filtro secundario de búsqueda de usuario
Aquí puede redefinir la búsqueda de usuarios que debería reconocer el RIPM.

1g. Active Directory Domain - Dominio de directorio activo
Esta opción representa el dominio de directorio activo que está configurado en el servidor de Directorio Activo de Microsoft. Esta opción solo es válida si ha elegido un Directorio Activo de Microsoft como tipo de servidor LDAP.

2. Remote Authentication Dial In User Service (RADIUS)
RADIUS es un protocolo de autenticación definido por el IETF (Grupo de Trabajo de Ingeniería de Internet). Existen dos especificaciones que constituyen el protocolo RADIUS: autenticación y administración. Estas especificaciones tienen como objetivo centralizar la autenticación, configuración y administración para servicios de acceso mediante línea telefónica a un servidor independiente. El protocolo RADIUS existe en varias implementaciones, como FreeRADIUS, OpenRADIUS abierto o RADIUS en sistemas UNIX. El protocolo RADIUS está bien definido y probado. Podemos recomendar todos los productos enumerados anteriormente, especialmente la implementación FreeRADIUS.

Nota: Por el momento, no se admite la opción “challenge/response”. Una respuesta de “Access Challenge” (reto de acceso) es considerada y evaluada como un “Access Reject” (rechazo de acceso).

Para llegar hasta un dispositivo remoto utilizando el protocolo RADIUS, debe acceder especificando su nombre de usuario y contraseña, que se le solicitará. El servidor RADIUS leerá los datos que ha introducido (autenticación) y el RIPM buscará su perfil (autorización). El perfil define (o limita) sus acciones y puede variar dependiendo de su situación específica. Si no existe tal perfil, se le negará el acceso mediante RADIUS. En términos del mecanismo de actividad a distancia, el acceso mediante RADIUS funciona como la Consola remota. Si no hay actividad durante media hora, su conexión al RIPM se interrumpirá y cerrará.

2a. Server - Servidor
Introduzca la dirección IP o el nombre de equipo del servidor RADIUS que se quiere conectar. Si va a utilizar el nombre de equipo, el DNS debe estar configurado y activado.

2b. Shared Secret - Secreto compartido
Un secreto compartido es una secuencia de texto que sirve de contraseña entre el cliente RADIUS y el servidor RADIUS. El RIPM sirve de cliente RADIUS. Se utiliza un secreto compartido para verificar que los mensajes RADIUS se envían mediante un dispositivo compatible con RADIUS que está configurado con el mismo secreto compartido y para verificar que el mensaje RADIUS no ha sufrido modificaciones durante el tránsito (para verifica la integridad del mensaje). Para el secreto compartido puede utilizar caracteres especiales y caracteres alfanuméricos estándares. Un secreto compartido puede consistir de hasta 128 caracteres y puede contener letras letras mayúsculas y minúsculas (A–Z, a–z), numerales (0–9), y otros símbolos (caracteres que no se definen como letras o números), como signos de exclamación o (“ ! ”) o asteriscos (“ * ”).

2c. Authentication Port - Puerto de autenticación
El puerto que utiliza el servidor RADIUS para las solicitudes de autenticación. El valor predeterminado es #1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:36:20 AM

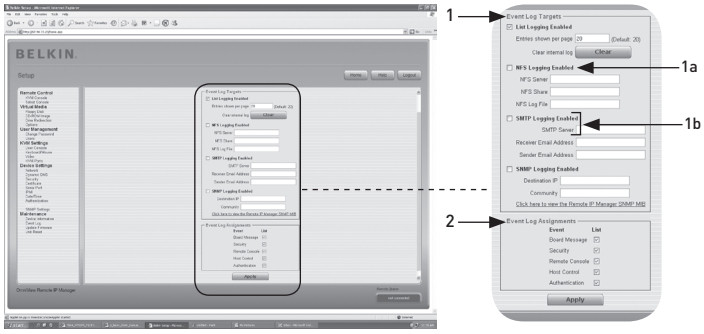
2d. Accounting Port - Puerto de administración
El puerto que utiliza el servidor RADIUS para las solicitudes de administración. El valor predeterminado es #1813.

2e. Timeout - Tiempo límite de inactividad
Fija el tiempo de vida de una solicitud en segundos. El tiempo de vida es el tiempo se espera para que se complete la solicitud. Si la tarea que se solicita no se ha completado en este intervalo de tiempo, se cancela. El valor predeterminado es un segundo.

2f Retries - Intentos
Fija el número de intentos que se realizan si una solicitud no ha podido completarse. El valor predeterminado es tres veces.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:36:20 AM

Registro de sucesos



Los sucesos importantes como un fallo de acceso o una actualización del firmware se registran en una selección de destinos de registro (vea la ilustración 6-33) Cada suceso pertenece a un grupo de suceso, que se puede activar por separado. La forma habitual de registrar sucesos es utilizar la lista de registro interna del RIPM. Para mostrar la lista de sucesos, haga clic en “Event Log” (Registro de sucesos) en la página de Mantenimiento. En los ajustes de registro de sucesos, puede elegir cuántas entradas del registro se muestran en cada página. También puede borrar el archivo de registro.

1. **Event Log Targets - Objetivos del registro de sucesos**
   Para registrar sucesos, puede utilizar la lista de registro interna del RIPM. Para mostrar la lista de sucesos, haga clic en “Event Log” (Registro de sucesos) en la página de Mantenimiento. Como la memoria del sistema del RIPM se utiliza para guardar toda la información, el número máximo de entradas de la lista de registro se ha limitado a 1.000 sucesos. Cada entrada que supere este límite hace que se borre la entrada más antigua.

   Advertencia: Si se utiliza el botón de reinicio de la portada HTML para reiniciar el RIPM, toda la información de registros se guardará de forma permanente y estará disponible después de que el RIPM se haya iniciado. Si el RIPM no recibe corriente o ha forzado un reinicio, todos los datos de registro se perderán. Para impedir que esto ocurra, utilice uno de los métodos de registro que se describen a continuación.

   1a. NFS Logging Enabled - Registro NFS (Sistema de archivos de red) activado
   Defina un servidor NFS al que se deben exportar los directorios y los enlaces estáticos, todos los datos de registro se escribirán en un archivo de esta ubicación. Para escribir los datos de registro de varios dispositivos de RIPM en un sola porción del NFS, debe definir un nombre de archivo exclusivo para cada dispositivo. Cuando cambie los ajustes NFS y pulse el botón “Apply” (Aplicar), la porción del NFS se actualizará inmediatamente. Esto significa que la porción del NFS y el servidor NFS deben completarse con las fuentes correctas, o de lo contrario aparecerá un mensaje de error.

   Nota: Al contrario que el archivo de registro interno del RIPM, el tamaño del archivo de registro del NFS es ilimitado. Cada suceso del registro se añadirá al final del archivo, de modo que este crece continuamente. De vez en cuando puede necesitar borrarlo o cambiar de sitio los sucesos registrados en el archivo.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:36:21 AM

1b. Ajustes SNMP

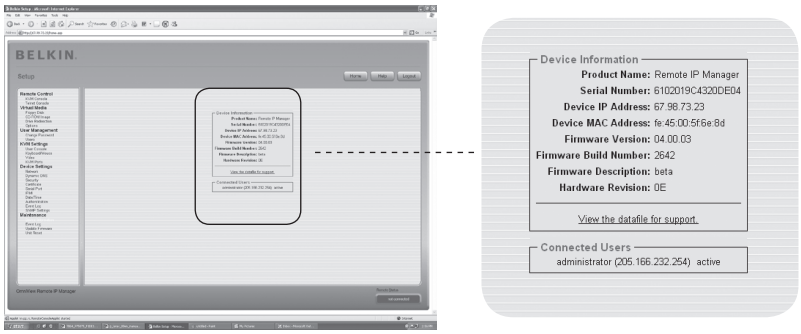
SMTP Logging Enabled - Registro de SMTP (protocolo simple de transferencia de correo electrónico) activado
Con esta opción, el RIPM es capaz de enviar correo electrónico a una dirección introducida en el espacio de texto para la dirección de correo electrónico de los ajustes de registro de sucesos. Estos mensajes contienen las mismas secuencias descriptivas que el archivo de registro interno, y el asunto del mensaje se rellena con el grupo de sucesos del suceso registrado que se ha producido. Para utilizar este destino de registro, debe especificar un servidor SMTP que sea accesible desde el RIPM y que no necesite autenticación (<serverip>:<port>).

SNMP Logging Enabled - Registro SNMP (protocolo simple de administración de redes) activado
Si se encuentra activado, el RIPM envía un*trap* (tipo de notificación) SNMP a la dirección IP cada vez que se produce un suceso de registro. Si el receptor requiere una secuencia de comunidad, puede fijarla en el campo correspondiente. La mayoría de los *traps* de suceso solo contienen una secuencia descriptiva que incluye toda la información sobre el suceso registrado. La autenticación y el suministro del equipo tienen sus propios traps estándares, que se crean automáticamente y que consisten en varios campos de información detallada sobre el suceso. Para recibir este trap SNMP, utilice cualquier receptor de traps de SNMP.

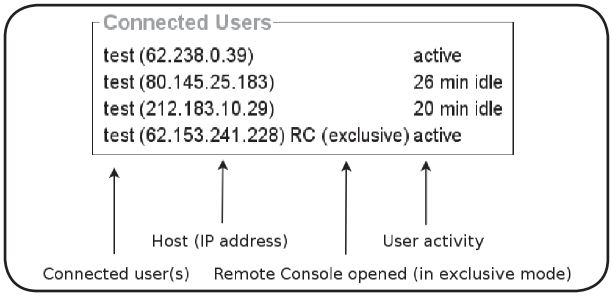
2. Event Log Assignments - Asignar registro de sucesos
Puede elegir qué acciones del RIPM se guardarán en el archivo de registro. Seleccione el cuadro o cuadros que desee y haga clic en “Apply” para confirmar su selección.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:36:21 AM

Información del dispositivo



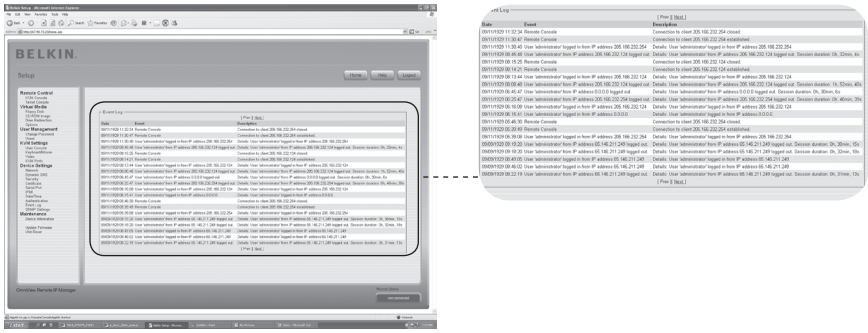
Esta sección contiene un resumen de información acerca de este RIPM y su firmware actual, y le permite reiniciar el RIPM. El archivo de datos para asistencia le permite descargar el archivo de datos del RIPM con la información de asistencia específica. Se trata de un archivo XML (eXtensible Markup Language) con información de asistencia personalizada, p. ej. el número de serie.



La ilustración anterior muestra la actividad del RIPM. De izquierda a derecha, la pantalla indica el usuario o usuarios conectados, la dirección IP del usuario del equipo, y el estado de actividad del RIPM. “RC” significa que la Consola remota está abierta. Si la Consola remota se abre en “modo exclusivo” se añade el término “(exclusive)”. Para más información sobre esta opción, consulte la sección “Barra de control de consola remota” en la sección 23 de este Manual del usuario. Para mostrar la actividad del usuario, la última columna contiene el término “active” para indicar que existe un usuario activo, o “20 min idle” para indicar que un usuario ha estado inactivo durante cierto tiempo, el número corresponde a los minutos.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:36:22 AM

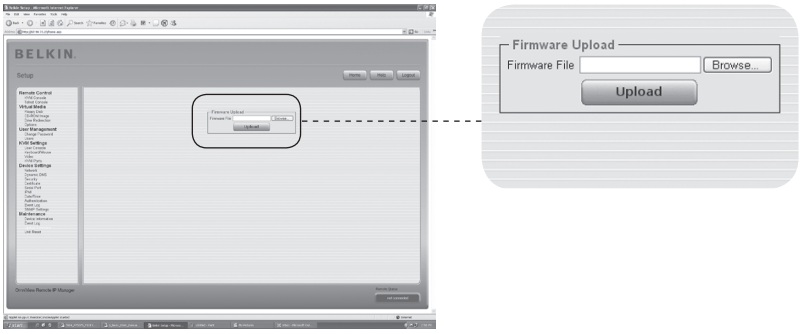
Registro de sucesos



La lista de registro de sucesos “Event Log” incluye los sucesos guardados por el RIPM, ampliados con la fecha del suceso, una breve descripción del suceso, y una dirección IP que indica el origen del suceso. Puede utilizar los botones “Prev” (Anterior) y “Next” (Siguiente) para buscar los datos.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:36:22 AM

Actualización del firmware



El RIPM es un ordenador completamente independiente, funciona con el software denominado firmware, que está escrito en su memoria de solo lectura (ROM). El firmware del RIPM se puede actualizar de manera remota para instalar funciones nuevas o mejoradas o características especiales. Una actualización de firmware nuevo es un archivo binario que se debe descargar de la página web de Belkin. Si el archivo de firmware está comprimido (p. ej. si la extensión es .zip) deberá descomprimirlo antes de proceder. En el sistema operativo Windows, puede utilizar WinZip (su dirección en Internet es http://www.winzip.com/) para descomprimir sus actualizaciones de firmware. **Nota:** Para actualizar el firmware del RIPM, debe guardar el archivo descomprimido de firmware nuevo en el sistema que haya conectado al RIPM.

La actualización del firmware es un proceso en tres etapas:

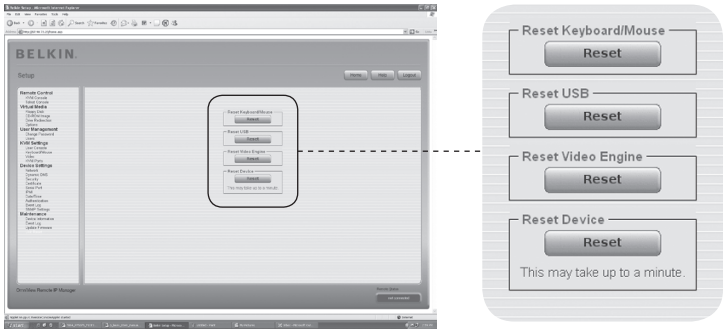
1. Cargue el archivo de firmware nuevo en el RIPM. Para hacer esto, seleccione el archivo en su sistema local utilizando el botón “Browse” (Examinar) del panel “Upload Firmware” (Cargar Firmware). A continuación, haga clic en “Upload” (Cargar) para transferir al RIPM el archivo previamente seleccionado en su sistema local. Cuando el archivo de firmware se ha cargado, el RIPM verificará automáticamente su validez y confirmará que no se han producido errores de transmisión. Si se produce un error, la función “Upload Firmware” (Cargar Firmware) se interrumpirá y el firmware actual quedará intacto.
2. Si la carga se realiza con éxito (lo que es muy probable que ocurra), aparecerá el panel “Update Firmware” (Actualizar Firmware). El panel mostrará el número de versión del firmware que se está utilizando actualmente y el número de versión del firmware que se ha cargado. Haga clic en “Update” (Actualizar) para sustituir la antigua versión por la nueva.

   Advertencia: Este proceso es irreversible y normalmente dura varios minutos. Asegúrese de que el suministro de corriente al RIPM no se interrumpe durante el proceso de actualización, una interrupción de corriente podría provocar que el RIPM diese problemas.
3. Después de que el firmware se haya actualizado, el RIPM se reiniciará automáticamente. Después de aproximadamente un minuto, se le redirigirá a la página de acceso para que acceda de nuevo.

   Advertencia: El proceso de actualización del firmware en 3 etapas y la completa comprobación de consistencia hacen que la actualización del firmware transcurra prácticamente sin errores. Sin embargo, sólo deben realizar una actualización del firmware los administradores o miembros del personal que tengan experiencia. Es esencial que el suministro de corriente al RIPM NO se interrumpa durante el proceso de actualización.

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:36:23 AM

Reinicio de la unidad



Esta sección describe los métodos que se utilizan para reiniciar determinadas partes del dispositivo. Esto concierne al teclado y el ratón, la pantalla de vídeo del ordenador conectado al RIPM, y el propio RIPM. Para activar un nuevo firmware actualizado, debe reiniciar el RIPM. Este proceso cierra automáticamente todas las conexiones actuales a la consola de administración y al RIPM, y sólo dura 30 segundos aproximadamente. El reinicio de dispositivos secundarios (p. ej. el motor de vídeo) requiere únicamente pocos segundos y no se cierran las conexiones. Para reiniciar un RIPM determinado, haga clic en el botón “Reset” como se muestra en la imagen anterior.

Nota: Solamente el administrador está autorizado a reiniciar el RIPM.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:36:23 AM

El ratón remoto no funciona o no está sincronizado.

En primer lugar, compruebe la conexión VGA. El RIPM y el monitor local deben ofrecer la misma resolución de vídeo. Asegúrese de que los ajustes de su ratón corresponden con su modelo de ratón, p. ej. PS/2 o USB. Asimismo, el modelo de ratón debe haberse establecido en el RIPM y en el sistema operativo del equipo (el ordenador conectado al RIPM). En algunas circunstancias, el proceso de sincronización del ratón puede producir errores. Consulte la sección "Configuración de vídeo, teclado y ratón" del capítulo 3 para más información.

La calidad de la imagen es mala o con poco detalle.

Utilice el menú "Reset" (Reinicio) para reiniciar el RIPM con sus valores predeterminados. A continuación, haga clic en el botón de ajuste automático "Auto-Adjust" para seleccionar una salida de vídeo apropiada. Compruebe que los cables de vídeo están conectados correctamente.

El acceso al RIPM falla.

Verifique su nombre de usuario y contraseña. El nombre de usuario predeterminado es "administrator", y la contraseña predeterminada es "belkin". Asegúrese de que su buscador de Internet está configurado para aceptar cookies.

La ventana de la Consola remota del RIPM no se abre.

Verifique que se ha cargado Java. La existencia de un firewall puede impedir el acceso a la Consola remota. Los puertos #80 TCP (para HTTP) y #443 (tanto para HTTPS como para RFB) deben estar abiertos (el servidor que tiene el firewall debe aceptar conexiones TCP de entrada en estos puertos).

La Consola remota no puede conectarse y muestra un error de tiempo límite de inactividad.

Verifique la configuración de red y su hardware. Si existe un servidor proxy entre el RIPM y su equipo, puede que no sea posible transferir los datos de vídeo utilizando RFB. Establezca una conexión directa entre el RIPM y el cliente. Además, compruebe los ajustes del RIPM y elija un puerto de servidor distinto para la transferencia RFB. Si utiliza un firewall, compruebe el puerto adecuado para aceptar conexiones. Puede limitar estas conexiones a las direcciones IP utilizadas por el RIPM y su cliente.

No se puede establecer conexión con el RIPM.

Examine su hardware. ¿Está conectado el RIPM a una fuente de alimentación? Verifique su configuración de red (dirección IP, router). Envíe un comando "ping" al RIPM para averiguar si el RIPM es accesible a través de la red.

Las combinaciones de teclas especiales (p. ej. ALT+F2, ALT+F3) son interceptadas por el sistema de la consola y no se transmiten al equipo.

Defina una "tecla de botón". Esto puede realizarse en los ajustes de la Consola remota (consulte la sección "Barra de control de Consola remota" en la página 23).

Las páginas web del RIPM no se muestran correctamente.

Compruebe los ajustes de caché de su buscador. Asegúrese de que en los

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:36:23 AM

ajustes de caché NO se ha seleccionado “never check for newer pages” (nunca buscar páginas más nuevas). Con ese ajuste, las páginas RIPM podrían descargarse del caché de su buscador y no del RIPM, lo que podría estar causando el problema.

Windows XP no vuelve a activarse cuando entra en el modo suspendido.

Posiblemente este es un problema de Windows XP. Intente no mover el puntero del ratón cuando XP cambia al modo suspendido. Consulte el manual de su sistema operativo para más información.

Cada vez que vuelvo a abrir el cuadro de diálogo de Consola remota, los punteros de ratón dejan de estar sincronizados.

Desactive la opción “Mover automáticamente el puntero al botón predeterminado en un cuadro de diálogo” en la configuración del ratón de su sistema operativo.

La Consola remota permanece en negro.

Compruebe si el RIPM solamente recibe alimentación mediante el puerto USB. Si no se recibe suministro suficiente a través del puerto USB, la Consola remota se abre pero se queda en negro. Verifique los ajustes del RIPM en la página 26 de este Manual del usuario. Compruebe que los cables de vídeo están conectados correctamente.

Los datos de vídeo en el monitor local aparecen rodeados por un borde negro.

Esto no es un fallo. El monitor local está programado en una modalidad de vídeo fija que se puede seleccionar en los ajustes del RIPM. Consulte la sección “Barra de control de Consola remota” en la página 23 de este Manual del usuario.

He olvidado mi contraseña. ¿Cómo puedo reiniciar el RIPM para restablecer los ajustes de fábrica?

Puede utilizar la interfaz Serie. Para una descripción detallada, consulte la sección “Reajuste del Remote IP Manager a los ajustes de fábrica” en la página 31 de este Manual del usuario.

Consulte www.belkin.com para más información sobre resolución de problemas y una lista del hardware que es compatible con el RIPM.

Nota: Si estas soluciones no resuelven la situación, llame al servicio de asistencia técnica 1-800-2BELKIN.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:36:23 AM

Declaración de la FCC

Declaración de conformidad con las normativas de la FCC sobre compatibilidad electromagnética

Nosotros, Belkin Corporation, con sede en 501 West Walnut Street, Compton, CA 90220 (EE. UU.), declaramos bajo nuestra sola responsabilidad que el producto:
F1DE101H

Declaración de conformidad CE
Nosotros, Belkin Corporation, declaramos bajo nuestra sola responsabilidad que el producto F1DE101H, al que hace referencia la presente declaración, está en conformidad con el Estándar de Emisiones EN55022, el Estándar de Inmunidad EN55024, y LVD EN61000-3-2 y EN61000-3-3.

ICES
Este aparato digital de la clase B cumple con la norma canadiense ICES-003. This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme á la norme NMB-003 du Canada.

Garantía del producto de 2 años de Belkin Corporation Limited

La cobertura de la presente garantía.
Belkin Corporation otorga una garantía al comprador original según la cual el producto no tendrá defectos en cuanto a diseño, montaje, materiales o mano de obra.

Cuál es el período de cobertura.
Belkin Corporation garantiza el producto Belkin durante dos años.

¿Qué haremos para resolver los problemas?
Garantía del producto.
Belkin reparará o sustituirá, según decida, cualquier producto defectuoso sin ningún tipo de cargo (excepto los gastos de envío del producto).

¿Qué no está cubierto por esta garantía?
Todas las garantías mencionadas anteriormente resultarán nulas y sin valor alguno si el producto Belkin no se le proporciona a Belkin Corporation para su inspección bajo requerimiento de Belkin con cargo al comprador únicamente, o si Belkin Corporation determina que el producto Belkin se ha instalado de un modo inadecuado, alterado de algún modo o forzado. La garantía del producto de Belkin no lo protege de los desastres naturales (que no sean relámpagos) tales como inundaciones, terremotos, guerras, vandalismo, robo, desgaste natural debido al uso normal, desgaste, agotamiento, obsolescencia, mal uso, daños a causa de alteraciones la alimentación (p. ej.. apagones, bajadas de tensión), modificación o alteración no autorizadas de programas o sistemas.

Cómo acceder a nuestros servicios.
Para obtener asistencia sobre algún producto de Belkin, debe seguir los siguientes pasos:

1. Póngase en contacto con Belkin Corporation en 501 W. Walnut St., Compton CA 90220, a la atención de: Servicio de atención al cliente, o llame al (800)-223-5546, en un plazo de 15 días desde el momento de la incidencia. Tenga preparada la siguiente información:
   a. El número de artículo del producto Belkin.
   b. El lugar de compra del producto.
   c. Cuándo compró el producto.
   d. Copia de la factura original.
2. El servicio de atención al cliente de Belkin le informará sobre cómo enviar la factura y el producto Belkin y sobre cómo proceder con su reclamación.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:36:24 AM

Belkin Corporation se reserva el derecho de revisar el producto Belkin dañado. Todos los costes de envío del producto Belkin a Belkin Corporation para su inspección correrán a cargo del comprador exclusivamente. Si Belkin determina, según su propio criterio, que resulta poco práctico el envío de los equipos dañados a Belkin Corporation, Belkin podrá designar, según su propio criterio, una empresa de reparación de equipos para que inspeccione y estime el coste de la reparación de dichos equipos. El coste, si existe, del envío de los equipos hacia y desde dicha empresa de reparaciones, y de la estimación correspondiente, correrá exclusivamente a cargo del comprador. Los equipos dañados deberán permanecer disponibles para su inspección hasta que haya finalizado la reclamación. Siempre que se solucionen las reclamaciones por negociación, Belkin Corporation se reserva el derecho a que esta garantía sea subrogada por cualquier póliza de seguros existente de la que disponga el comprador.

Relación de la garantía con la legislación estatal.
ESTA GARANTÍA CONTIENE LA GARANTÍA EXCLUSIVA DE BELKIN CORPORATION, NO EXISTE NINGÚN OTRO TIPO DE GARANTÍAS, EXPRESAS O, EXCEPTO LAS REQUERIDAS POR LA LEY, IMPLÍCITAS, INCLUIDAS LA CONDICIÓN O GARANTÍA IMPLÍCITA DE CALIDAD, COMERCIABILIDAD E IDONEIDAD PARA UN FIN PARTICULAR, Y TALES GARANTÍAS IMPLÍCITAS, SI EXISTIESEN, ESTÁN LIMITADAS EN DURACIÓN AL TÉRMINO DE LA PRESENTE GARANTÍA.

Algunas jurisdicciones no permiten la limitación de la duración de las garantías implícitas, por lo que cabe la posibilidad de que las anteriores limitaciones no le afecten.

EN NINGÚN CASO BELKIN CORPORATION SERÁ RESPONSABLE DE LOS DAÑOS IMPREVISTOS, ESPECIALES, DIRECTOS, INDIRECTOS, CONSECUENTES O MÚLTIPLES, INCLUYENDO, AUNQUE NO EXCLUSIVAMENTE, LA PÉRDIDA DE NEGOCIO O BENEFICIOS QUE PUEDA SURGIR DE LA VENTA O EL EMPLEO DE CUALQUIER PRODUCTO BELKIN, INCLUSO SI SE HA INFORMADO A BELKIN DE LA POSIBILIDAD DE DICHOS DAÑOS.

Esta garantía le proporciona derechos legales específicos y usted puede beneficiarse asimismo de otros derechos que pueden variar entre las distintas jurisdicciones. Algunas jurisdicciones no permiten la exclusión o limitación de los daños fortuitos, consecuentes, o de otro tipo, por lo que puede que las limitaciones mencionadas anteriormente no le afecten.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:36:24 AM

BELKIN®

OmniView® Remote IP Manager

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Ángeles, CA 90220, EE.UU.
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Reino Unido
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Países Bajos
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Iberia
Avda. Cerro del Águila 3
28700 San Sebastián de los Reyes
España
+34 9 16 25 80 00
+34 902 02 00 34 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, Francia
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH
Hanebergstrasse 2
80637 Múnich, Alemania
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

© 2006 Belkin Corporation. Todos los derechos reservados. Todos los nombres comerciales son marcas registradas de los respectivos fabricantes enumerados. Mac OS y Macintosh son marcas registradas de Apple Computer, Inc., registrado en EE.UU. y otros países.

P75075ea

BELKIN®

OmniView® Remote IP Manager

Controllo

Per controllare il computer o lo switch KVM tramite un browser web, da qualsiasi parte

EN
FR
DE
NL
ES
IT

Manuale d'uso

F1DE101Hea

Indice

Indice

1-1 Introduzione e contenuto della confezione | Descrizione generale

Grazie per aver acquistato questo Remote IP Manager, unità di gestione remota via IP della serie OmniView di Belkin, a cui ci si riferirà con l'acronimo RIPM (Remote IP Manager). Progettato per offrire alle imprese un modo semplice per aggiungere la tecnologia KVM-over-IP alle configurazioni di server e KVM, il RIPM rappresenta la soluzione più efficiente per ridurre l'inattività dei server e i costi del servizio. Ora gli amministratori di rete possono controllare i server 24 ore su 24 grazie all'accesso remoto da qualsiasi luogo.

Il RIPM si integra facilmente in un impianto di rete locale LAN di piccole o grandi dimensioni. Leggere attentamente questo manuale d'uso per installare e utilizzare nel modo corretto il RIPM, e per risolvere eventuali anomalie. Noi teniamo a cuore la vostra azienda e siamo certi che
anche voi scoprirete perché oltre 1 milione di prodotti OmniView Belkin sono già utilizzati in tutto il mondo.


OmniView Remote IP Manager


Kit di cavi PS/2


Cavo VGA


Cavo Null DB9


Cavo mini-USB


Un alimentatore di corrente 5V CC, 2A


Staffa per montaggio su rack con rispettive viti


Cd-rom con il software di installazione


Manuale d'uso


Guida di installazione rapida

Cartolina di registrazione

P75075ea_F1DE101Hea_man.indb 1 8/16/2006 11:36:27 AM

- **Accesso remoto**
  L'unità RIPM offre l'accesso remoto alla configurazione KVM e a tutti i server collegati. È anche in grado di offrire accesso remoto a un singolo computer o server.

- **Utenti digitali**
  L'unità RIPM consente a un utente digitale di avere accesso agli switch KVM e ai server. Consente inoltre ad altri 25 utenti di visualizzare simultaneamente i video digitali per una risoluzione collettiva delle anomalie.

- **Basato su browser web**
  L'interfaccia dell'unità RIPM è basata sul browser web. È quindi accessibile da ogni computer a condizione che sia connesso a una rete locale LAN, WAN o a una comune connessione TCP/IP. L'installazione non rischiede alcun software aggiuntivo.

- **Interfaccia utente di facile approccio**
  L'interfaccia utente di facile approccio consente di impostare e cambiare facilmente le funzioni dell'unità RIPM attraverso il browser web, senza dover installare un altro software sul computer.

- **Accesso al livello BIOS**
  L'unità RIPM consente di accedere al sistema BIOS dei server in modo da apportare delle modifiche e riavviare i calcolatori.

- **Supporto per dispositivi seriali**
  L'unità RIPM fornisce supporto per un dispositivo seriale, come un'unità di distribuzione energetica, in modo da poter effettuare reboot hardware dei server a distanza.

- **Protezione avanzata**
  L'unità RIPM offre un sistema di protezione basato su crittografia SSL a 256 bit e una password multiutente per impedire gli accessi non autorizzati ai server.

- **Supporto virtuale***
  I supporti virtuali consentono di trasferire immagini e file tra computer locali e remoti, di caricare un software a distanza, di aggiornare le applicazioni e il sistema operativo, e di effettuare test di verifca da un CD.

*Disponibile solo su computer con Windows®.

P75075ea_F1DE101Hea_man.indb 2 8/16/2006 11:36:28 AM

- **Gestione degli account**
  L'unità RIPM consente all'amministratore di creare degli account per molteplici utenti e di controllare l'accesso ai server.

- **Registro eventi**
  Il registro eventi memorizza e archivia tutte le attività degli utenti sull'unità RIPM.

- **Notifica via e-mail**
  L'unità RIPM consente all'amministratore di monitorare l'attività dell'utente di inviare via e-mail delle notifiche di login, di login non valido e di logout.

- **Supporto multipiattaforma**
  L'unità RIPM funziona con server e switch KVM con interfaccia PS/2 o USB.

- **Risoluzione video**
  Con una larghezza di banda di 117 MHz, questa unità è in grado di supportare risoluzioni video per un massimo di 1600x1200 a 75 Hz.

- **Possibilità di montaggio su rack 0U**
  L'unità RIPM è sufficientemente compatta per essere collocata sulla scrivania o montata sul restro di un armadio per server per un'installazione di tipo 0U.

- **Aggiornamenti del firmware**
  Gli aggiornamenti rapidi consentono all'utente di disporre sempre dei più recenti aggiornamenti per l'unità. Questi aggiornamenti del software garantiscono che l'unità sia compatibile con gli ultimi dispositivi e operativa per tutto il ciclo di vita. Andate su www.belkin.com per l'assistenza e le informazioni sugli aggiornamenti.

P75075ea_F1DE101Hea_man.indb 3 8/16/2006 11:36:28 AM

Requisiti dell'hardware

- Remote IP Manager della serie OmniView (incluso)
- Kit di Cavi PS/2 (incluso)
- Cavo VGA (incluso)
- Cavo mini USB (incluso)
- Alimentatore di corrente 5V CC, 2A (incluso)
- Tastiera, monitor e mouse
- Connessione alla rete utilizzando la porta 10/100Base-T Ethernet (RJ45)
- Cavo Cat5
- Staffe di montaggio su rack con rispettive viti (comprese per eventuale installazione su rack)

P75075ea_F1DE101Hea_man.indb 4 8/16/2006 11:36:28 AM

Windows 2000, 2003, XP; Red Hat® Linux® 7.x e successive;
UNIX®; Mac OS® X v10.0 e successive (con switch KVM);
Sun™ Solaris™ 8.x e successive (con adattatore Sun — Belkin, cod. prod. F1DE083)

Browser supportati

- Microsoft® Internet Explorer 6.0 e successive
- Netscape® Navigator® 7.0

P75075ea_F1DE101Hea_man.indb 5 8/16/2006 11:36:28 AM

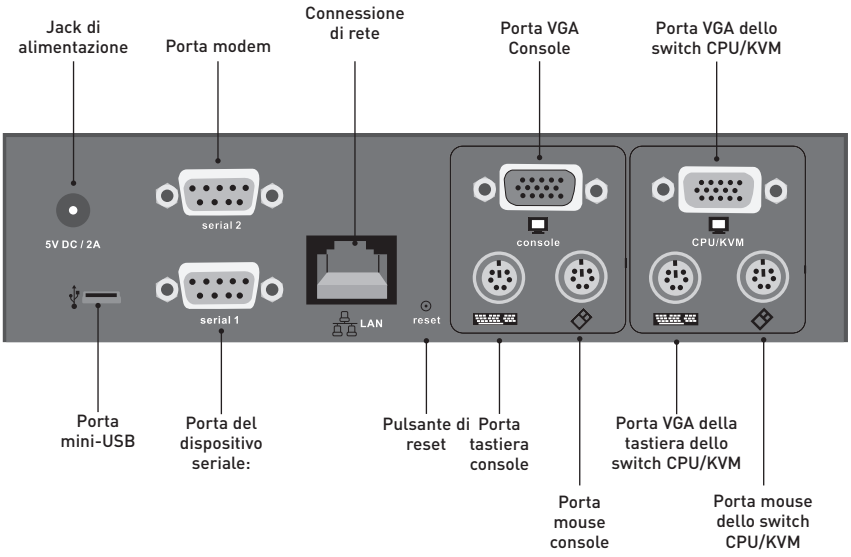
Codice prodotto:	F1DE101H
Alimentazione:	5V CC, 2A
Nº di server supportati:	1 locale, 1 digitale (1 utente simultaneo)
Emulazione tastiera:	PS/2 e USB
Emulazione mouse:	PS/2 e USB
Monitor supportati:	CRT e LCD (con supporto VGA)
Risoluzione supportata:	fino a 1600x1200 a 75Hz
Larghezza di banda remota massima:	5MB
Ingresso tastiera:	miniDIN6 (PS/2)
Ingresso mouse:	miniDIN6 (PS/2)
Porta monitor:	HDDB15 femmina (VGA)
Porta USB della CPU:	Mini USB
Connessione di rete:	RJ45
Modalità di crittografia:	a 256 bit SSL, a 128 bit, AES, DES, 3DES
Supporto per autenticazione:	LDAP (via client LDAP locale), RADIUS, AD
Protocollo supportato:	SNMP v1, IPv4
Porta del dispositivo seriale:	DB9
Indicatori LED:	2
Rivestimento:	in metallo
Dimensioni:	171 (Larg) x 44 (Alt) x 114 (Lung) mm
Peso:	0,75 kg
Temperatura di funzionamento:	da 0° a 48,89° C
Temperatura di immagazzinamento:	da -20° C a 60° C
Umidità:	da 5% a 80%
Garanzia:	2 anni

Nota bene: le specifiche sono soggette a variazioni senza obbligo di preavviso.

P75075ea_F1DE101Hea_man.indb 6 8/16/2006 11:36:28 AM

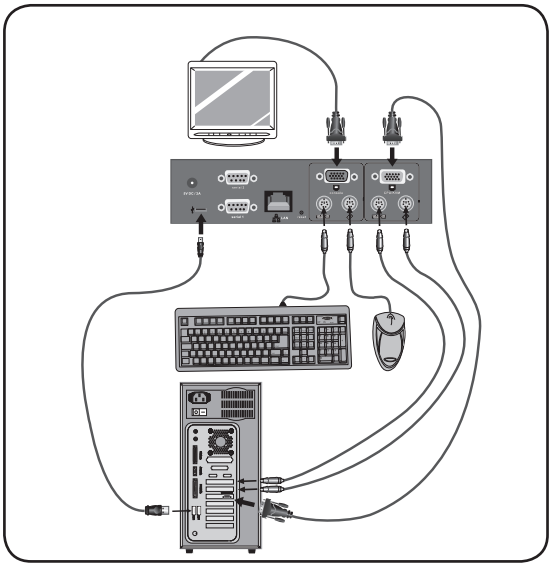
Fronte dell'unità

Retro dell'unità

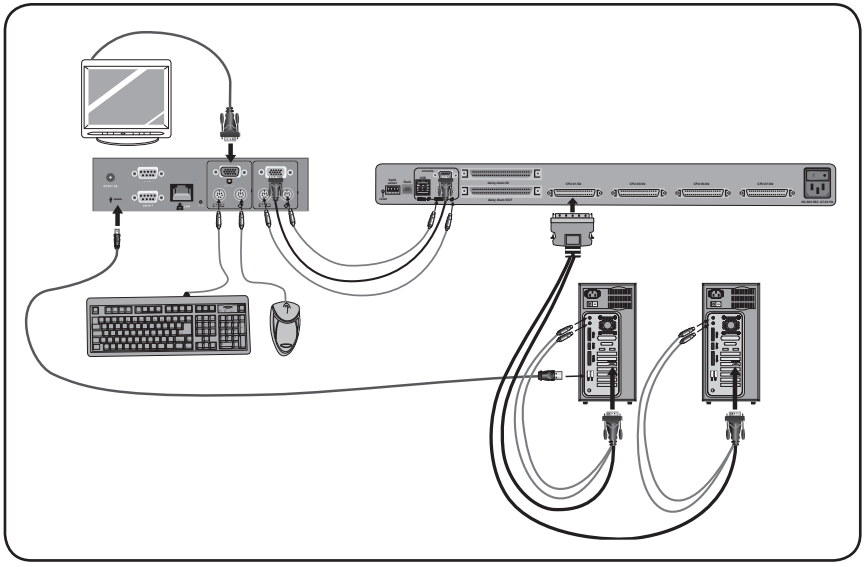


P75075ea_F1DE101Hea_man.indb 7 8/16/2006 11:36:29 AM

Configurazione tipica con un computer



Configurazione tipica con uno switch KVM



P75075ea_F1DE101Hea_man.indb 8 8/16/2006 11:36:33 AM

Fase 1 | Installazione dell'unità in un armadio per server:

L'unità viene fornita con alcune staffe regolabili ideali per il montaggio su rack da 19 pollici.

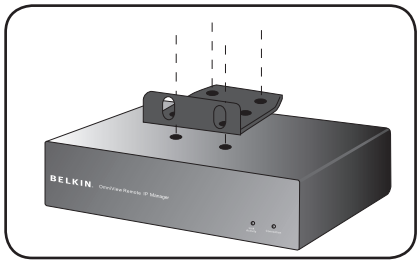


Fig. 1

1.1 Applicare la staffa sul lato superiore o inferiore dell'unità utilizzando le viti in dotazione.

1.2 Montare l'unità RIPM sul rack. Vedi **Fig. 1.**

Nota bene: Le viti di montaggio per il rack non sono incluse. Utilizzare le viti specificate dal produttore del rack.

Prima di tentare di collegare qualsiasi periferica all'unità RIPM o ai computer, accertarsi che tutti le apparecchiature e le periferiche siano spente. Belkin Corporation declina qualsiasi responsabilità per eventuali danni causati da un mancato adempimento a queste indicazioni.

Fase 2 | Collegamento della console all'unità RIPM

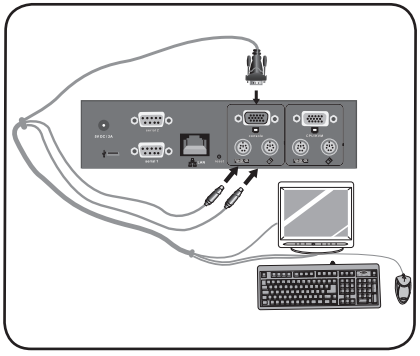


Fig. 2

2.1 Collegare la tastiera e il mouse alle porte per la tastiera e il mouse presenti sull'unità.

2.2 Collegare il monitor alla porta VGA della "Console" sull'unità.
Vedi **Fig. 2.**

P75075ea_F1DE101Hea_man.indb 9 8/16/2006 11:36:37 AM

Fase 3 Opzione 1: Collegamento dell'unità a uno switch KVM (Sistema host)

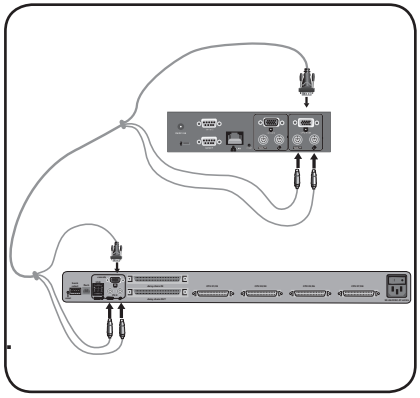


Fig. 3

3.1 Spegnere lo switch KVM.

3.2 Utilizzando il kit di cavi PS/2 e VGA incluso, collegare un'estremità del cavo alle porte per mouse, tastiera e monitor "CPU/switch KVM" sull'unità RIPM. Vedi **Fig. 3.**

3.3 Collegare l'altra estremità alle porte per mouse, tastiera e monitor sullo switch KVM.

Fase 3 Opzione 2: Collegamento dell'unità a computer (Sistema host)

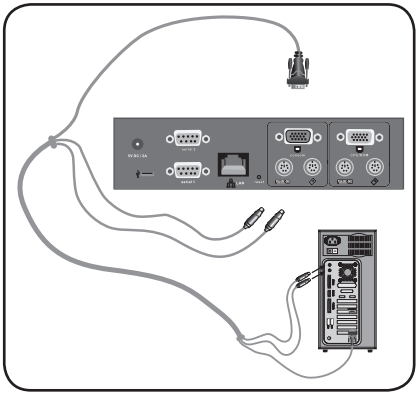


Fig. 4

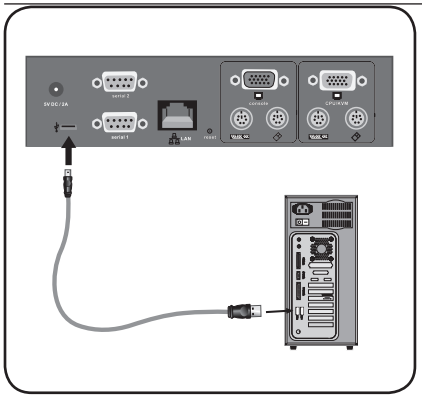
3.1 Spegnere il computer.

3.2 Utilizzando il kit di cavi PS/2 e VGA incluso, collegare un'estremità del cavo alle porte per mouse, tastiera e monitor "CPU/switch KVM" sull'unità RIPM. Vedi **Fig. 4.**

3.3 Collegare l'altra estremità alle porte per mouse, tastiera e monitor sul computer.

P75075ea_F1DE101Hea_man.indb 10 8/16/2006 11:36:39 AM

Fase 4 Collegamento del cavo mini USB per la funzione di supporto virtuale



4.1 Spegnere il computer.

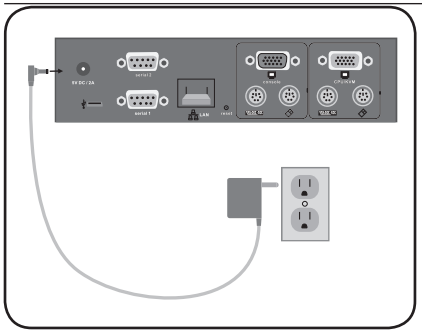
4.2 Utilizzando il cavo mini USB incluso, collegare un'estremità del cavo alla porta mini-USB dell'unità e l'altra estremità a una porta USB del computer. Vedi **Fig. 5.**

Fig. 5

Nota bene: È possibile collegare all'unità RIPM ogni tipo di computer con sistema operativo Windows per utilizzare la funzione di supporto virtuale; non occorre che il computer sia il sistema host.

Nota bene: Se il computer NON ha Windows, non occorre eseguire l'installazione sopra descritta.

Fase 5 Accensione dell'unità RIPM



5.1 Collegare l'alimentatore a una presa di alimentazione disponibile.

5.2 Inserire lo spinotto cilindrico nella presa dell'unità RIPM. Vedi **Fig. 6.**

5.3 Accendere lo switch KVM o il computer.

Fig 6

P75075ea_F1DE101Hea_man.indb 11 8/16/2006 11:36:41 AM

Esistono due modi per installare e configurare l'unità RIPM. È possibile usare il software d'installazione su CD incluso nella confezione o collegare un cavo di interfaccia seriale all'unità RIPM e servirsi del software del terminale (ad es., HyperTerminal®).

Nota bene: Belkin consiglia di utilizzare il software d'installazione incluso.

P75075ea_F1DE101Hea_man.indb 12 8/16/2006 11:36:42 AM

Software d'installazione

Il software contenuto nel software consente di configurare l'unità RIPM con la rete in modo da potervi accedere a distanza.

1. Collegare l'unità al computer attraverso la rete locale. Avviare il software d'installazione su CD-ROM dal computer a cui è stata installata l'unità RIPM.
2. Seguire l'installazione guidata per configurare l'unità. Occorre disporre di un indirizzo IP, una maschera di sottorete e le informazioni di accesso che sarano assegnati all'unità. Queste informazioni vengono fornite dall'amministratore di rete. Una volta completata la configurazione, il sistema visualizzerà un messaggio di conferma. Ora è l'unità RIPM è configurata e pronta per l'uso.
3. Questo CD-ROM contiene anche il software necessario per trasferire file tra computer locali e remoti. Per maggiori informazioni, leggere la sezione "Supporto virtuale" di questo manuale d'uso.

P75075ea_F1DE101Hea_man.indb 13 8/16/2006 11:36:42 AM

Per configurare l'unità RIPM tramite l'interfaccia seriale, è necessario disporre del cavo null modem incluso. Collegare il cavo null modem alla porta "Serial 01" dell'unità e alla porta seriale del computer. L'interfaccia seriale deve essere regolata secondo i parametri come descritto qui sotto:

Parametro	**Valore**
Bit/secondo	115200
Bit di dati	8
Parità	no
Bit di arresto	1
Controllo di flusso	nessuno

Utilizzare un programma di software remoto (ad es. HyperTerminal) per connettersi all'unità RIPM. Risettare l'unità e premere subito il tasto "ESC". Apparirà il seguente prompt "=>". Inviare il comando "config" e premere il tasto "ENTER". Il sistema vi richiederà di regolare la configurazione automatica dell'IP, l'indirizzo IP, la maschera di sottorete e il gateway predefinito. Premendo il tasto "ENTER" senza inserire i valori, le impostazioni rimarranno invariate. Il valore del gateway deve essere impostato su "0.0.0.0" (per nessun gateway) o qualsiasi altro valore per l'indirizzo IP del gateway. Dopo la conferma, l'unità RIPM eseguirà un risettaggio utilizzando i nuovi valori.

P75075ea_F1DE101Hea_man.indb 14 8/16/2006 11:36:42 AM

Interfaccia Web

L'unità RIPM è accessibile da un comune browser web compatibile con Java™. È possibile utilizzare il protocollo HTTP o una connessione protetta da crittografia via HTTPS. Immettere l'indirizzo IP configurato dell'unità nel browser web. Le impostazioni del login iniziale sono:

Parametro	Valore
Login	administrator
Password	belkin

È particolarmente consigliabile cambiare queste impostazioni su valori specifici per l'utente dalla pagina "Gestione dell'utente".

Telnet

Per accedere ad una periferica arbitraria collegata ad una delle porte seriali dell'unità RIPM tramite un terminale, è possibile utilizzare un client standard telnet.

L'interfaccia primaria dell'unità RIPM è l'interfaccia HTTP. Per utilizzare la finestra Remote Console del proprio sistema host, il browser deve prevedere la presenza di Java Runtime Environment (versione 1.1 o successive). Anche se il browser utilizzato non avesse alcun supporto Java, come nel caso di piccole periferiche palmari, si può continuare comunque a gestire il proprio sistema host remoto tramite i modelli di gestione visualizzati sul browser stesso.

È consigliabile utilizzare i seguenti browser nel caso si debba eseguire un collegamento non protetto con l'unità RIPM:

- Microsoft Internet Explorer (versione 5.0 o successiva) su Windows 2000 e XP
- Netscape Navigator 7.0 su Windows 2000 e XP

Per accedere al sistema di host remoto utilizzando una connessione crittografata, è necessario un browser in grado di supportare il protocollo HTTPS. Soltanto una chiave da 128 bit può garantire un alto livello di protezione.

P75075ea_F1DE101Hea_man.indb 15 8/16/2006 11:36:42 AM

Aprire il browser web. Digitare l'indirizzo dell'unità che è stato configurato durante la procedura d'installazione. A tal fine, è possibile utilizzare un indirizzo IP o un nome di dominio e host, nel caso in cui si fosse assegnato all'unità un nome simbolico nel DNS.

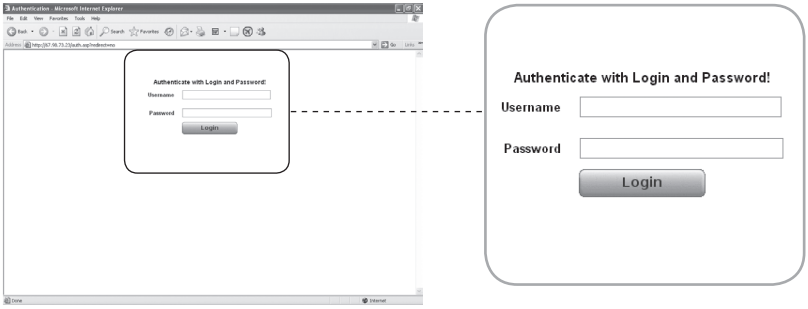
Per esempio, digitare il seguente indirizzo nella barra degli indirizzi del browser web quando si effettua una connessione non protetta:

http://192.168.1.22/

Quando si usa una protezione protetta, digitare:

http://192.168.1.22/

Questo vi porterà alla pagina di login come illustrato qui di seguito:



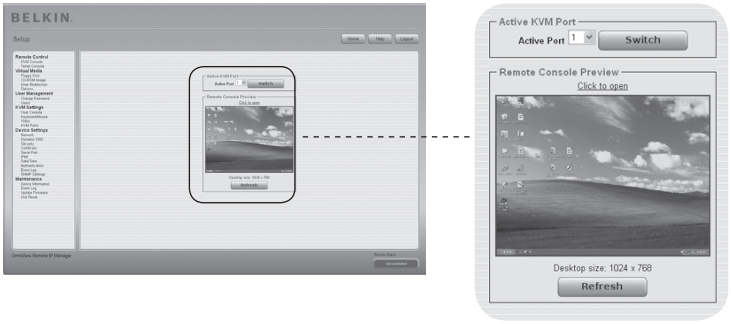
L'unità RIPM è dotata di un account integrato per l'amministratore cui è concesso amministrare il vostro sistema.

Parametro	Valore
Login	administrator
Password	belkin

Nota bene: il browser web deve essere in grado di accettare i cookie; altrimenti il login non è possibile.

P75075ea_F1DE101Hea_man.indb 16 8/16/2006 11:36:43 AM

La console remota visualizza lo schermo, la tastiera e il mouse del sistema host remoto in cui è stata installata l'unità RIPM. Il browser web utilizzato per accedere all'unità RIPM deve disporre di Java Runtime Environment (versione 1.1 o successiva). Tuttavia, è particolarmente consigliabile installare Sun JVM (Java Virtual Machine) 1.4. La console remota si comporterà esattamente come se si fosse seduti davanti allo schermo del sistema remoto; la tastiera e il mouse possono essere utilizzati come si è soliti fare. Aprire la console remota selezionando l'immagine d'anteprima sul sito principale del front end in HTML.



Tra le opzioni del menu disponibili figurano:

Pulsante di autoregolazione

Se la risoluzione video ottenuta fosse di qualità molto bassa o risultasse in qualche modo distorta, premere il pulsante ed attendere alcuni secondi, consentendo all'unità RIPM di eseguire le regolazioni necessarie per ottenere la qualità video migliore possibile.

Sincronizzazione del mouse

Questa opzione consente di sincronizzare il cursore del mouse locale con quello remoto. Questa funzione è particolarmente utile quando si utilizzano impostazioni accelerate del mouse sul sistema host.

Impostazioni video nel menu delle opzioni

Questa opzione consente di aprire una nuova finestra, dotata degli elementi necessari per controllare le impostazioni video dell'unità RIPM. Alcuni valori relativi alla luminosità e al contrasto dell'immagine visualizzata possono essere modificati, migliorando in questo modo la qualità video. È possibile anche tornare alle impostazioni standard per tutte le modalità video o soltanto per quella corrente.

Nota bene: Se al primo avvio il cursore del mouse locale non è sincronizzato con quello del mouse remoto, premere una volta il tasto "Auto-Adjust".

P75075ea_F1DE101Hea_man.indb 17 8/16/2006 11:36:43 AM

Tra l'unità RIPM e l'host, vi sono due interfacce disponibili per la trasmissione dei dati della tastiera e del mouse: USB e PS/2 (disponibili separatamente). Il funzionamento corretto del mouse remoto dipende da diverse impostazioni, di cui tratteremo nelle seguenti sottosezioni.

Interfaccia USB del Remote IP Manager

Per utilizzare l'interfaccia USB, occorre collegare l'host controllato e l'unità di gestione con i cavi appropriati. Per esempio, se nel BIOS dell'host controllato non vi è un supporto per tastiera USB e si è collegato soltanto il cavo USB, non si potrà accedere alla tastiera remota durante il processo di accensione dell'host. Vi preghiamo di leggere la sezione "Tastiera/Mouse" a pagina 48.

Impostazioni della tastiera del Remote IP Manager

Le impostazioni dell'unità per il tipo di tastiera dell'host devono essere corrette cosicché la tastiera remota possa funzionare correttamente. Verificare le impostazioni nel front end dell'unità RIPM. Vi preghiamo di leggere la sezione "Tastiera/Mouse" a pagina 48.

Impostazioni del mouse remoto

Un problema comune ai dispositivi KVM è la sincronizzazione tra il cursore del mouse locale e quello del mouse remoto. L'unità RIPM affronta questa situazione con un intelligente algoritmo di sincronizzazione. L'unità RIPM prevede tre modalità di impostazione del mouse.

- **Rilevazione automatica della velocità del mouse**
  Questa modalità cerca di rilevare automaticamente le impostazioni della velocità e dell'accelerazione del sistema host. Leggere la sezione qui sotto per informazioni più dettagliate.

- **Rilevazione della velocità del mouse fisso**

  Questa modalità traduce i movimenti del mouse dalla console remota in modo tale che il movimento di un pixel provochi il movimento di un altro pixel sul sistema remoto. Questo parametro è regolabile tramite il ridimensionamento. Vi preghiamo di ricordare che ciò funziona solo quando l'accelerazione del mouse sul sistema remoto è disattivata.

- **Modalità di mouse singolo e doppio**
  Questa modalità è descritta nella sezione "Modalità di mouse singolo e doppio" a pagina 20.

P75075ea_F1DE101Hea_man.indb 18 8/16/2006 11:36:43 AM

Sincronizzazione e rilevazione automatica della velocità del mouse

Questa modalità esegue la rilevazione della velocità durante la sincronizzazione del mouse. Ogni volta che il mouse non si sposta in modo corretto, vi sono due modi per resincronizzare il mouse locale e quello remoto:

- **Sincronizzazione rapida**
  Si tratta di una modalità di sincronizzazione rapida utilizzata per correggere un'eventuale distorsione provvisoria ma fissa. Scegliere questa opzione dal menu delle opzioni della console remota. Se impostata, è anche possibile premere la sequenza di tasti di scelta rapida per la sincronizzazione del mouse (vedi la sezione "Barra di controllo della console remota" a pagina 23).

- **Sincronizzazione intelligente**
  Se la sincronizzazione non dovesse funzionare o se le impostazioni del mouse fossero state modificate nel sistema host, utilizzare la resincronizzazione intelligente. Questo metodo regola i parametri per l'effettivo movimento del cursore del mouse in modo che quest'ultimo sia visualizzato sullo schermo nella corretta posizione. Questo metodo richiede più tempo rispetto alla sincronizzazione rapida e può essere attivato mediante la voce adatta nel menu delle opzioni della console remota. La sincronizzazione intelligente richiede che l'immagine sia regolata correttamente. Utilizzare la funzione di autoregolazione o la correzione manuale nel pannello delle impostazioni video per impostare l'immagine. La forma del cursore del mouse ha un'influenza significativa sul rilevamento del cursore. È consigliabile utilizzare una forma semplice, ma comune, per il cursore. Nel maggior parte dei casi, la rilevazione e la sincronizzazione delle forme del cursore potrebbe fallire. In generale, è quasi impossibile che le forme del cursore che cambiano durante il rilevamento del cursore vengano visualizzate nell'immagine trasferita a video. L'utilizzo di una forma standard del cursore garantisce che il processo di rilevamento e quello di sincronizzazione si svolgano nel modo migliore possibile.

Il tasto "Mouse" sulla console remota può comportarsi in modi diversi, a seconda dallo stato attuale della sincronizzazione del mouse. Solitamente, premento questo tasto si esegue una sincronizzazione rapida, tranne in situazioni in cui la modalità del video è stata di recente modificata. Vi preghiamo di leggere anche la sezione "Barra di controllo della console remota" a pagina 23.

Nota bene: Se al primo avvio il cursore del mouse locale non è sincronizzato con quello del mouse remoto, premere una volta il tasto "Auto-Adjust"..

P75075ea_F1DE101Hea_man.indb 19 8/16/2006 11:36:44 AM

Impostazione del mouse del sistema host

Il sistema operativo dell'host riconosce diverse impostazioni per il driver del mouse.

Sebbene l'unità RIPM funzioni con mouse accelerati e sia in grado di sincronizzare il cursore del mouse locale con quello del mouse remoto, le seguenti restrizioni potrebbe impedire il corretto svolgimento del processo di sincronizzazione.

- **Driver speciali per mouse**
  Si tratta di driver di mouse in grado di influire sul processo di sincronizzazione che può compromettere la sincronizzazione dei mouse. In caso la sincronizzazione venisse compromessa, accertarsi di non utilizzare alcun driver per mouse speciale specifico del rivenditore sul proprio sistema host.

- **Impostazioni del mouse su Windows 2003 Server/XP**
  Windows XP prevede un'impostazione chiamata "migliora l'accelerazione del mouse"
  che deve essere disattivata.

- **Active Desktop**
  Se la funzione "Active Desktop" di Microsoft Windows è abilitata, non utilizzare uno sfondo normale. È necessario scegliere un disegno di fondo. In alternativa, si potrebbe anche disabilitare del tutto la funzione di Active Desktop.

  Posizionare il cursore del mouse nell'angolo in alto a sinistra della schermata applet e muoverlo leggermente avanti e indietro. In questo modo si resincronizzerà il mouse.
  Se la resincronizzazione fallisce, disabilitare l'accelerazione del mouse e ripetere la procedura.

- **Modalità di mouse singolo e doppio**
  Le informazioni sopra menzionate valgono per la modalità di mouse doppio, per cui il cursore del mouse locale e quello del mouse remoto sono visibili e devono essere sincronizzati.
  L'unità RIPM prevede anche la modalità di mouse singolo, per cui soltanto il cursore del mouse remoto è visibile. Attivare questa modalità nella console remota (vedi la sezione "Barra di controllo della console remota" a pagina 23) e cliccare nella finestra. Il cursore del mouse locale sarà nascosto e quello del mouse remoto potrà essere controllato direttamente. Per disattivare questa modalità, occorre definire una sequenza di tasti di scelta rapida per il mouse nel pannello delle impostazioni della console remota. Premere questo tasto per liberare il cursore del mouse locale memorizzato.

P75075ea_F1DE101Hea_man.indb 20 8/16/2006 11:36:44 AM

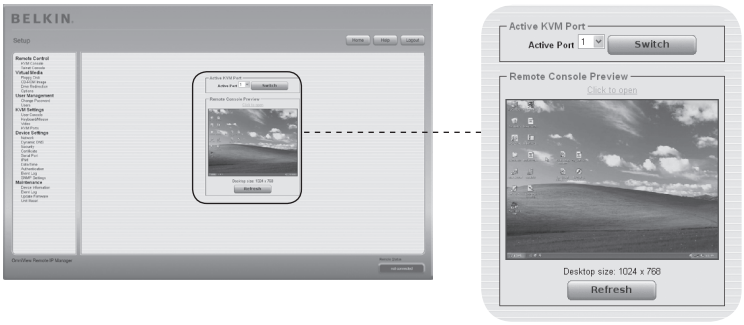
Impostazioni consigliate del mouse

Windows 2000, 2003, XP (tutte le versioni)	In generale, è consigliabile utilizzare un mouse tramite USB. Scegliere USB senza la sincronizzazione del mouse.
Mac OS X	È consigliabile utilizzare la modalità di mouse singolo.
Sun Solaris	Regolare le impostazioni del mouse tramite “xset m 1” o utilizzando il pannello di controllo CDE per un’impostazione “1:1, no acceleration”. In alternativa, si può anche utilizzare la modalità di mouse singolo.
Linux	Scegliere l’opzione “Altri sistemi operativi” dal menu “Tipo di mouse”. Quindi, scegliere l’opzione “Auto Mouse Speed” (Rilevazione automatica della velocità del mouse) Questo vale per mouse USB e PS/2.

P75075ea_F1DE101Hea_man.indb 21 8/16/2006 11:36:44 AM

Navigazione

Una volta che il collegamento con l'unità è avvenuto con successo, appare la pagina principale dell'unità RIPM. Questa pagina consiste di tre parti, ognuna delle quali contiene informazioni specifiche. I tasti sul lato superiore consentono di navigare all'interno del front end
(vedi la tabella per maggiori dettagli). Il riquadro in basso a sinistra contiene una barra di navigazione che consente di commutare tra le diverse sezioni dell'unità. Le informazioni specifiche di un compito, che dipendono dalla sezione precedentemente scelta, sono visualizzate nel riquadro di destra.



Nota bene: Se non si riscontra alcuna attività per 30 minuti, l'unità RIPM vi scollegherà automaticamente. Cliccando su uno dei link, si ritornerà alla schermata di login.

P75075ea_F1DE101Hea_man.indb 22 8/16/2006 11:36:44 AM

La parte superiore della finestra della console remota contiene una barra di controllo. Utilizzando i suoi elementi, è possibile vedere lo stato della console remota e influenzare le impostazioni della console remota. Qui di seguito riportiamo una descrizione per ogni comando.

- **Pulsante di autoregolazione**

Se la risoluzione video ottenuta fosse di qualità molto bassa o risultasse in qualche modo distorta, premere il pulsante ed attendere alcuni secondi, consentendo all'unità RIPM di eseguire le regolazioni necessarie per ottenere la qualità video migliore possibile.

- **Sincronizzazione del mouse**

Questa opzione consente di sincronizzare il cursore del mouse locale con quello remoto. Questa funzione è particolarmente utile quando si utilizzano impostazioni accelerate del mouse sul sistema host. In generale, non c'é bisogno di modificare le impostazioni del mouse.

- **Modalità di mouse singolo e doppio**

Scegliere questa modalità per passare dalla modalità di mouse singolo (per cui soltanto il cursore del mouse remoto è visibile) alla modalità di doppio mouse (per cui il cursore del mouse remoto e quello del mouse locale sono visibili e sincronizzati). La modalità di mouse singolo è disponibile solo con Sun JVM (versione 1.4 o successive).

- **Opzioni**

Per aprire il menu delle opzioni, cliccare il tasto "Opzioni".

Qui di seguito riportiamo una breve descrizione di questa opzione:

- **Solo Monitor**

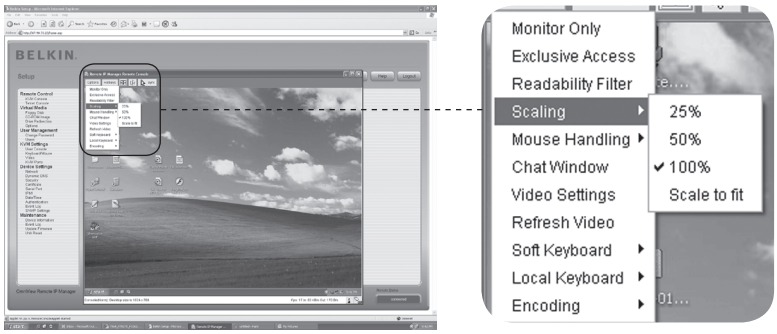
  Attivare o disattivare il filtro "Solo Monitor". Se il filtro è attivo, l'interazione con la console remota non sarà possibile, ma la si potrà monitorare.

- **Accesso esclusivo**

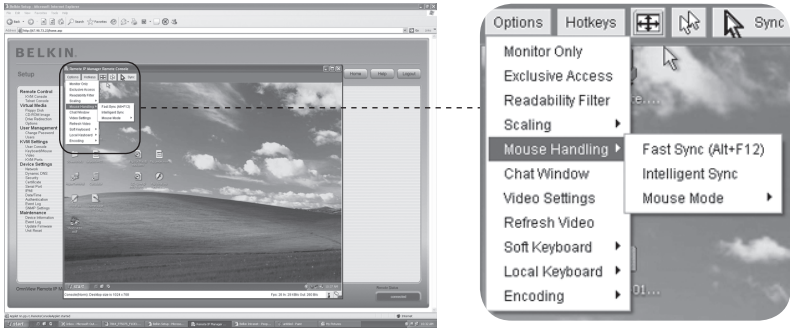
  Con l'autorizzazione appropriata, è possibile chiudere la console remota di tutti gli altri utenti. Nessuno potrà aprire la console remota nello stesso tempo finché non si disabiliterà l'accesso esclusivo o ci si scollegherà.

P75075ea_F1DE101Hea_man.indb 23 8/16/2006 11:36:45 AM

- **Ridimensionamento**
  Consente di ridimensionare la console remota. Si possono ancora utilizzare mouse e tastiera, ma l'algoritmo di ridimensionamento non mantiene tutti i dettagli di visualizzazione.



- **Gestione del mouse**
  Il menu secondario per la gestione del mouse mette a disposizione due opzioni per sincronizzare il cursore del mouse locale e di quello remoto.



- **Sincronizzazione rapida**
  Si tratta di una modalità di sincronizzazione rapida utilizzata per correggere un'eventuale distorsione provvisoria ma fissa.

- **Sincronizzazione intelligente**
  Utilizzare questa opzione se la sincronizzazione rapida non funziona o se le impostazioni del mouse sul sistema host sono state modificate.

  Avvertenza: Questo metodo richiede più tempo rispetto alla sincronizzazione rapida e necessita di un'immagine regolata in modo corretto. Utilizzare la funzione di autoregolazione o la correzione manuale nel pannello delle impostazioni video per impostare l'immagine.

P75075ea_F1DE101Hea_man.indb 24 8/16/2006 11:36:46 AM

- **Cursore locale**

  Propone un elenco di forme diverse del cursore tra cui scegliere quella per il puntatore del mouse locale. La forma selezionata sarà salvata per l'utente connesso e verrà attivata ogni volta che questo utente apre la console remota. Il numero delle forme disponibili dipende dalla versione di Java Virtual Machine (JVM): le versioni 1.2 e successive prevedono un elenco completo.

- **Impostazioni video**

  Apre una schermata per modificare le impostazioni video dell'unità RIPM. L'unità presenta due diversi dialoghi che influenzano le impostazioni video.

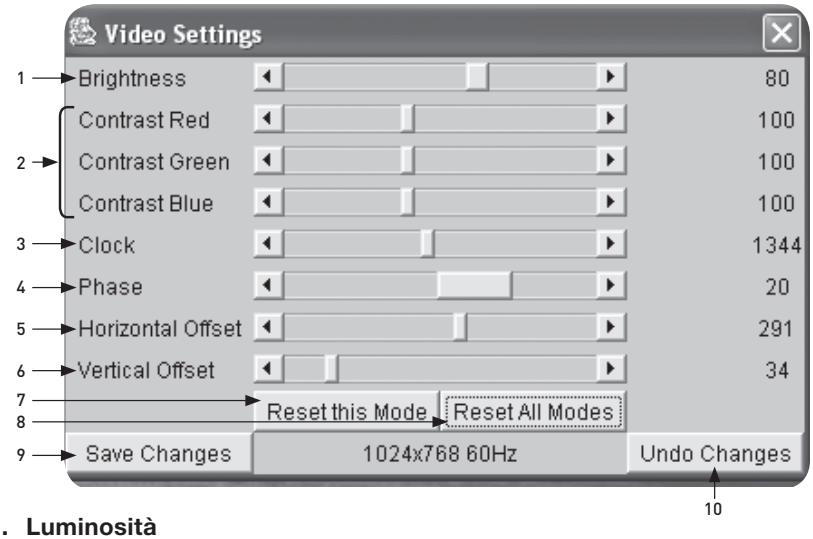
- **Impostazioni video tramite front end in HTML**

  Selezionare questa opzione per abilitare la porte video locale. Questa opzione determina se l'uscita video locale dell'unità è attiva e sta trasferendo il segnale in entrata proveniente dal sistema host.

  L'opzione "Noise Filter" (Filtro rumori) definisce la modalità di reazione dell'unità alle piccole modifiche al segnale video in entrata. L'impostazione di un filtro di grandi dimensioni necessita un minor traffico di rete e assicurerà una visualizzazione in video più rapida, sebbene i cambiamenti più piccoli in alcune zone potrebbero non essere riconosciuti. Un filtro di piccole dimensioni visualizza istantaneamente tutti i cambiamenti, ma, anche se il contenuto dello schermo, in realtà, non sta cambiando potrebbe causare una crescita costante del traffico di rete (a seconda della qualità del segnale video in entrata). Le impostazioni predefinite potrebbe essere adatte alla maggior parte delle situazioni.

P75075ea_F1DE101Hea_man.indb 25 8/16/2006 11:36:46 AM

Impostazioni video tramite la console remota



1. **Luminosità**
   Regola la luminosità dell'immagine.
2. **Contrasto**
   Regola il contrasto della nitidezza dell'immagine.
3. **Frequenza**
   Definisce la frequenza orizzontale per una linea video e dipende dalla modalità video. Le schede video di un altro tipo potrebbe richiedere valori diversi. Le impostazioni predefinite insieme alla procedura di autoregolazione dovrebbero essere appropriate per tutte le configurazioni comuni. Per ottenere una migliore qualità dell'immagine, provare a modificare queste impostazioni insieme alla fase di campionamento.
4. **Fase**
   Definisce la fase per il campionamento video, utilizzato per regolare la qualità del display e l'impostazione della frequenza di campionamento.
5. **Spostamento orizzontale**
   Con i pulsanti sinistro e destro, spostare l'immagine in direzione orizzontale con questa opzione selezionata.
6. **Spostamento verticale**
   Con i pulsanti sinistro e destro, spostare l'immagine in direzione verticale con questa opzione selezionata.
7. **Ripristina questa modalità**
   Ripristina le impostazioni predefinite per questa modalità.
8. **Ripristina tutte le modalità**
   Ripristina le impostazioni predefinite per tutte le modalità.
9. **Salva modifiche**
   Salva le modifiche in modo permanente.
10. **Annulla modifiche**
    Ripristina le ultime impostazioni.

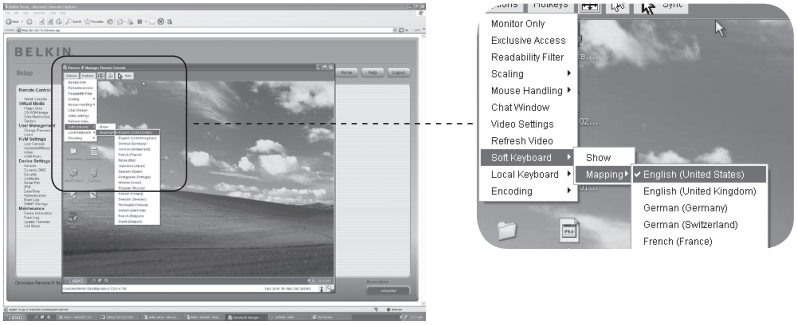
P75075ea_F1DE101Hea_man.indb 26 8/16/2006 11:36:46 AM

Sequenza di mappatura

Tastiera virtuale
Apre il menu per la tastiera virtuale.

Mostra
Visualizza la tastiera virtuale. La tastiera virtuale serve nel caso in cui il sistema host utilizza una lingua e una mappatura del paese completamente diverse da quelle della macchina di amministrazione.

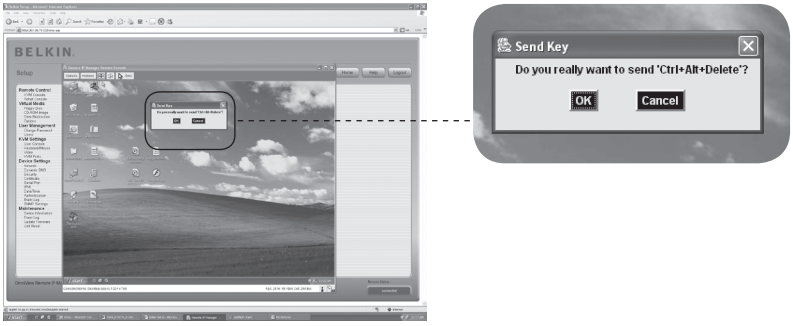
Mappatura
Serve per scegliere la lingua appropriata e effettuare la mappatura della tastiera virtuale.



P75075ea_F1DE101Hea_man.indb 27 8/16/2006 11:36:47 AM

Tastiera locale
Serve per cambiare la mappatura della lingua del browser che esegue l'applet sulla console remota. Normalmente, l'applet determina automaticamente il valore corretto. Tuttavia, a seconda delle impostazioni di JVM e del browser, ciò non è sempre possibile. Un esempio tipico è costituito da un sistema tedesco localizzato che utilizza una mappatura inglese (USA) della tastiera. In questo caso, è necessario regolare manualmente l'impostazione della tastiera locale sulla lingua corretta.

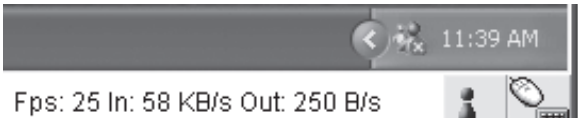
Tasti di scelta rapida
Apre un elenco di tasti di selta rapida predefiniti. Scegliere una voce e il comando sarà inviato al sistema host. È possibile aggiungere un dialogo di conferma che sarà visualizzato prima che il comando selezionato sia inviato all'host remoto. Selezionare "OK" per eseguire il comando sull'host remoto.



P75075ea_F1DE101Hea_man.indb 28 8/16/2006 11:36:47 AM

La linea di stato mostra la console remota e lo stato della connessione. Le dimensioni dello schermo remoto sono visualizzate sulla sinistra. Il valore tra le parentesi descrive la connessione alla console remota. Con “Norm” si indica una connessione standard senza crittografia; “SSL” indica una connessione sicura che utilizza SSL.

Il traffico di rete in entrata (“In:”) e in uscita (“Out”) sono espressi in kilobyte per secondo. Se la codifica compressa è abilitata, un valore tra parentesi visualizzerà la velocità di trasferimento compressa.



Il tasto successivo mostra le impostazioni di accesso alla console remota.

Uno o più utenti sono connessi alla console remota dell’unità RIPM.

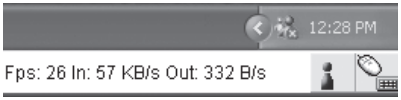
Voi disponete di un accesso esclusivo. Nessun altro utente può accedere all’host remoto dalla console remota se non si disabilita questa opzione.

P75075ea_F1DE101Hea_man.indb 29 8/16/2006 11:36:48 AM

Un utente remoto ha l'accesso esclusivo. Non è possibile accedere all'host remoto dalla console remota se l'altro utente non disabilita questa opzione.

Il tasto sull'estrema destra mostra lo stato delle impostazioni di "Solo Monitor".

L'opzione "Solo Monitor" è disabilitata.



L'opzione "Solo Monitor" è abilitata.

Per maggiori informazioni sulle impostazioni di Solo Monitor e Accesso esclusivo, leggere la sezione "Barra di controllo della console remota" a pagina 23 di questo manuale d'uso.

P75075ea_F1DE101Hea_man.indb 30 8/16/2006 11:36:49 AM

Ripristino delle impostazioni predefinite dell'unità RIPM

Per resettare l'unità e ripristinare i valori predefiniti delle impostazioni di rete

1. Effettuare una connessione seriale per la configurazione iniziale (HyperTerminal)

Bit per secondo:	115200
Bit di dati:	8
Parità:	nessuno
Bit di arresto:	1
Controllo di flusso:	hardware o nessuno

2. Premere il tasto di ripristino situato tra il jack di alimentazione su CC e il jack di rete. Rilasciare il tasto di ripristino e premere immediatamente ESC per diverse volte nel programma terminale seriale (HyperTerminal) fin quando non appare il prompt "=>".

Nota bene: Se il prompt non viene visualizzato tre secondi dopo aver rilasciato il tasto di reset, ripetere la fase 1 e 2. L'unità rileverâ il comando ESC solo durante i primi tre secondi del processo di accensione.

3. Quando richiesto, digitare "defaults" il premere il tasto Invio. L'unità RIPM, quindi, si caricherà e ripristinerà le impostazioni predefinite.

4. Spegnere il server (il computer al quale l'unità è collegata localmente).

5. Staccare l'alimentatore dall'unità insieme ai cavi della porta "CPU/KVM switch" e al cavo di rete.

6. Ricollegare i cavi e accendere il server.

Ora è possibile riconfigurare l'unità con le impostazioni di rete attraverso una connessione HyperTerminal o utilizzando un software d'installazione.

Scollegamento dal Remote IP Manager

Questo tasto consente all'utente attuale di disconnettersi e visualizza una nuova schermata di login. Vi preghiamo di notare che il sistema si scollegherà automaticamente se non si registra alcuna attività per più di 30 minuti.

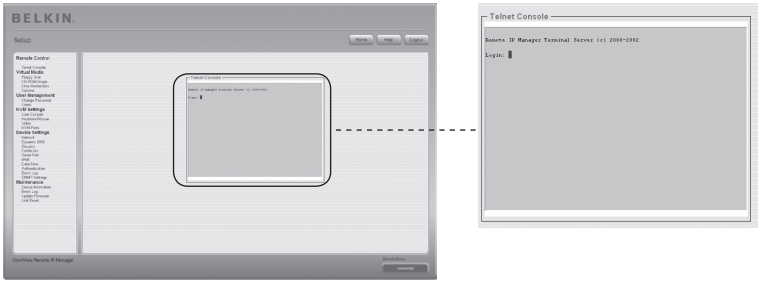
P75075ea_F1DE101Hea_man.indb 31 8/16/2006 11:36:49 AM

Console KVM

Anteprima della console remota

Per aprire la console KVM, fare clic sulla voce menu sulla sinistra o sull'immagine della console sulla destra. Per aggiornare l'immagine, fare clic sul tasto "Refresh" (Aggiorna).

Console Telnet



Il firmware dell'unità dispone di un gateway Telnet che consente all'utente di collegarsi all'unità tramite un client Telnet standard. Per collegarsi all'unità RIPM utilizzando il protocollo Telnet, occorre utilizzare un programma terminale come xterm, TeraTerm o PuTTY. IN alternativa, è anche possibile inviare un comando Telnet sulla linea di comando o utilizzare la finestra di dialogo "Esegui" dal menu di avvio di Windows. Come esempio, digitare la seguente frase:

Telnet: 192.168.1.22

P75075ea_F1DE101Hea_man.indb 32 8/16/2006 11:36:50 AM

Sostituire l'indirizzo IP con un indirizzo assegnato dall'unità RIPM durante l'installazione. Il sistema vi richiederà il nome utente e la password per collegarsi con il dispositivo. Le informazioni che occorre inserire per l'autenticazione sono uguali a quelle dell'interfaccia web. Ciò significa che la gestione dell'interfaccia Telnet è controllata interamente con le funzioni appropriate dell'interfaccia web. Una volta che il collegamento con l'unità è stato effettuato con successo, il sistema visualizzerà una linea di comando in cui potrete inserire i corretti comandi di gestione. In generale, l'interfaccia Telnet supporta due modalità operative: La modalità a linea di comando e la modalità terminale. La modalità a linea di comando è utilizzata per controllare o visualizzare alcuni parametri. Nella modalità terminale, l'accesso passante alla porta seriale 1 è attivato (se le impostazioni seriali sono corrette). Per accedere all'unità RIPM tramite l'interfaccia seriale, è necessario usare un cavo null modem. Tutti gli input sono reindirizzati al dispositivo sulla porta seriale 1 e le risposte sono visualizzate sull'interfaccia Telnet.

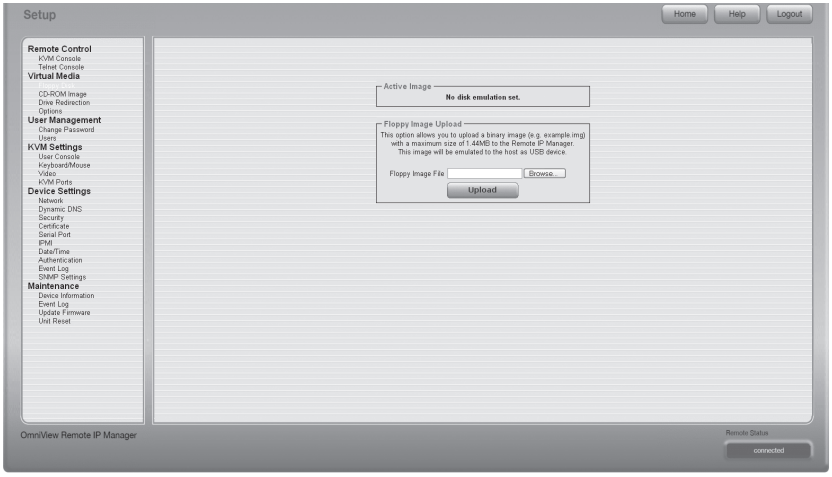
Il seguente elenco mostra l'uso e la sintassi dei comandi.

Help	Visualizza un elenco di comandi possibili.
cls	Ripulisce lo schermo.
quit	Chiude la sessione in esecuzione e si scollega dal client.
version	Visualizza le informazioni sulla versione del software.
terminal	Avvia la modalità a passante terminale per la porta seriale 1. La sequenza di comnadi "esc exit" ritorna alla modalità a linea di comando. Il comando ha un parametro opzionale (1o 2) per selezionare la porta seriale desiderata per l'accesso passante.

.

P75075ea_F1DE101Hea_man.indb 33 8/16/2006 11:36:50 AM

Floppy Disk



Questa funzione serve per inviare e trasferire file di immagini. Questa opzione consente di inviare all'unità un'immagine binaria (esempio.img) di una grandezza massima di 1,44 MB. Questa immagine sarà simulata sull'host come un dispositivo USB. Tutti gli altri formati devono essere trasferiti utilizzando una funzione di reindirizzamento sull'unità disco. Per usare un'immagine di dimensioni maggiori, creare questa immagine con Windows Share.

Invio di un'immagine floppy

Fase 1: Fare clic su "Browse" per specificare il file da trasferire.

Fase 2: Fare clic su "Upload" per inviare il file all'unità RIPM. Un messaggio confermerà che il file è stato correttamente inviato all'unità RIPM.

Fase 3: Fare clic su "KVM Console" nella sezione della console remota dell'interfaccia RIPM per accedere al desktop del computer remoto.

Fase 4: Fare doppio clic sull'icona Risorse del computer.

Fase 5: Nelle risorse del computer figurerà una seconda voce per il floppy drive. Questa voce è denominata "3-1⁄2 Floppy (B)". È possibile accedere ai file che sono stati trasferiti qui.

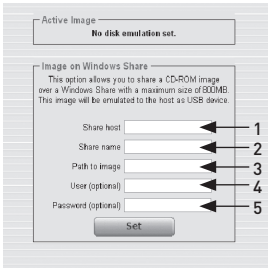
P75075ea_F1DE101Hea_man.indb 34 8/16/2006 11:36:51 AM

Immagine del CD-ROM

Utilizzare l'immagine su Windows Share (SAMBA).

Per includere un'immagine da Windows Share, selezionare "CD-ROM" dal sottomenu.

Occorre fornire le seguenti informazioni per creare in modo corretto l'immagine selezionata:



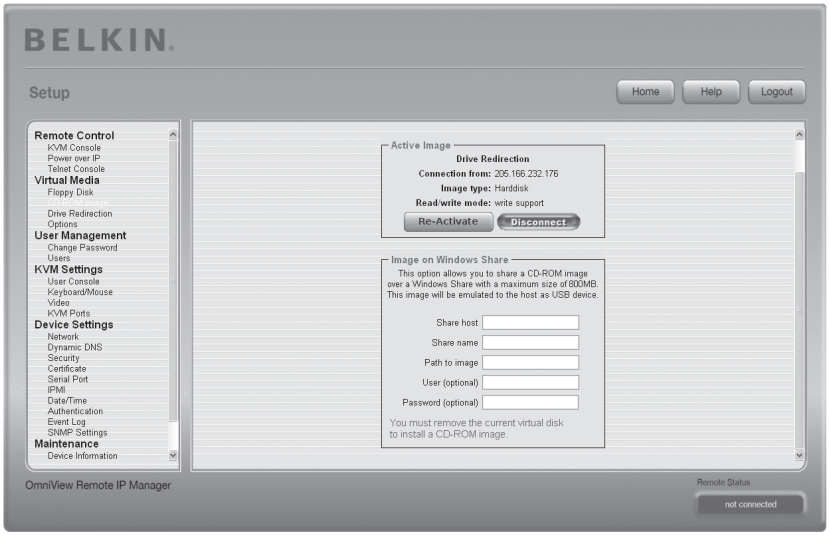
1. **Condividi host**
   Il nome del server o il suo indirizzo IP. (L'indirizzo IP si ottiene avviando il software di reindirizzamento dell'unità - descritto qui sotto).
2. **Condividi nome**
   Il nome della casella condivisa da utilizzare.
3. **Percorso dell'immagine**
   Il percorso del file di immagine.
4. **Utente (opzionale)**
   Se necessario, specificare il nome utente per la condivisione. Se non è specificato
   e viene attivato un account guest, le informazioni di questo account saranno utilizzate per il login.
5. **Password (opzionale)**
   Se viene richiesta la password, specificare la password per il nome utente fornito.

P75075ea_F1DE101Hea_man.indb 35 8/16/2006 11:36:51 AM

Invio di un'immagine del CD-ROM

Fase 1: Aprire e avviare il software di reindirizzamento dell'unità disco

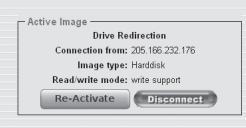
Fase 2: Quando il software di reindirizzamento dell'unità disco si è collegato, lasciare aperta questa finestra e andare sull'immagine del CD-ROM nella sezione Supporto virtuale dell'interfaccia RIPM..



Nota bene: L'indirizzo IP riportato sotto "Connection From" è l'indirizzo IP utilizzato come indirizzo host di condivisione. Per verificare la correttezza dell'indirizzo IP assegnato dal software di reindirizzamento dell'unità disco, collegare l'unità RIPM al computer usando un cavo seriale e aprire una sessione di HyperTerminal. Collegarsi come "ping" e digitare l'indirizzo IP nello stesso modo in cui appare nel campo "Share Host". Dovrebbe comparire il messaggio "<IP> is alive!"

P75075ea_F1DE101Hea_man.indb 36 8/16/2006 11:36:52 AM

Fase 3: Fare clic su “Re-Activate” nella sezione Active Image.



Fase 4: Inserire l’indirizzo IP assegnato dal software di reindirizzamente dell’unità disco nel campo “Share Host “.

Fase 5: Inserire il nome di condivisione e il percorso dell’immagine.

Fase 6: Per inviare il file, cliccare sul tasto “Set”. Il file sarà visualizzato come un dispositivo USB sul computer remoto.

L’immagine specificata dovrebbe essere accessibile dall’unità RIPM. Le informazioni sopra menzionate devono essere fornite dal punto di vista dell’unità. È importante specificare gli indirizzi IP corretti e i nomi dei dispositivi. In caso contrario, l’unità potrebbe non essere in grado di accedere al file di immagine di riferimento e il file non potrà essere montato (il sistema visualizzerà un messaggio di errore). È consigliabile utilizzare valori corretti e ripetere questa operazione, se necessario.

La condivisione specificata deve essere configurata in modo corretto. Per questo occorre un’autorizzazione. Non è possibile ottenere questa autorizzazione in qualità di utente ordinario. Occorre collegarsi come amministratore di sistema o richiedere l’aiuto dell’amministratore di sistema.

P75075ea_F1DE101Hea_man.indb 37 8/16/2006 11:36:52 AM

Reindirizzamento dell'unità disco

La funzione di reindirizzamento dell'unità disco offre un altro modo per utilizzare l'unità disco virtuale sul computer remoto. È possibile utilizzare l'unità disco sul computer local dal terminale remoto condividendo l'unità disco su una connessione di rete TCP. Le periferiche di archiviazione, come floppy disc, dischi rigidi, CD-ROM e dischi rimovibili (quali chiavette USB) possono essere reindirizzate. È anche possibile configurare il calcolatore remoto per poter scrivere dati sul disco locale.

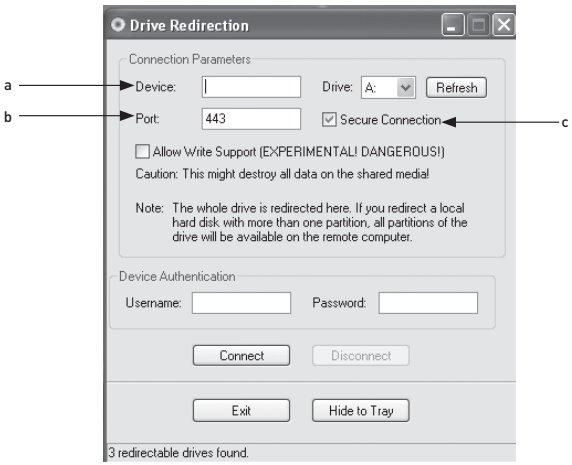
***Nota bene:** Belkin non consiglia di abilitare il supporto in scrittura durante il reindirizzamento di dischi rigidi e non sarà esente da ogni responsabilità in caso di perdita o corruzione di dati durante questo processo.

Vi preghiamo di utilizzare questa funzione con molta cautela. Il reindirizzamento dell'unità disco si svolge a un livello di gran lunga inferiore al sistema operativo, tanto che né il sistema operativo locale né quello remoto possono riconoscere che si sta effettuando un reindirizzamento dell'unità disco. Ciò può causare delle incongruità nel caso in cui uno dei sistemi operativi (sulla macchina locale o sull'host remoto) scrive dati sul dispositivo. Con il supporto in scrittura abilitato, il computer remoto può danneggiare i dati e il file system sul dispositivo reindirizzato. Se, invece, il sistema operativo locale scrive dati sul dispositivo reindirizzato, la memoria cache dell'unità disco sul sistema operativo dell'host remoto potrebbe contenere vecchi dati che confondono il sistema operativo dell'host remoto. È pertanto consigliabile utilizzare con molta cautela la funzione di reindirizzamento dell'unità disco, in particolar modo il supporto in scrittura.

Nota bene: Per poter utilizzare la funzione di reindirizzamento dell'unità disco, occorre installare il software di reindirizzamento dell'unità disco (incluso nella confezione) sul computer che si utilizza per accedere a distanza all'unità RIPM.

P75075ea_F1DE101Hea_man.indb 38 8/16/2006 11:36:52 AM

1. **Aprire l'applicazione di reindirizzamento dell'unità disco.**



2. **Specificare i parametri della connessione di rete.**
   - **a. Dispositivo**
     Questo è l'indirizzo IP dell'unità RIPM alla quale si desidera collegarsi.
   - **b. Porta**
     Questa è la porta di rete. Per default, l'unità RIPM utilizza la porta della console remota (#443). È possibile modificare questo valore se, nelle impostazioni di rete dell'unità, la porta della console remota è stata cambiata.
   - **c. Connessione protetta**
     Spuntare questa casella per effettuare una connessione protetta via SSL. Così facendo si aumenta il livello di protezione; tuttavia, si potrebbe ridurre la velocità di connessione.
3. **Selezionare l'unità disco che si desidera reindirizzare.** Tutti i dispositivi disponibili verranno visualizzati (tramite lettere corrispondenti alle unità disco). Vi preghiamo di notare che l'unità RIPM condivide l'intera unità disco con il computer remoto e non soltanto una partizione. Se il disco rigido dispone di più di una partizione, tutte le lettere delle unità disco a cui appartengono, verranno reindirizzate. Utilizzare il tasto "Refresh" per ricreare l'elenco di lettere delle unità disco, in particolar modo per le chiavette USB.
4. **Supporto in scrittura**

   Avvertenza: Utilizzare questa funzione con cautela. Il supporto in scrittura consente al computer remoto di scrivere sull'unità disco locale. Se il sistema locale e quello remoto cercano contemporaneamente di scrivere dati sullo stesso **dispositivo, il file system sull'unità disco sarà distrutto.** Utilizzare questa funzione soltanto nella certezza assoluta che si possa eseguire in modo sicuro.

   Nota bene: Belkin non consiglia di abilitare il supporto in scrittura durante il reindirizzamento di dischi rigidi e non sarà esente da ogni responsabilità

P75075ea_F1DE101Hea_man.indb 39 8/16/2006 11:36:52 AM

in caso di perdita o corruzione di dati durante questo processo.

5. **Autenticare il dispositivo.** Per utilizzare il reindirizzamente dell'unità disco, occorre autenticare l'unità RIPM con un nome utente e una password validi. È necessaria l'autorizzazione per modificare la configurazione del disco virtuale.
6. **Effettuare il reindirizzamento dell'unità disco premendo una volta il tasto "Connect".**
   Se tutte le impostazioni sono corrette, la barra di stato visualizzerà che la connessione è stata effettuata, che il tasto "Connect" è disabilitato e che il tasto "Disconnect" è abilitato. In caso di errore, la barra di stato
   mostrerà un messaggio di errore.

   Il software di reindirizzamento dell'unità disco cerca di chiudere l'unità disco prima che venga reindirizzata. Questo impedisce al sistema operativo locale di accedere all'unità disco non appena viene reindirizzata. Il tentativo fallirà se durante l'operazione verrà aperto un file sull'unità disco. In caso di un errore di chiusura, vi si richiederà di confermare di voler stabilire la connessione. Tuttavia, non dimenticare che se il supporto in scrittura è abilitato, il reindirizzamento dell'unità disco potrebbe danneggiare un'unità disco non chiusa.
7. Utilizzare il tasto "Disconnect" per arrestare il reindirizzamento di un'unità disco dopo l'avvio della procedura.
8. Fare clic su "Exit" per chiudere il programma di reindirizzamento dell'unità disco. Se si attiva una connessione di reindirizzamento dell'unità disco, la connessione verrà chiusa prima che l'applicazione termini.
9. Utilizzare il tasto "Hide to Tray" per minimizzare l'applicazione senza terminarla completamente. La connessione rimarrà attiva fin quando non si chiuderà l'applicazione. È possibile accedere al software facendo doppio clic sull'icona presente sulla barra di sistema. L'icona indica anche se la connessione è stata stabilita o meno. Fare clic sull'icona con il tasto destro per aprire il sottomenu.

Opzioni:

Disabilita il reindirizzamento dell'unità disco
Questo disattiverà il reindirizzamento dell'unità disco.

Imponi connessioni di sola lettura
Questo disattiva il supporto in scrittura per il reindirizzamento dell'unità disco.

Fare clic su "Apply" per applicare le modifiche.

P75075ea_F1DE101Hea_man.indb 40 8/16/2006 11:36:52 AM

Come creare un'immagine

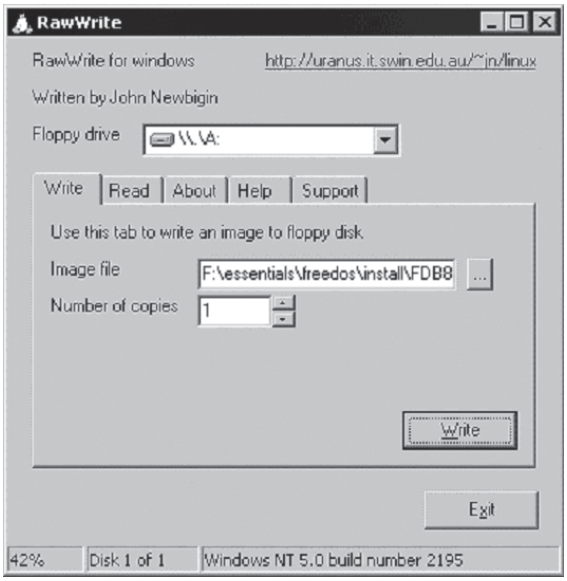
Immagini floppy

Sistemi operativi UNIX® e simili a UNIX

Per creare un file di immagine, utilizzare "dd". Si tratta di uno dei programmi di utilità di UNIX più originali ed è presente in ogni sistema operativo di tipo UNIX (UNIX, Sun Solaris, Linux). Per creare un'immagine floppy, copiare il contenuto di un floppy su un file. Si può utilizzare il seguente comando: dd [if=/dev/fd0] [of=/tmp/floppy.image]. In questo caso, "dd" legge il disco intero dal dispositivo "/dev/fd0" e salva i dati elaborati nel file di emissione specificato "/tmp/floppy.image". Regolare i parametri secondo le proprie esigenze (dispositivi di entrata, ecc.)

MS Windows

È possibile utilizzare lo strumento "RawWrite for Windows".



Selezionare la scheda "Read" dal menu. Immettere (o scegliere) il nome del file nel quale si desidera salvare il contenuto del floppy. Cliccare sul tasto "Copy" per inizializzare il processo di creazione dell'immagine. Per gli strumenti associati, andate sulla home page di "fdos project" **(http://www.fdos.org).**

P75075ea_F1DE101Hea_man.indb 41 8/16/2006 11:36:53 AM

Immagini di CD-ROM/ISO 9660

Sistemi operativi UNIX® e simili a UNIX

Per creare un file di immagine, utilizzare “dd”. Si tratta di uno dei programmi di
utilità di UNIX più originali ed è presente in ogni sistema operativo di tipo UNIX (UNIX, Sun Solaris, Linux). Per creare un’immagine del CD-ROM, copiare il contenuto del CD-ROM su un file. Si può utilizzare il seguente comando:

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

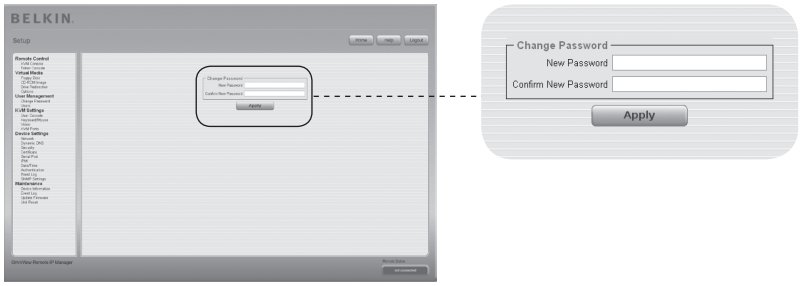
In questo caso, “dd” legge il disco intero dal dispositivo “/dev/cdrom” e salva i dati elaborati nel file di emissione specificato “/tmp/cdrom.image”. Regolare i parametri secondo le proprie esigenze (dispositivi di entrata, ecc.)

MS Windows

Per creare un file di immagine, utilizzare il proprio programma preferito di CD imaging. Copiare tutto il contenuto del disco in un solo file di immagine ISO sul disco rigido. Per esempio, con “Nero”, scegliere “Copy and Backup” e andare nella sezione “Copy Disc”. Selezionare il lettore CD-ROM o DVD dal quale si desidera creare un’immagine ISO. Specificare il nome del file dell’immagine ISO e salvare il contenuto CD-ROM nello stesso file.

P75075ea_F1DE101Hea_man.indb 42 8/16/2006 11:36:53 AM

Modifica password

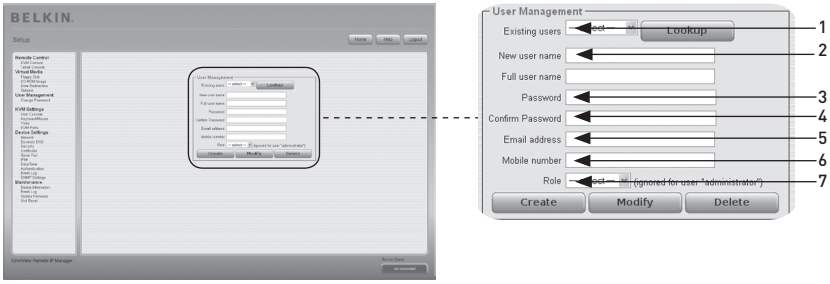


Per modificare la password, immettere la nuova password nel campo corrispondente. Ridigitare la password nel campo sottostante.

Fare clic su "Apply" per applicare le modifiche.

P75075ea_F1DE101Hea_man.indb 43 8/16/2006 11:36:53 AM

Utenti



Gestione dell'utente

L'uintà RIPM dispone di un account preconfigurato per l'amministatroe che ha un'autorizzazione permanente. Questo utente gode di tutti i diritti per poter configurare il dispositivo e usare tutte le funzioni dell'unità. Alla consegna, la password per l'account dell'amministratore è "belkin". Accertarsi di cambiare la password immediatamente dopo l'installazione o dopo la prima connessione all'unità RIPM. Riportiamo qui di seguito un elenco completo delle opzioni disponibili. Questo elenco può essere visto soltanto dall'amministratore.

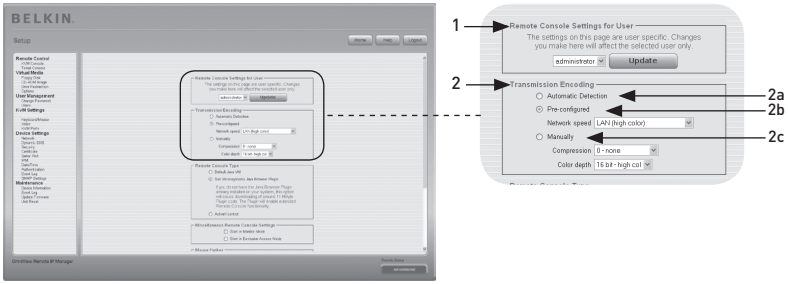
1. **Utenti registrati**
   Selezionare l'utente che si desidera modificare. Una volta selezionato un utente, fare clic sul tasto "lookup" per vedere tutte le rispettive informazioni.
2. **Nuovo nome utente**
   Il nuovo nome utente per l'account selezionato.
3. **Password**
   La passoword per il nome di login. Deve essere di almeno quattro caratteri.
4. **Conferma la password**
   Conferma della password di cui sopra.
5. **Indirizzo e-mail**
   Questo è facoltativo.
6. **Numero di telefono**
   Anche questo è facoltativo.
7. **Ruolo**
   Oltre a essere un amministratore o un utente comune, ogni utente può essere il membro di un gruppo (chiamato "ruolo"). Scegliere il ruolo che si desidera dalla casella.
   Per creare un nuovo utente, premere il tasto "Create". Il tasto "Modify" modifica le impostazioni dell'utente visualizzato. Per eliminare un utente, premere il tasto "Delete".

   Nota bene: L'unità RIPM è dotata di processore e memoria indipendenti dall'host con una limitazione in termini di istruzioni di elaborazione e spazio di memorizzazione. Per garantire un tempo di risposta accettabile, è consigliabile non collegare contemporaneamente più di 25 utenti all'unità. Lo spazio di memorizzazione disponibile sull'unità RIPM dipende dalla configurazione e dall'utilizzo dell'unità RIPM (file di registro, ecc.)

P75075ea_F1DE101Hea_man.indb 44 8/16/2006 11:36:54 AM

Console dell'utente

Qui di seguito riportiamo le impostazioni specifiche per l'utente. Ciò significa che l'amministratore può personalizzare le impostazioni per ogni singolo utente. Modificando le impostazioni di un untente non si modificano anche quelle degli altri utenti.



1. **Impostazioni della console remota per l'utente**

   Questa casella visualizza l'ID dell'utente a cui si riferiscono i valori e a cui sono state modificate le impostazioni. Selezionare l'utente desiderato dalla casella e premere il tasto "Update". In questo modo verranno visualizzate le impostazioni dell'utente indicate qui sotto.

   Nota bene: Non è consentito modificare le impostazioni di altri utenti se non si dispongono dei diritti di accesso necessari per questa operazione. Per un utente comune, non è possibile modificare le impostazioni di un altro utente senza l'autorizzazione necessaria.

2. **Codifica di trasmissione**

   L'impostazione della codifica di trasmissione consente di modificare l'algoritmo di codifica dell'immagine che trasmette dati video alla finestra della console remota. Con queste impostazioni è possibile ottimizzare la velocità dello schermo remoto in base al numero di utenti contemporaneamente connessi e alla larghezza di banda della linea di connessione (Modem, ISDN, DSL, LAN ecc.).

   2a. Rilevamento automatico

   La codifica e il livello di compressione sono determinati automaticamente dalla larghezza di banda disponibile e dal contenuto attuale dell'immagine video.

   2b. Impostazioni preconfigurate

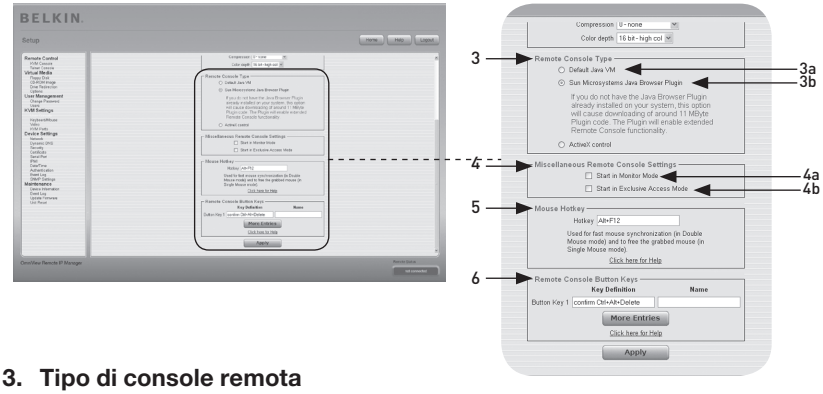
   Le impostazioni preconfigurate forniscono risultati migliori grazie alla regolazione della compressione ottimizzata e alla profondità del colore per la velocità di rete indicata.

   2c. Configurazione manuale

   Ciò consente di regolare separatamente il livello di compressione e la profondità del colore. A seconda del livello di compressione selezionato, il flusso di dati tra l'unità RIPM e la console remota verrà compresso per salvare la larghezza di banda. Dal momento in cui gli alti livelli di compressione richiedono molto tempo, non dovrebbero essere usati quando diversi utenti accedono contemporaneamente all'unità RIPM. La profondità standard del colore è di 16 bit (65536 colori). Le altre profondità di colore sono intese per le connessioni di rete più lente in modo da consentire una trasmissione di dati più rapida. Pertanto, il livello di compressione 0 (nessuna compressione)

P75075ea_F1DE101Hea_man.indb 45 8/16/2006 11:36:55 AM

utilizza solo profondità di colore da 16 bit. Con larghezza di banda inferiori, si consigliano profondità da 4 bit (16 colori) e da 2 bit (4 gamme di grigio) per interfacce desktop tipiche. Le immagini simili a fotografie ottengono risultati migliori con profondità di colore da 4 bit. La profondità di colore da 1 bit (bianco/nero) dovrebbe essere usata solo per connessioni di rete estremamente lente.



3. Tipo di console remota

Specificare il visualizzatore della console remota da utilizzare.

3a. Java Virtual Machine (JVM) di default

Questa funzione utilizza il JVM di default del browser web, o il JVM di Microsoft per Internet Explorer o il JVM di Sun.

3b. Plug-In del browser di Java su Sun Microsystems

Questo plug-in istruisce il browser web del sistema di amministrazione sulle modalità d'uso del JVM di Sun Microsystems. La JVM è presente nel browser utilizzato per lanciare il codice della finestra della console remota, che corrisponde in effetti ad un'applet Java. Se questa casella viene spuntata per la prima volta sul proprio sistema di amministrazione e se il plug-in Java non è ancora stato installato nel sistema, esso verrà scaricato ed installato automaticamente. Tuttavia, per consentire l'installazione, è comunque necessario rispondere alle varie richieste con "YES". La quantità di dati da scaricare è di circa 11 MB. Il vantaggio di scaricare la JVM Sun consiste nel poter disporre di una JVM stabile ed identica in tutte le varie piattaforme. Il software della console remota è ottimizzato per questa versione di JVM ed offre una vasta gamma di funzioni se fatto funzionare su una JVM Java.

4. Impostazioni varie della console remota

4a. Avvia in modalità monitor

Consente di selezionare il valore iniziale della modalità monitor. Per default, la modalità monitor è attivata. Attivandola, la finestra della console remota si avvia in modalità di sola lettura.

4b. Avvia in modalità di accesso esclusivo

Abilita la modalità di accesso esclusivo all'avvio della console remota. Utilizzando questa modalità, la console remota di tutti gli altri utenti si chiuderà. Nessun altro utente potrà aprire la console remota simultaneamente fin quando non si disabiliterà l'opzione o ci si scollegherà.

5. Tasti di scelta rapida del mouse

I tasti di scelta rapida del mouse consentono di specificare una combinazione di tasti per avviare il processo di sincronizzazione del mouse (immettendo la combinazione sulla console remota) o di lasciare inalterata la modalità di mouse singolo.

P75075ea_F1DE101Hea_man.indb 46 8/16/2006 11:36:56 AM

6. Tasti di comando della console remota

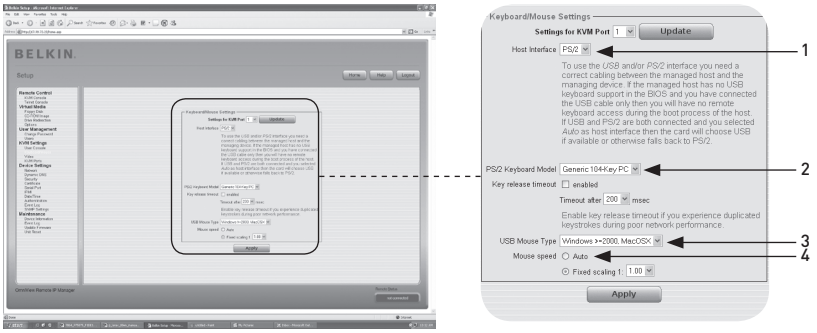
Consentono di simulare le battute di tasti sul sistema remoto che non possono essere effettuate localmente. Questo potrebbe essere necessario se manca un tasto o se il sistema operativo locale della console remota sta ricevendo incondizionatamente una battuta. Gli esempi più comuni sono “Control+Alt+Delete” su Windows e DOS, che sono sempre riconosciuti o la sequenza di tasti “Control+Backspace” su Linux, che può essere utilizzata per terminare il server X. Per definire o modificare una sequenza di tasti, leggere le istruzioni che descrivono l’impostazione di un comando. In generale, la sintassi per un comando è la seguente:

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

Il termine tra parentesi è opzionale. L’asterisco indica che occorre aggiungere tanti altri comandi quanti ne richiede il vostro caso. Il termine “confirm” aggiunge un dialogo di conferma visualizzato prima che le battute possano essere inviate all’host remoto. Con “keycode” si intende il comando da inviare. Diversi codici possono essere concatenati con un segno + o -. Il segno + consente combinare in sequenza i tasti, tutti i tasti saranno premuti fino a quando si troverà un segno – alla fine della combinazione. In questo caso, tutti i tasti premuti saranno lasciati nella sequenza inversa. Quindi, il segno - serve a premere e rilasciare separatamente i tasti. Il segno < rilascia soltanto l’ultimo comando. L’asterisco inserisce una pausa della durata di 100 millisecondi. Per esempio, la combinazione dei tasti Ctrl, Alt e F2 è rappresentata dalla sequenza “Ctrl+Alt+F2”.

P75075ea_F1DE101Hea_man.indb 47 8/16/2006 11:36:56 AM

Tastiera/Mouse



1. **Interfaccia host**
   L'interfaccia host abilita l'interfaccia alla quale il mouse è collegato. Si può scegliere "Auto" per un rilevamento automatico, "USB" per un mouse USB o "PS/2" per un mouse PS/2.

   Nota bene: per utilizzare l'interfaccia USB, occorre collegare l'host controllato e l'unità di gestione con i cavi appropriati. Per esempio, se nel BIOS dell'host controllato non vi è un supporto per tastiera USB e si è collegato soltanto il cavo USB, non si potrà accedere alla tastiera remota durante il processo di accensione dell'host. Se USB e PS/2 sono entrambi connessi e si seleziona "Auto" come interfaccia host, USB verrà selezionato all'avvio, se disponibile. Se USB non è disponibile, "PS/2" verrà selezionato.

   Per ottenere l'accesso alla tastiera remota USB durante il processo di accensione dell'host, occorre soddisfare le seguenti condizioni:

   - il BIOS dell'host deve avere un supporto per tastiera USB
   - il cavo USB deve essere collegato o selezionato nell'opzione "Host Interface"

2. **Modello di tastiera PS/2**
   Consente di scegliere il layout di una tastiera tra "Generic 101-Key PC" per un layout standard, "Generic 104-Key PC" per un layout standard con l'aggiunta di tre tasti Windows, "Generic 106-Key PC" per una tastiera giapponese e "Apple Macintosh" per una tastiera Macintosh®. Se si desidera interrompere la tastiera, selezionare l'opzione appropriata e inserire il valore di tempo desiderato nel campo corrispondente.

3. **Tipo di mouse USB**
   Abilita il tipo di mouse USB. Scegliere l'opzione appropriata dalla casella. Per una descrizione dettagliata del tipo di mouse e le opzioni consigliate per i diversi sistemi operativi, leggere la sezione "Impostazioni consigliate del mouse" a pagina 21 di questo manuale d'uso.*

*Questo funzione è compatibile soltanto col sistema operativo Windows.

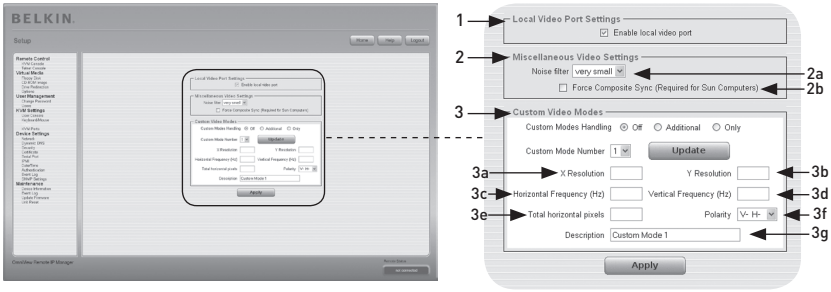
P75075ea_F1DE101Hea_man.indb 48 8/16/2006 11:36:57 AM

4. **Velocità del mouse**
   - **Rilevazione automatica della velocità del mouse**
     Utilizzare questa opzione se le impostazioni del mouse sull'host utilizzano un'ulteriore accelerazione. L'unità RIPM rileva l'accelerazione e la velocità del mouse durante il processo di sincronizzazione del mouse.
   - **Rilevazione della velocità del mouse fisso**
     Utilizzare questa opzione per una trasmissione diretta degli spostamenti del mouse tra il cursore del mouse locale e di quello remoto. Occorre impostare una graduazione fissa che determina di quanto si sposta il cursore del mouse remoto quando il cursore del mouse locale si sposta di un pixel. Questa opzione funziona soltanto quando le impostazioni del mouse sull'host sono lineari, ovvero quando non vi è alcuna accelerazione del mouse.

   Per impostare le opzioni, fare clic sul tasto "Apply".

P75075ea_F1DE101Hea_man.indb 49 8/16/2006 11:36:57 AM

Video



Per impostare le opzioni (vedi sotto), fare clic sul tasto “Apply”.

1. **Impostazioni della porta video locale**

   Abilita porta video locale

   Questa opzione monitora l’uscita video locale dell’unità e indica se è attiva e se sta trasmettendo il segnale in entrata dal sistema host.

2. **Impostazioni video varie**

   2a. Filtro rumori

   Questa opzione definisce la modalità di reazione dell’unità alle piccole modifiche al segnale video in entrata. L’impostazione di un filtro di grandi dimensioni necessita un minor traffico di rete e assicurerà una visualizzazione in video più rapida, sebbene i cambiamenti più piccoli in alcune zone potrebbero non essere riconosciuti. Un filtro di piccole dimensioni visualizza istantaneamente tutti i cambiamenti, ma, anche se il contenuto dello schermo, in realtà, non sta cambiando potrebbe causare una crescita costante del traffico di rete (a seconda della qualità del segnale video in entrata).

   2b. Forza sincronizzazione composita (per computer Sun)

   Per supportare la trasmissione dei segnali da una macchina Sun, abilitare questa opzione. Se questa funzione non è abilitata, l’immagine della console remota non sarà visibile.

3. **Modalità video personalizzate**

   Il numero massimo di risoluzioni video personalizzabili è quattro.

   L’opzione “Custom Modes Handling” consente di disabilitare le modalità personalizzate (“Off”) o di impostare risoluzioni video standard o esclusive (“Only”). L’ultima opzione (“Additional”) consente di forzare una modalità video speciale pe l’unità RIPM. Per modificare i parametri per la modalità video personalizzata, scegliere il numero appropriato dalla casella e premere il tasto “Update”. Vi sarà richiesto di fornire alcune informazioni in modo che la modalità video possa essere riconosciuta in modo corretto:

   Avvertenza: L’opzione “Host Monitor Settings” è soltanto per utenti esperti. Un uso scorretto di questa opzione può danneggiare la trasmissione dei segnali video. Accertarsi di aver compreso a fondo questa funzione prima di cercare di modificare le impostazioni del monitor dell’host.

P75075ea_F1DE101Hea_man.indb 50 8/16/2006 11:36:58 AM

3a. Risoluzione X
Si riferisce al numero visibile di pixel orizzontali.

3b. Risoluzione X
Si riferisce al numero visibile di pixel verticali.

3c. Frequenza orizzontale (Hz)
Si riferisce alla frequenza (di linea) orizzontale espressa in hertz.

3d. Frequenza verticale (Hz)
Si riferisce alla frequenza verticale espressa in hertz.

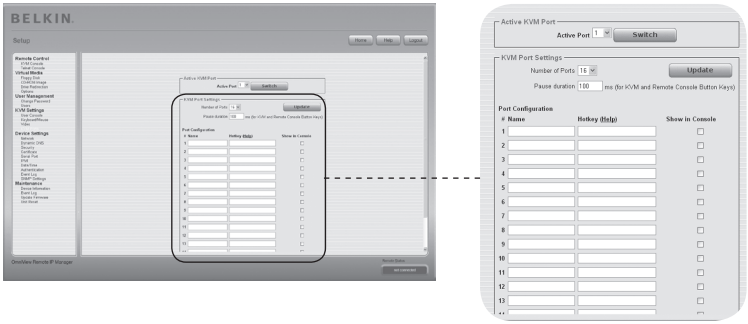
3e. Pixel orizzontali totali
Si riferisce al numero totale di pixel per linea, tra cui le zone vuote e quelle non visibili.

3f. Polarità
Si riferisce alla caratteristica positiva o negativa dei signali di sincronizzazione. V indica la polarità verticale; H indica la polarità orizzontale.

3g. Descrizione
Qui è possibile assegnare un nome alla modalità, che viene visualizzato nella console remota se la modalità personalizzata è attiva.

Porte KVM

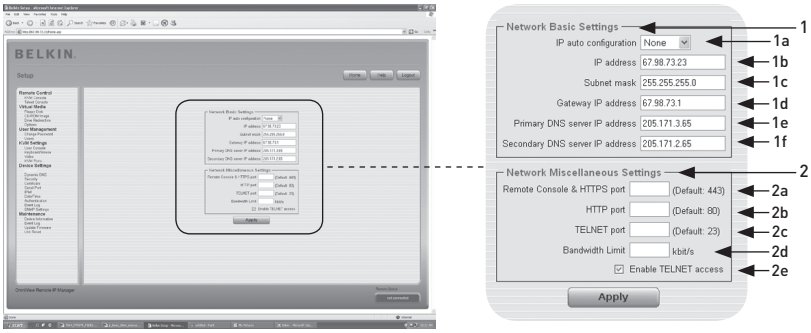
È possibile selezionare il numero di porte utilizzate dallo switch KVM collegato e si può assegnare un nome ad ogni porta. Per mettere a disposizione le funzioni di commutazione della porta KVM attraverso l'unità RIPM, è necessario stabilire le combinazioni di tasti per le varie porte.



P75075ea_F1DE101Hea_man.indb 51 8/16/2006 11:36:58 AM

Rete

Il pannello delle impostazioni di rete raffigurato qui sotto (Network Settings) consente di modificare i parametri relativi alla rete. Una volta applicate, le nuove impostazioni di rete entrano immediatamente in funzione.



Avvertenza: La modifica delle impostazioni di rete dell'unità RIPM potrebbe causare la perdita della connessione di rete. Se queste impostazioni vengono modificate a distanza, accertarsi che i valori siano corretti e di poter ancora accedere all'unità RIPM.)

1. **Impostazioni di base**

   1a. Configurazione automatica dell'IP
   Con questa opzione è possibile definire il percorso dal quale l'unità rileva le proprie impostazioni di rete (o un server BOOTP o DHCP). per il DHCP, selezionare "DHCP"; per il BOOTP, selezionare "bootp". Scegliendo "none" (nessuno), si disabilita la configurazione automatica dell'IP.

   1b. L'indirizzo IP è assegnato dal proprio amministratore di rete.

   1c. Il termine **"Subnet Mask"** si riferisce all'indirizzo della rete locale, utilizzato per determinare la sottorete alla quale appartiene un indirizzo IP.

   1d. Indirizzo IP del gateway
   Se l'unità RIPM deve essere accessibile da altri reti diverse da quella locale, impostare questo indirizzo IP sui valori dell'indirizzo IP del router della rete locale.

   1e. Indirizzo IP del server DNS primario
   Questo è dell'indirizzo IP del server DNS primario in formato punteggiato. Questa opzione si può lasciare in bianco; tuttavia, in questo caso, l'unità non sarà in grado di eseguire la risoluzione del nome.

   1f. Indirizzo IP del server DNS secondario
   Questo è l'indirizzo IP del server DNS secondario in formato punteggiato. Sarà utilizzato nel caso in cui il server DNS primario non non può essere contattato.

P75075ea_F1DE101Hea_man.indb 52 8/16/2006 11:36:59 AM

2. Impostazioni di rete varie

2a. Porta per HTTPS e console remota
Si tratta dell'indirizzo della porta dalla quale il server della console remota e il server HTTPS ricevono informazioni. Se lasciata inutilizzata o aperta, viene utilizzato il valore standard.

2b. Porta HTTP
Si tratta dell'indirizzo della porta da cui il server HTTP dell'unità riceve informazioni. Se lasciata inutilizzata o aperta, viene utilizzato il valore standard.

2c. Porta Telnet
Si tratta dell'indirizzo della porta da cui il server Telnet dell'unità riceve informazioni. Se lasciata inutilizzata o aperta, viene utilizzato il valore standard.

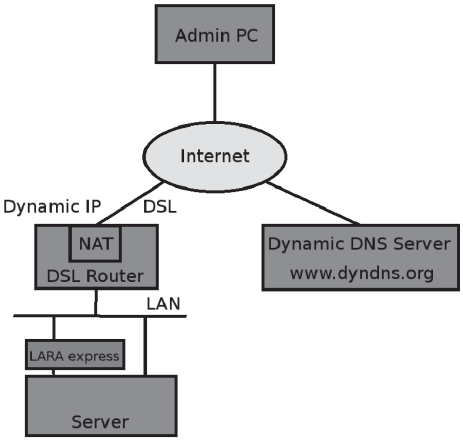
2d. Limite della larghezza di banda
Questa opzione si riferisce al traffico di rete massimo generato attraverso il dispositivo di rete Ethernet (espresso in Kbps).

2e. Abilita l'accesso Telnet
Impostare questa opzione in modo da consentire all'utente di accedere all'unità utilizzando il gateway Telnet (leggere la sezione "Console Telnet" a pagina 32).

P75075ea_F1DE101Hea_man.indb 53 8/16/2006 11:36:59 AM

DNS dinamico

È possibile utilizzare un servizio gratuito di DNS dinamico (dyndns.org) nel seguente contesto:



Contesto di DNS dinamico

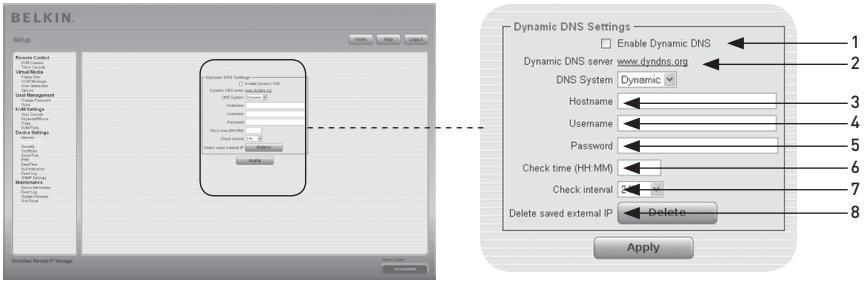
È possibile accedere all'unità RIPM attraverso l'indirizzo IP del router DSL, che è assegnato dinamicamente dal provider. Dal momento in cui l'amministratore non conosce l'indirizzo IP assegnato dal provider, l'unità si collega a un DNS dinamico speciale a intervalli regolari e registra qui il proprio indirizzo IP. L'amministratore può contattare questo server e rilevare lo stesso indirizzo IP appartenente alla scheda di rete. L'amministratore deve registrare l'unità RIPM per usare il servizio con il DNS dinamico e assegnarvi un nome host specifico. Il nome utente e la password saranno assegnati durante il processo di registrazione. Queste informazioni di account e il nome dell'host servono per determinare l'indirizzo IP dell'unità RIPM registrata.

Occorre eseguire le seguenti operazioni per abilitare il DNS dinamico:

- Verificare che l'interfaccia LAN dell'unità sia configurata in modo corretto.
- Inserire i parametri di configurazione delle impostazioni di DNS dinamico indicati a pagina 55.

P75075ea_F1DE101Hea_man.indb 54 8/16/2006 11:37:00 AM

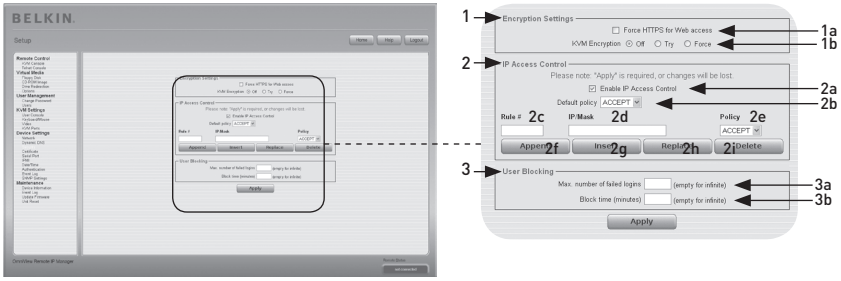
Impostazioni del DNS dinamico



1. **Abilita DNS dinamico**
   Questo abilita il servizio di DNS dinamico. Ciò richiede un indirizzo IP per il server DNS configurato.
2. **Server DNS dinamico**
   L'unità RIPM si registra a intervalli regolari in questo percorso. Al momento dell'immissione in commercio, il DNS dinamico è un'impostazione fissa dal momento in cui soltanto dyndns.org è supportato.
3. **Nome dell'host**
   RIPM è il nome dell'host fornito dal DNS dinamico. Utilizzare il nome interno, ad es., "testserver.dyndns.org" (o "RIPM.dyndns.org"), e non soltanto il nome effettivo dell'host.
4. **Nome utente**
   Durante la registrazione manuale con il DNS dinamico, occorre registrare questo nome utente.
   Nota bene: Il nome utente non deve contenere spazi.
5. **Password**
   Durante la registrazione manuale con il DNS dinamico, occorre registrare questa password.
6. **Verifica ora**
   La scheda RIPM si registra nel DNS dinamico sotto "Check Time".
7. **Verifica intervallo**
   Questo è l'intervallo di riferimento per comunicare con il DNS dinamico dall'unità RIPM.
   Nota bene: L'unità RIPM dispone di un proprio orologio in tempo reale indipendente. Verificare con attenzione che l'impostazione dell'orologio dell'unità sia corretta.
8. Utilizzare l'opzione **"Delete saved external IP"** se si desidera aggiornare l'indirizzo IP salvato esternamente. Per eliminare l'indirizzo salvato, premere il tasto "Delete".

P75075ea_F1DE101Hea_man.indb 55 8/16/2006 11:37:01 AM

Protezione



1. **Impostazioni della crittografia**

   1a. Obbliga HTTPS

   Se questa opzione è attiva, l'accesso al Web è possibile soltanto utilizzando una connessione di tipo HTTPS. L'unità RIPM non "reagirà" alle informazioni proveniente dalla porta HTTP per le connessioni in entrata. In caso si desideri creare un proprio certificato SSL per identificare l'unità, leggere la sezione "Certificato" a pagina 58.

   1b. Crittografia KVM

   Questa opzione controlla la crittografia del protocollo Remote Frame Buffer (RFB). La console remota utilizza utilizza l'RFB per trasmettere dati dello schermo alla macchina dell'amministratore e i dati della tastiera e del mouse all'host. Impostandola su "Off", non si userà alcuna crittografia. Impostandola su "Try", l'applet tenta di effettuare una connessione crittografata. Se non è possibile stabilire una connessione, si utilizzerà una connessione non crittografata. Impostandola su "Force", l'applet tenta di effettuare una connessione crittografata. Se la connessione fallisce, il sistema genera un rapporto di errore.

2. **Controllo di accesso all'IP**

   Questa sezione spiega le impostazioni associate al controllo di accesso all'IP. È utilizzato per limitare l'accesso a una serie di determinati client. Questi client saranno identificati dagli indirizzi IP dai quali stanno tentando di effettuare delle connessioni.

   Avvertenza: Le impostazioni del controllo di accesso all'IP vengono applicate soltanto all'interfaccia LAN.

   2a. Abilita controllo di accesso all'IP

   Abilita il controllo di accesso basato sugli indirizzi IP di origine.

   2b. Default Policy

   Questa opzione controlla i pacchetti IP in entrata che non soddisfano nessuna delle regole configurate. Possono essere accettati o respinti.

   Avvertenza: se si imposta questa funzione su "DROP" (Respingi) o se non sono state impostate le regole per "ACCEPT" (Accetta), l'accesso al web tramite la rete LAN viene disabilitato. Per riabilitare l'accesso è possibile modificare le impostazioni di protezione tramite il modem o disabilitando temporaneamente il controllo di accesso all'IP con la procedura di configurazione iniziale.

   2c. Numero della regola

   Deve contenere il numero di una regola per la quale siano validi i seguenti comandi. Questo campo viene ignorato nel caso si aggiunga una nuova regola.

P75075ea_F1DE101Hea_man.indb 56 8/16/2006 11:37:01 AM

2d. IP/Mask
Specifica l'indirizzo IP o la gamma di indirizzi IP per il quali è valida la regola in questione. Nei seguenti esempi, il numero concatenato ad un indirizzo IP con '/' corrisponde al numero di bit validi che saranno utilizzati per l'indirizzo IP dato).

192.168.1.22/32 corrisponde all'indirizzo IP 192.168.1.22

192.168.1.0/24 corrisponde ai pacchetti IP con gli indirizzi di origine compresi tra 192.168.1.0 e 192.168.1.255

0.0.0.0/0 corrisponde a qualsiasi pacchetto IP

2e. Policy
La policy determina cosa occorre fare con i pacchetti corrispondenti. Possono essere accettati o respinti.

Avvertenza: L'ordine delle regole è importante. Le regole sono controllate in ordine ascendente affinché si trova una corrispondenza. Tutte le regole al di sotto di quella corrispondente saranno ignorate. La default policy sarà applicata se non si trovano corrispondenze.

2f. Aggiunta di una regola
Inserire l'IP/mask e impostare la policy. Quindi premere il tasto "Append".

2g. Immissione di una regola
Inserire il numero della regola e l'IP/mask. Impostare la policy. Quindi premere il tasto "Insert".

2h. Sostituzione di una regola
Inserire il numero della regola e l'IP/mask. Impostare la policy. Quindi premere il tasto "Replace".

2i. Eliminazione di una regola
Inserire il numero della regola e premere il tasto "Delete".

3. Blocco utente
Il meccanismo di blocco utente consente all'amministratore di disabilitare il collegamento di un determinato utente nel caso in cui la password venga digitata in modo errato per diverse volte. La durata del blocco è configurabile.

3a. Numero massimo di login falliti
Inserire il numero massimo di tentativi di collegamento falliti dopo i quali un utente dovrebbe essere bloccato. Lasciare vuoto questo campo per disabilitare la funzione di blocco utente.

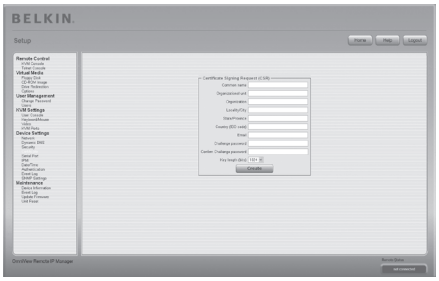
3b. Durata del blocco
La quantità di minuti durante i quali l'utente viene bloccato dopo aver inserito per troppe volte una password errata. Lasciare vuoto questo campo per bloccare l'utente finché non sarà sbloccato manualmente.

Sblocco utenti
Esistono due possibilità per sbloccare un utente bloccato:

- Un utente principale può accedere alle impostazioni di gestione dell'utente (leggere la sezione "Gestione dell'utente") e premere il tasto "Unblock".
- Un amministratore può utilizzare la console seriale per la configurazione iniziale e collegarsi come utente "bloccato". L'unità RIPM richiederà la password dell'amministratore e fornirà un elenco di utenti bloccati che possono essere sbloccati.

P75075ea_F1DE101Hea_man.indb 57 8/16/2006 11:37:01 AM

Certificato



Impostazioni del certificato

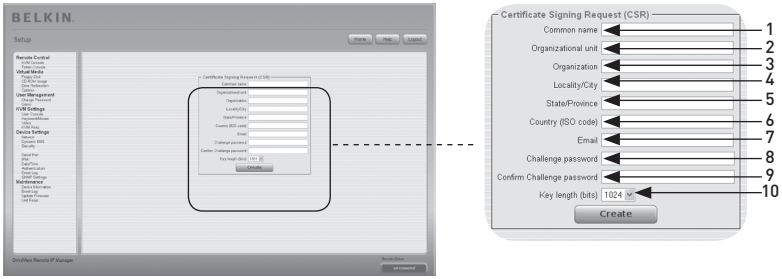
L'unità RIPM utilizza il protocollo SSL per qualsiasi tipo di traffico crittografato con il client collegato. Durante l'impostazione della connessione, l'unità RIPM deve esporre la propria identità ad un client utilizzando un certificato crittografico. Alla consegna, questo certificato e la chiave segreta sottostante saranno uguali per tutte le unità RIPM prodotte e non corrisponderanno con la configurazione di rete che sarà applicata all'unità RIPM dal proprio utente. La chiave segrate del certificato è utilizzata anche per la protezione dello scambio di informazioni tramite il protocollo PPP È possibile produrre e installare un nuovo certificato base64 x.509 che sia unico per una determinata unità RIPM. Per farlo, l'unità RIPM è in grado di generare un nuovo codice di criptazione e la Richiesta Sottoscrizione del Certificato che deve essere certificata da un'apposita autorità. Un'autorità di certificazione ha il compito di accertare l'identità dell'utente, oltre a sottoscrivere per questo ed emettere un certificato SSL. Per produrre e installare un certificato SSL per l'unità, fare quanto segue:

- Creare una richiesta di SSL utilizzando il pannello mostrato nella figura sottostante. Occorre
  compilare una serie di campi, ognuno dei quali è descritto qui sotto.
  Una volta fatto questo, fare clic sul tasto "Create" per inizializzare la creazione della richiesta. La richiesta può essere scaricata sulla macchina dell'amministrazione con il tasto
  "Download CSR".
- Inviare la richiesta salvata ad un'autorità per la certificazione. L'utente riceverà un nuovo certificato dall'autorità incaricata.
- Trasferire il certificato all'unità utilizzando il tasto "Create".

Dopo aver completato queste tre operazioni, l'unità disporrà del proprio certificato che identificherà la scheda sui propri client.

Avvertenza: Nel caso la richiesta venisse distrutta sull'unità RIPM, non esiste modo per ripristinarla! Se la si dovesse cancellare per sbaglio, eseguire di nuovo le tre operazioni.

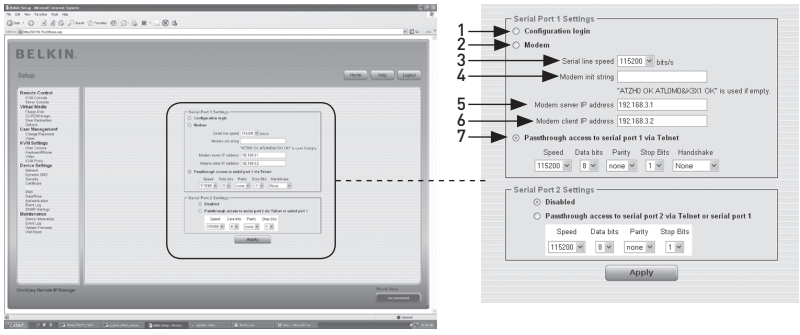
P75075ea_F1DE101Hea_man.indb 58 8/16/2006 11:37:02 AM



1. **Nome comune**
   Si tratta del nome di rete dell'unità RIPM una volta installata nella rete dell'utente (solitamente il nome di dominio completamente autorizzato). È identico al nome che è
   utilizzato per accedere all'unità RIPM con un browser web ma senza prefisso "http://". Se si accede all'unità utilizzando HTTPS, e il nome qui indicato e il nome effettivo della rete sono differenti, il browser visualizzerà un messaggio
   di avvertimento.
2. **Unità organizzativa**
   Questo campo specifica a quale reparto dell'azienda appartiene l'unità RIPM.
3. **Organizzazione**
   Il nome dell'organizzazione aziendale cui appartiene l'unità RIPM.
4. **Località/Città**
   La città in cui è ubicata la struttura organizzativa.
5. **Regione/Provincia**
   La regione o la provincia in cui è ubicata la struttura organizzativa.
6. **Nazione (codice ISO)**
   La nazione all'interno della quale si trova la struttura organizzativa (un codice ISO di due lettere).
7. **Challenge Password**
   Alcune autorità di certificazione richiedono una cosiddetta "Challenge Password", una password specifica per autorizzare eventuali variazioni successive del certificato (per es. revoca di un certificato). La lunghezza minima di questa password è di quattro caratteri.
8. **Conferma Challenge Password**
   Richiede di ridigitare la challenge password.
9. **Email**
   Si riferisce all'indirizzo e-mail di una persona di contatto responsabile per l'unità RIPM e la sua protezione.
10. **Lunghezza della chiave**
    Si tratta della lunghezza del codice generato in bit. Nella maggior parte dei casi, 1024 bit sono sufficienti. Eventuali codici più lunghi possono comportare un intervallo di risposta più lento dell'unità RIPM durante l'impostazione della connessione.

P75075ea_F1DE101Hea_man.indb 59 8/16/2006 11:37:03 AM

Porta seriale



Le impostazioni seriali dell'unità RIPM consentono di specificare quali periferiche sono collegate alla porta seriale e come utilizzarle. Per accedere all'unità RIPM tramite l'interfaccia seriale, è necessario usare un cavo null modem.

1. **Configurazione o collegamento alla console**
   Non usare la porta seriale per le funzioni speciali; usarla solo per la configurazione iniziale.
2. **Modem**
   L'unità RIPM prevede la possibilità di accesso a distanza utilizzando una linea telefonica in aggiunta all'accesso standard attraverso la scheda di rete Ethernet integrata. Il modem deve essere collegato all'interfaccia seriale dell'unità RIPM. Logicamente, collegare l'unità RIPM utilizzando il telefono non significa altro che impostare una connessione dedicata punto-a –punto dal computer con funzioni RIPM all'unità RIPM. In altre parole, l'unità RIPM funge da provider di servizi Internet con il quale è possibile collegarsi. La connessione viene impostata utilizzando il protocollo Point-to-Point (PPP). Prima di collegare l'unità RIPM, accertarsi di configurare il proprio computer RIPM come necessario. Per esempio; per i sistemi operativi Windows, è possibile collegare una connessione di accesso remoto che abbia di default le giuste impostazioni come PPP. Il pannello delle impostazioni del modem consente di configurare l'accesso remoto all'unità RIPM usando un modem. Qui di seguito riportiamo la descrizione di ogni parametro. Le impostazioni del modem fanno parte del pannello delle impostazioni seriali.
3. **Velocità di linea seriale**
   La velocità alla quale l'unità sta comunicando con il modem. La maggior parte dei modem in commercio supporta il valore standard di 115,200 bps. Se si utilizza un modem vecchio o nel caso si dovessero verificare dei problemi, cercare di ridurre questa velocità.
4. **Stringa di inizializzazione del modem**
   La stringa di inizializzazione viene utilizzata dall'unità RIPC per inizializzare il modem. Il valore predefinito funzionerà per tutti i modem standard collegati direttamente ad una linea telefonica. Se si possiede un modem speciale o se il modem è collegato ad uno switch telefonico locale che richiede una speciale sequenza di digitazione per stabilire la connessione con la rete pubblica, queste impostazioni possono essere modificate assegnando una nuova stringa. Per quanto riguarda la sintassi dei comandi AT, vedere il manuale del modem.

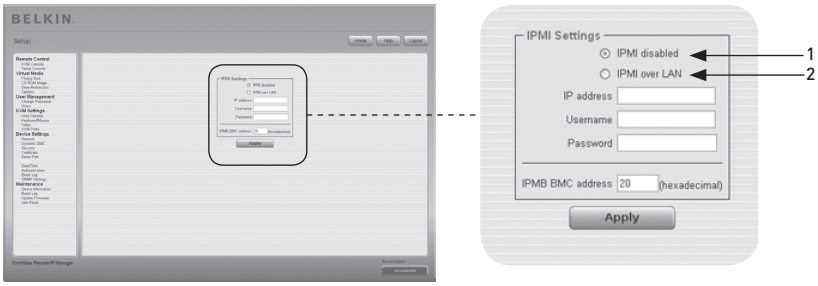
P75075ea_F1DE101Hea_man.indb 60 8/16/2006 11:37:03 AM

5. **Indirizzo IP server del modem**
   L'indirizzo IP viene assegnato all'unità RIPM durante lo scambio di informazioni tramite il protocollo PPP. Poiché si tratta di una connessione IP point-to-point, è consentito indicare praticamente qualsiasi indirizzo IP, ma è necessario accertarsi che questo non interferisca con le impostazioni IP dell'unità RIPM e del computer RIPM. Il valore predefinito funziona nella maggior parte dei casi.
6. **Indirizzo IP client del modem**
   L'indirizzo IP viene assegnato al computer RIPM durante lo scambio di informazioni tramite il protocollo PPP. Poiché si tratta di una connessione IP point-to-point, è consentito indicare praticamente qualsiasi indirizzo IP, ma è necessario accertarsi che questo non interferisca con le impostazioni IP dell'unità RIPM e del computer RIPM. Il valore predefinito funziona nella maggior parte dei casi.
7. **Accesso di transito alla porta seriale via Telnet**
   Con questa opzione è possibile collegare qualsiasi periferica alla porta seriale ed accedere ad essa (a condizione che preveda un supporto terminale) via Telnet. Selezionare le opzioni adatte per la porta seriale ed utilizzare l'unità Telnet o un client standard Telnet per collegarsi all'unità RIPM. Per maggiori informazioni sull'interfaccia Telnet, leggere la sezione "Console Telnet".

   Nota bene: Su www.belkin.com è possibile trovare un elenco di tutti i modem compatibili.

P75075ea_F1DE101Hea_man.indb 61 8/16/2006 11:37:04 AM

Interfaccia per la gestione intelligente della piattaforma (IPMI)



L'IPMI dell'unità RIPM offre un ulteriore modo per attivare o disattivare il sistema e per eseguire resettaggi rapidi. Inoltre, queste funzioni consentono di visualizzare un registro di eventi del sistema host e lo stato di alcuni sensori di sistema (ad es., la temperatura). Se il sistema host supporta l'IPMI, si può accedere al sistema in uno dei seguenti modi:

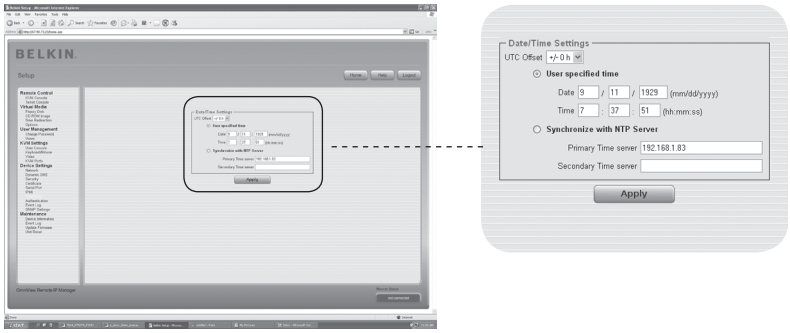
- IPMI su LAN (IPMI v1.5 è richiesto)
- Impostazioni dell'IPMI

La figura qui sopra mostra il pannello delle impostazioni dell'IPMI. Le opzioni sono descritte sotto.

1. **IPMI disabilitata**
   Disabilita l'IPMI sull'unità RIPM. Questo significa che lo stato e il registro eventi non sono disponibili dall'IPMI; che le funzioni di accensione/spegnimento e di resettaggio non usano l'IPMI ma l'ATX (Advanced Technology Extended) e che il cavo di reset è collegato dall'unità RIPM alla scheda madre.
2. **IPMI su LAN**
   L'IPMI si può anche collegare su una connessione LAN. Il prerequisito per questo tipo di accesso è un sistema host con IPMI v1.5 e un adattatore di rete con una connessione di banda laterale al controller di gestione della scheda madre (BMC). Nelle impostazioni dell'IPMI, occorre inserire l'indirizzo IP del sistema host e la password corretta per la connessione LAN. Si può anche accedere agli altri sistemi IPMI inserendo i rispettivi indirizzi IP.

P75075ea_F1DE101Hea_man.indb 62 8/16/2006 11:37:04 AM

Data e ora

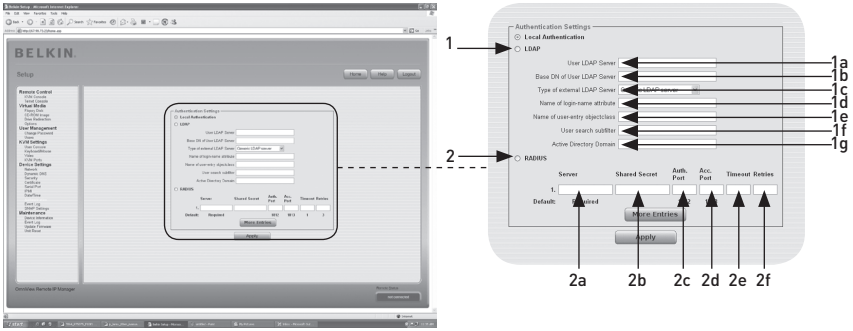


Questo link si riferisce a una pagina dove è possibile impostare l'orologio in tempo reale interno dell'unità. È possibile modificare manualmente l'orologio o usare il server di sincronizzazione dell'ora NTP. Senza un server di sincronizzazione dell'ora, l'impostazione dell'ora non sarà costante e sarà necessario modificarla ogni volta che l'unità non è alimentata per più qualche minuto. Per evitare che ciò accada, si può utilizzare il server di sincronizzazione NTP che imposta automaticamente l'orologio interno sui valori dell'ora di Greenwich. Siccome il server NTP è sempre impostato sull'ora di Greenwich, si può impostare uno scostamento statico per avere l'ora locale.

Avvertenza: Al momento non c'é nessun modo per impostare automaticamente l'ora legare. Occorre impostare lo scostamento dell'ora di Greenwich due volte l'anno a seconda delle norme locali.

P75075ea_F1DE101Hea_man.indb 63 8/16/2006 11:37:05 AM

Autenticazione



L'unità RIPM consente di utilizzare un'autenticazione locale o di conservare le informazioni in un protocollo LDAP (Lightweight Directory Access Protocol) o in un server RADIUS (Remote Authentication Dial-In User Service). Per il LDAP o il RADIUS, occorre specificare alcune informazioni nel pannello delle impostazioni dell'autenticazione. Per maggiori informazioni sulle impostazioni LDAP e RADIUS, leggere qui sotto.

1. LDAP

1a. Server LDAP dell'utente
Inserire il nome o l'indirizzo IP del server LDAP contenente tutte le voci dell'utente. Se si sceglie un nome al posto di un indirizzo IP, occorre configurare un server DNS nelle impostazioni di rete.

1b. Base DN del server LDAP dell'utente
Specificare il nome determinato dove l'albero della directory si avvia nel server LDAP dell'utente.

1c. Tipo di server LDAP esterno
Imposta il tipo di server LDAP esterno. Questo è necessario perché alcuni tipi di server richiedono una gestione speciale. Inoltre, i valori predefiniti dello schema LDAP sono impostati in modo appropriato. È possibile scegliere tra un server LDAP generico, un Novell Directory Service una Microsoft Active Directory. Se non si dispone né di un Novell Directory Service né di una Microsoft Active Directory, scegliere un server LDAP generico e modificare lo schema LDAP (vedi sotto).

1d. Nome dell'attributo del nome di login
Si tratta del nome dell'attributo contenente l'unico nome di login di un utente. Per usare i valori predefiniti, lasciare vuoto questo campo. I valori predefiniti dipendono dal tipo di server LDAP selezionato.

1e. Nome della categoria di oggetti
Si tratta della categoraia di oggetti che identifica un utente nella directory LDAP. Per usare i valori predefiniti, lasciare vuoto questo campo. I valori predefiniti dipendono dal tipo di server LDAP selezionato.

P75075ea_F1DE101Hea_man.indb 64 8/16/2006 11:37:05 AM

1f. Filtro secondario di ricerca utente
Consente di effettuare una ricerca avanzata per utenti che dovrebbe essere riconosciuti dall'unità.

1g. Dominio della directory attiva
Questa opzione rappresenta il dominio della directory attiva che viene configurato nel server della Microsoft Active Directory. Questa opzione è valida soltanto se si è scelta una Microsoft Active Directory come tipo di server LDAP.

2. Remote Authentication Dial In User Service (RADIUS)
RADIUS è un protocollo specificato dall'organizzazione mondiale di esperti IETF. Esistono due specifiche che compongono il protocollo RADIUS: autenticazione e accounting. Queste specifiche intendono centralizzare l'autenticazione, la configurazoine e l'accounting per i servizi di collegamento a un server indipendenti. Esistono diverse implementazioni del protocollo RADIUS: FreeRADIUS, OpenRADIUS o RADIUS su sistemi UNIX. Il protocollo RADIUS ha superato ogni test ed è conforme a tutte le specifiche. Possiamo raccomandare tutti i prodotti sotto elencati, soprattutto l'implementazione di FreeRADIUS.

Nota bene: attualmente non supportiamo opzioni di convalida/risposta. Una risposta "Access Challenge" è vista e considerata come "Access Reject".

Per accedere a un dispositivo remoto usando il protocollo RADIUS, occorre collegarsi. Sarà necessario specificare il nome utente e la password. Il server RADIUS leggerà i dati immessi (Autenticazione) e l'unità ricercherà il vostro profilo (Autorizzazione). Il profilo definisce (o limita) le vostre azioni e potrebbe differire a seconda della situazione. Se non si trova tale profilo, l'accesso via RADIUS sarà rifiutato. In qualità di meccanismo di attività remota, il login via RADIUS funziona come la console remota. Se non si registra alcuna attività per più di trenta minuti, la connessione all'unità sarà interrotta e chiusa.

2a. Server
Inserire l'indirizzo IP o il nome dell'host del server RADIUS da collegare. Se si sta usando il nome dell'host, il DNS deve essere configurato e abilitato.

2b. Chiave simmetrica
Una chiave simmetrica (detta anche shared secret) è una stringa di testo che funge da password tra il client RADIUS e il server RADIUS. L'unità RIPM funge da client RADIUS. Una chiave simmetrica viene utilizzata per verificare che i messaggi di RADIUS siano inviati da un dispositivo compatibile con RADIUS configurato con la stessa chiave simmetrica. Per la chiave simmetrica, si può utilizzare ogni tipo di carattere alfanumerico e speciale. Una chiave simmetrica può consistere di 128 caratteri e contenere lettere maiuscole e minuscole, numeri e altri simboli (caratteri non definiti come lettere o numeri), come punti esclamativi o asterischi.

2c. Porta di autenticazione
La porta con cui comunica il server RADIUS per le richieste di autenticazione. Il valore predefinito è #1812.

P75075ea_F1DE101Hea_man.indb 65 8/16/2006 11:37:06 AM

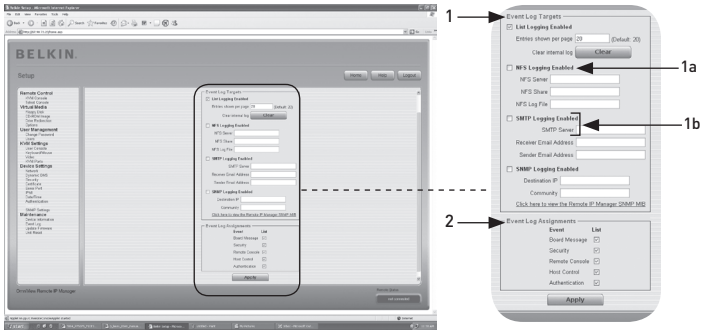
2d. Porta di accounting
La porta con cui comunica il server RADIUS per le richieste di accounting. Il valore predefinito è #1813.

2e. Timeout
Imposta il tempo di vita del pacchetto o time-to-live (in secondi). Il time-to-live indica il tempo di attesa per il completamento della richiesta. Se la richiesta non è completata all'interno di questo intervallo di tempo, sarà cancellata. Il valore predefinito è di un secondo.

2f. Tentativi
Impostare il numero di tentativi se una richiesta non può essere completata. Il valore predefinito è di tre tentativi.

P75075ea_F1DE101Hea_man.indb 66 8/16/2006 11:37:06 AM

Registro eventi



Gli eventi importanti come un errore di login o un aggiornamento del firmware sono registrati in una serie di campi di destinazione (vedi figg. 6-33). Ogni evento appartiene a un gruppo di eventi che può essere attivato separatamente. Il modo più comune per registrare gli eventi è quello di usare l'elenco di registrazione interno dell'unità RIPM. Per visualizzare l'elenco di registrazione, cliccare su "Event Log" sulla pagina Manutenzione. Nelle impostazioni del registro eventi, è possibile scegliere la quantità di voci da registrare su ogni pagina. Si può anche pulire l'archivio di registrazione.

1. **Oggetti del registro eventi**
   Per registrare degli eventi, occorre utilizzare l'elenco di registrazione interno dell'unità RIPM. Per visualizzare l'elenco di registrazione, cliccare su "Event Log" sulla pagina Manutenzione. Dal momento in cui la memoria del sistema è utilizzata per salvare tutte le informazioni, il numero massimo di voci di registrazione è limitato a 1000 eventi. Ogni registrazione che eccede questo limite soprascrive la più vecchia.

   Avvertenza: Se il tasto di reset sul front-end in HTML è usato per riavviare l'unità, tutte le informazioni di registrazione saranno salvate permanentemente e saranno disponibili dopo il riavvio dell'unità. Se l'unità RIPM non è alimentata o si esegue un resettaggio, tutte le informazioni di registrazione saranno perse. Per evitare ciò, utilizzare uno dei metodi descritti qui di seguito.

   1a. Registrazione del sistema di file distribuito (NFS) abilitata
   Definire un server NFS verso i quali le directory e i link statici devono essere esportati; tutte le informazioni di registrazione saranno pertanto scritte su un file in quel percorso. Per scrivere le informazioni di registrazione da più dispositivi RIPM a un solo NFS share, occorre definire un nome di file che sia unico per ogni dispositivo. Quando si modificano le impostazioni del NFS e si preme il tasto "Apply", il NFS share sarà montato immediatamente. Ciò significa che il NFS share e il server NFS devono ricevere sorgenti di informazione valide o si riceverà un messaggio di errore.

   Nota bene: Contrariamente all'archivio di registrazione interno dell'unità RIPM, le dimensioni dell'archivio di registrazione interno del sistema di file distribuito (NFS) non è limitato. Ogni evento sarà aggiunto alla fine del file in modo che si espanda continuamente. Ogni tanto bisognerebbe eliminare o spostare gli eventi registrati nell'archivio.

P75075ea_F1DE101Hea_man.indb 67 8/16/2006 11:37:06 AM

1b. Impostazioni SNMP

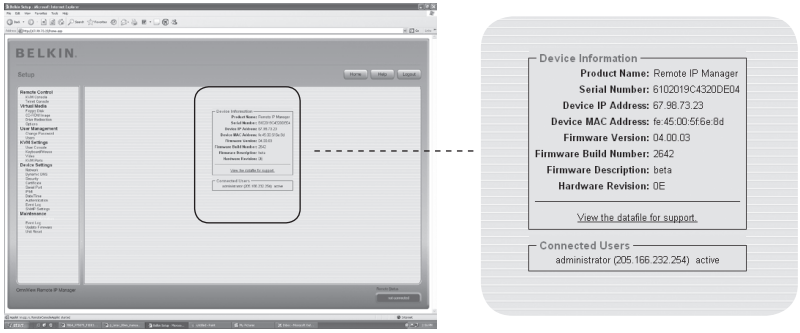
Registrazione del protocollo SMTP abilitata
Con questa opzione, l'unità RIPM è in grado di inviare le e-mail a un indirizzo immesso in un campo di testo di indirizzo e-mail nelle impostazioni del registro eventi. Questi messaggi contengono le stesse stringhe descrittive presenti nell'archivio di registrazione interno e l'oggetto del messaggio corrisponde al gruppo eventi dell'evento di registrazione occorso. Per utilizzare questo percorso di registrazione, occorre specificare un server SMTP che sia raggiungibile dall'unità RIPM e che non necessiti di alcuna autenticazione (<serverip>:<port>).

Registrazione del protocollo SNMP abilitata
Se attivata, l'unità invia un trap SNMP all'indirizzo IP specificato ogni volta che si verifica un evento di registrazione. Se il ricevente richiede una stringa di comunità, è possibile impostarla nel campo appropriato. Nella maggior parte dei trap dell'evento compare soltanto una stringa descrittiva con tutte le informazioni sull'evento di registrazione. L'autenticazione e l'alimentazione dell'host hanno dei trap standard propri, che creano automaticamente e che sono composti da diversi campi che informano sull'evento. Per ricevere questo trap SNMP, utilizzare un
listener di trap SNMP.

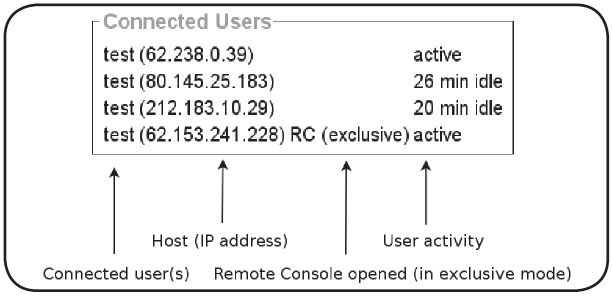
2. Assegnazioni del registro eventi
È possibile scegliere le azioni da salvare nell'archivio di registrazione. Spuntare le caselle desiderate e fare clic su "Apply" per confermare la scelta.

P75075ea_F1DE101Hea_man.indb 68 8/16/2006 11:37:07 AM

Informazioni sul dispositivo



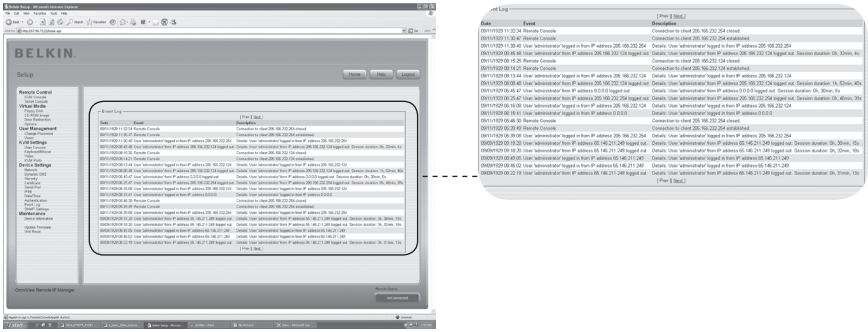
Questa sezione contiene una sintesi delle informazioni su questa unità RIPM ed il suo attuale firmware, oltre a come azzerare i parametri dell'unità RIPM. L'archivio di dati per il supporto consente di scarcare l'archivio dati dell'unità con informazioni specifiche per il supporto. Questo è un file XML (eXtensible Markup Language) con informazioni di supporto personalizzate, ad es. il numero seriale.



La figura sopra riportata raffigura l'attività dell'unità. Da sinistra verso destra, la figura mostra gli utenti connessi, l'indirizzo IP dell'utente dell'host e lo stato dell'attività dell'unità RIPM. "RC" significa che la console remota è aperta. Se la console remota è aperta nella modalità esclusiva, il termine "exclusive mode" verrà aggiunto. Per maggiori informazioni su questa opzione, leggere la sezione "Barra di controllo della console remota" a pagina 23 di questo manuale d'uso. Per visualizzare l'attività dell'utente, l'ultima colonna contiene il termine "active" per indicare un utente attivo o "20 min idle" per indicare un utente che non è stato attivo per un determinato periodo di tempo.

P75075ea_F1DE101Hea_man.indb 69 8/16/2006 11:37:07 AM

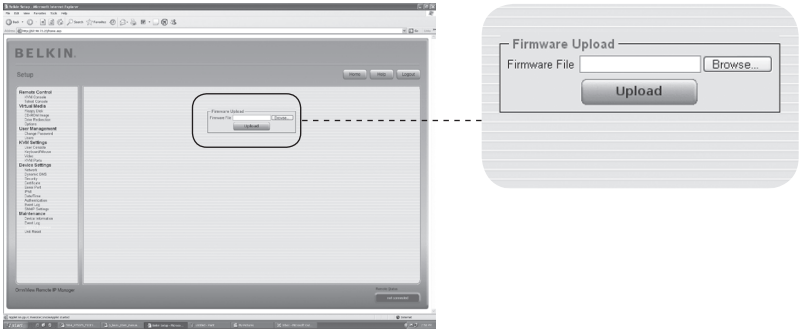
Registro eventi



L’elenco del registro eventi comprende gli eventi conservati dall’unità, quelli estesi dalla data dell’evento, una breve descrizione dell’evento e un indirizzo IP che indica l’origine dell’evento richiesto. Occorre utilizzare i tasti “Prev” e “Next” per sfogliare i dati.

P75075ea_F1DE101Hea_man.indb 70 8/16/2006 11:37:08 AM

Aggiornamenti del firmware



L'unità RIPM è un computer completamente autonomo; utilizza un software conosciuto come firmware, scritto sulla propria memoria di sola lettura (ROM). Il firmware dell'unità può essere aggiornato a distanza per installare funzionalità nuove o versioni migliori. Un nuovo aggiornamento del firmware è un file binario che deve essere scaricato dal sito web di Belkin. Se il file del firmware è compresso (ad es., se l'estensione del file è .zip), occorre decomprimerlo prima di procedere. Nei sistemi operativi di Windows, è possibile utilizzare WinZip (reperibile sul web al link http://www.winzip.com/) per decomprimere gli aggiornamenti del firmware.
Nota bene: per aggiornare il firmware, occorre salvare il nuovo file decompresso del firmware sul sistema che si collega all'unità RIPM.

Aggiornamento del firmware in tre fasi:

1. Trasferire in nuovo file del firmware sull'unità RIPM. A tal fine, selezionare il file sul sistema locale utilizzando il tasto "Browse" dal pannello "Upload Firmware". Quindi fare clic su "Upload" per trasferire sull'unità il file precedentemente selezionato dal sistema locale. Una volta trasferito il file del firmware, l'unità RIPM verificherà automaticamente la correttezza e confermerà che non si sia verificato alcun errore di trasmissione. Se si verifica un errore, la funzione di upload del firmware sarà interrotta e il firware rimarrà intatto.
2. Se il trasferimento avviene con successo (come dovrebbe succedere), comparirà il pannello "Update Firmware". Il pannello visualizzerà la versione del firmware attualmente in esecuzione e la versione del firmware trasferito. Fare clic su "Update" per sostituire la vecchia versione con quella nuova.

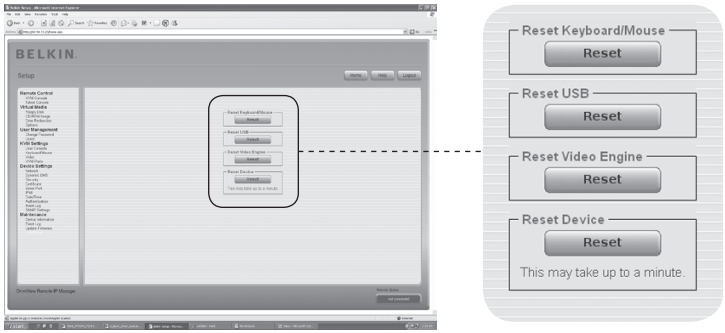
   Avvertenza: Questo processo è irreversibile e solitamente richiede diversi minuti. Verificare che l'alimentazione dell'unità non venga interrotta durante il processo di aggiornamento; un'interruzione della corrente potrebbe rendere instabile l'unità.
3. Una volta aggiornato il firmware, l'unità RIPM eseguirà automaticamente un resettaggio. Dopo circa un minuto, sarete reindirizzati sulla pagina di login per un nuovo collegamento.

   Avvertenza: Questo processo di aggiornamento del firmware in tre fasi e di verifica della correttezza garantisce che l'aggiornamento del firmware

P75075ea_F1DE101Hea_man.indb 71 8/16/2006 11:37:09 AM

avverrà senza errori. Tuttavia, l'aggiornamento del firmware dovrebbe essere effettuato soltanto da personale specializzato. È importante che l'alimentazione dell'unità NON venga interrotta durante il processo di aggiornamento.

Resettaggio dell'unità



Questa sezione descrive i metodo utilizzati per resettare determinate parti del dispositivo. Questo riguarda la tastiera, il mouse, lo schermo video del computer collegati all'unità e la stessa unità RIPM. Per attivare il nuovo firmware aggiornato, occorre resettare l'unità. Questo processo chiuderà automaticamente tutte le connessioni aperte alla console di amministrazione e all'unità e richiederà circa 30 secondi. Il resettaggio dei sottodispositivi (come la macchina video) richiede soltanto alcuni secondi e non chiuderà le connessioni. Per resettare un'unità RIPM specifica, fare clic sul tasto "Reset" come mostrato nella figura qui sopra.

Nota bene: Soltanto l'amministratore può resettare l'unità RIPM.

P75075ea_F1DE101Hea_man.indb 72 8/16/2006 11:37:09 AM

Il mouse remoto non funziona o non è sincronizzato.

Verificare prima di tutto la connessione VGA. L'unità RIPM e il monitor locale devono supportare la stessa risoluzione video. Verificare che le impostazioni del mouse corrispondano con il modello del mouse (PS/2 o USB). Inoltre, il modello del mouse deve essere impostato sull'unità RIPM e sul sistema operativo dell'host (il computer collegato all'unità). In alcune circostanze, il processo di sincronizzazione del mouse può causare degli errori. Per maggiori informazioni, leggere la sezione "Mouse, tastiera e configurazione video" nel capitolo 3.

La qualità video è cattiva e/o presenta granulosità.

Utilizzare la voce del menu "Reset" per impostare l'unità sui propri valori predefiniti. Quindi cliccare sul tasto "Auto-Adjust" per selezionare un'uscita video appropriata. Verificare che i cavi video siano collegati nel modo corretto.

Il collegamento con l'unità non è riuscito

Verificare il nome utente e la password. Il nome utente predefinito è "administrator" e la password predefinita è "belkin". Accertarsi che il browser web sia configurato per accettare i cookie.

La finestra della console remota non si apre.

Verificare che Java sia stato caricato. Un firewall potrebbe impedire l'accesso alla console remota. Le porte TCP #80 (per HTTP) e #443 (per HTTPS e RFB) devono essere aperte (il server che fornisce il firewall deve accettare le connessioni TCP in entrata su queste porte).

La console remota non è in grado di collegarsi e visualizza un errore di time-out

Verificare che l'installazione dell'hardware e della rete. Se c'è un server proxy tra l'unità e l'host, non sarà possibile trasferire dati video utilizzando l'RFB. Stabilire una connessione diretta tra l'unità e il client. Inoltre, verificare le impostazioni dell'unità e scegliere una porta server diversa per il trasferimento RFB. Se si usa un firewall, verificare che la porta accetti le connessioni. È possibile limitare queste connessioni agli indirizzi IP utilizzati dall'unità e dal client.

Nessuna connessione possibile con l'unità.

Controllare l'hardware. L'unità RIPM è collegata con la presa di alimentazione? Verificare la configurazione di rete (indirizzo IP, router). Inviare una richiesta "ping" all'unità per sapere se l'unità è raggiungibile tramite la rete.

Le combinazioni di comandi particolari (come ALT+F2, ALT+F3) sono intercettate dal sistema della console e non vengono trasmesse all'host.

Definire una cosiddetta "sequenza di tasti". Questo si può fare nelle impostazioni della console remota (leggere la sezione "Barra di controllo della console remota a pag.23).

P75075ea_F1DE101Hea_man.indb 73 8/16/2006 11:37:10 AM

Le pagine web dell'unità non sono visualizzate nel modo corretto.

Verificare le impostazioni della memoria del browser. Accertarsi che le impostazioni della memoria cache non siano impostate su "never check for newer pages". Con questa impostazioni, le pagine dell'unità RIPM potrebbero essere caricate dalla memoria cache del browser e non dall'unità, causando il problema in questione.

Windows XP non si risveglia dalla modalità di standby.

Molto probabilmente si tratta di un problema di Windows XP. Cercare di non muovere il cursore del mouse quando Windows XP entra in modalità di standby. Per maggiori informazioni, leggere il manuale del sistema operativo.

Ogni volta che riapro la finestra di dialogo della console remota, i cursori dei mouse non sono più sincronizzati.

Disabilita l'opzione "Centra automaticamente il puntatore del mouse sul tasto di default delle finestre di dialogo" nelle impostazioni del mouse del sistema operativo.

La console remota rimane oscurata.

Verificare se l'unità RIPM è alimentata solo tramite USB. Se non riceve sufficiente corrente via USB, la console remota si apre ma rimane oscurata. Verificare le impostazioni dell'unità a pagine 26 di questo manuale d'uso. Verificare che i cavi video siano collegati nel modo corretto.

I dati video sul monitor locale sono circondati da un bordo nero.

Non si tratta di un errore. Il monitor locale è programmato su una modalità video fissa che può essere selezionata nelle impostazioni video dell'unità. Leggere la sezione "Barra di controllo della console remota" a pagina 23 di questo manuale d'uso.

Ho dimenticato la password. Come posso ripristinare le impostazioni predefiinte dell'unità?

Si può usare l'interfaccia seriale. Per maggiori informazioni, leggere la sezione "Ripristino delle impostazioni predefinite dell'unità RIPM" a pagina 31 di questo manuale d'uso.

Andare su www.belkin.com per ulteriori suggerimenti di risoluzione delle anomalie e un elenco di dispositivi compatibili con l'unità RIPM.

Nota bene: Se la situazione non cambia dopo aver fatto questi tentativi, contattare il servizio di assistenza tecnico al 1-800-2BELKIN.

P75075ea_F1DE101Hea_man.indb 74 8/16/2006 11:37:10 AM

Dichiarazione FCC

Dichiarazione di conformità con le norme FCC per la compatibilità elettromagnetica

Belkin Corporation, con sede al 501 West Walnut Street, Compton, CA 90220, dichiara sotto la propria piena responsabilità che il prodotto,

F1DE101H

cui questa dichiarazione fa riferimento:
è conforme alla sez. 15 delle norme FCC. Le due condizioni fondamentali per il funzionamento sono le seguenti: (1) il dispositivo non deve causare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, comprese eventuali interferenze che possano causare un funzionamento anomalo.

Dichiarazione di conformità CE
Noi sottoscritti, Belkin Corporation, dichiariamo sotto la nostra piena responsabilità che il prodotto F1DE101H, cui questa dichiarazione fa riferimento, è realizzato in conformità allo Standard sulle Emissioni EN550022 e alla Norma di Immunità EN550024, nonché agli standard LVP EN610003-2 e EN61000-3-3.

ICES
Questo apparecchio digitale di classe B è conforme allo standard canadese ICES-003. Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Garanzia di 2 anni offerta da Belkin Corporation

Oggetto della garanzia.
Belkin Corporation garantisce al primo acquirente di qualsiasi adattatore di corrente Belkin è esente da difetti di montaggio, materiale e lavorazione.

Qual è il periodo di copertura?
Belkin Corporation garantisce il prodotto Belkin per due anni.

Cosa faremo per correggere eventuali problemi?
Garanzia sul prodotto.
Belkin provvederà a riparare o sostituire gratuitamente, a sua discrezione, qualsiasi prodotto che dovesse risultare difettoso (escluse le spese di trasporto).

Cosa non copre la garanzia?
Tutte le garanzie di cui sopra saranno rese nulle qualora il prodotto Belkin non fosse fornito alla Belkin Corporation per essere sottoposto alle necessarie verifiche dietro espressa richiesta di Belkin e a spese del cliente, oppure nel caso la Belkin Corporation dovesse stabilire che il prodotto non è stato correttamente installato o che sia stato in qualche modo alterato o manomesso. La Garanzia sul prodotto Belkin non copre danni da imputarsi a calamità naturali (tranne i fulmini), tra cui allagamenti o terremoti, da guerre, atti di vandalismo, furti, usura, erosione, assottigliamento, obsolescenza, abusi, danni dovuti ad interferenze di bassa tensione (tra cui parziali oscuramenti o abbassamenti di tensione), programmazione non autorizzata oppure modifiche o alterazioni all'apparecchiatura dell'impianto.

Come usufruire del servizio di garanzia.
Per usufruire dell'assistenza per il proprio prodotto Belkin, è necessario:

1. Contattare la Belkin Corporation all'indirizzo 501 W. Walnut St., Compton CA 90220, att.: Customer Service, oppure chiamare il numero (800)-223-5546, entro 15 giorni dall'evento. Avere a disposizione le seguenti informazioni::
   a. Il codice del prodotto Belkin.
   b. Il luogo di acquisto del prodotto.
   c. La data di acquisto del prodotto.
   d. Copia della ricevuta originale.
2. Il rappresentante del Servizio Clienti Belkin vi spiegherà come inviare la ricevuta e il prodotto Belkin e come procedere con il reclamo.

P75075ea_F1DE101Hea_man.indb 75 8/16/2006 11:37:10 AM

Belkin Corporation si riserva il diritto di riesaminare il prodotto Belkin danneggiato. Tutte le spese di spedizione per il prodotto Belkin restituito alla Belkin Corporation sono a carico dell'acquirente. Se Belkin determina, a sua discrezione, che inviare l'apparecchio danneggiato non è pratico, Belkin potrebbe decidere, a sua discrezione di farlo ispezionare e determinare il costo della riparazione. In caso ci fossero delle spese di spedizione per inviare e ricevere l'apparecchio dopo l'ispezione, queste saranno a carico dell'acquirente. Eventuali apparecchi danneggiati dovranno essere mantenuti disponibili per eventuali verifiche fino alla risoluzione della richiesta di indennizzo. Al raggiungimento dell'accordo, Belkin Corporation si riserva il diritto di essere surrogato da eventuali polizze assicurative dell'acquirente.

Cosa stabilisce la legge riguardo alla garanzia.
LA PRESENTE GARANZIA E L'UNICA GARANZIA, ESPLICITA O IMPLICITA, DELLA BELKIN CORPORATION. SI ESCLUDE QUALSIASI GARANZIA IMPLICITA, DI COMMERCIABILITÀ E DI ATTITUDINE PER SCOPI PARTICOLARI CHE VANNO OLTRE QUESTA GARANZIA ESPLICITA SCRITTA.

Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non fare al caso vostro.

IN NESSUN CASO BELKIN CORPORATION POTRÀ ESSERE CONSIDERATA RESPONSABILE DI ALCUN DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIFICO O DANNI MULTIPLI TRA I QUALI, MA NON SOLO, EVENTUALI DANNI DI MANCATI AFFARI O MANCATO GUADAGNO DERIVATI DALLA VENDITA O UTILIZZO DELL'ADATTATORE DI CORRENTE BELKIN, ANCHE NEL CASO IN CUI BELKIN FOSSE STATA INFORMATA DELLA POSSIBILITÀ DI TALI DANNI.

Questa garanzia consente di godere di diritti legali specifici ed eventuali altri diritti che possono variare di stato in stato. Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non fare al caso vostro.

Smaltimento dei rifiuti di apparecchiature da parte di privati nell'Unione Europea.
Questo simbolo posto sul prodotto o sulla sua confezione indica che tale prodotto non deve essere gettato via insieme ai rifiuti domestici. L'utente ha la responsabilità di liberarsi dell'apparecchiatura portandola in un punto di raccolta deputato al riciclaggio di rifiuti di apparecchi elettrici ed elettronici. La raccolta separata e il riciclaggio degli apparecchi da smaltire contribuiranno alla salvaguardia delle risorse naturali e garantiranno che il prodotto sia riciclato in modo da non mettere in pericolo la salute umana. Per maggiori informazioni sui punti di smaltimento e riciclaggio per le apparecchiature elettroniche, vi preghiamo di contattare il vostro comune, il servizio di smaltimento rifiuti domestici o il negozio in cui avete acquistato.

P75075ea_F1DE101Hea_man.indb 76 8/16/2006 11:37:10 AM

BELKIN®

OmniView® Remote IP Manager

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, Regno Unito
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Paesi Bassi
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spagna
+34 9 16 25 80 00
+34 9 02 02 00 34 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, Francia
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH
Hanebergstrasse 2
80637 Monaco di Baviera, Germania
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

© 2006 Belkin Corporation. Tutti i diritti riservati. Tutti i nomi commerciali sono marchi registrati dei rispettivi produttori indicati. Mac OS e Macintosh sono marchi della Apple Computer, Inc., registrata negli USA e in altri Paesi.

P75075ea

BELKIN®

OmniView® Remote IP Manager

BELKIN®

www.belkin.com

Belkin Corporation
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spain
+34 9 16 25 80 00
+34 9 02 02 00 34 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt, France
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

Belkin GmbH
Hanebergstrasse 2
80637 Munich, Germany
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

© 2006 Belkin Corporation. All rights reserved. All trade names are registered trademarks of respective manufacturers listed.
Mac OS and Macintosh are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

P75075ea