Manuals+ — User Manuals Simplified.

BELKIN F1DE101G OmniView Remote IP Console User Manual

BELKIN
®

OmniView™
Remote IP Console
Remotely control a server, or multiple servers
with a KVM Switch, over TCP/IP networks

User Manual
ENTERPRISE Quad-Bus Series
F1DE101G

Contents

OVERVIEW

Introduction

Congratulations on your purchase of this Belkin OmniView ENTERPRISE Quad-Bus Series Remote IP Console (the RIPC). Our diverse line of KVM solutions exemplifies the Belkin commitment to delivering high-quality, durable products at a reasonable price. Designed to give you control of your computer or KVM switch from anywhere around the world through any web browser, the RIPC can be easily configured to accommodate your existing LAN setup, large or small.

Belkin has designed and developed the RIPC with the server administrator in mind. The result is a powerful, yet easy-to-install and -use remote solution that surpasses all other solutions with advanced features and functionality.

This manual will provide all the details you'll need about the RIPC, from installation to operation and troubleshooting, in the unlikely event of a problem.

Thank you for purchasing the OmniView ENTERPRISE Quad-Bus Series Remote IP Console. 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.

Package Contents

- One OmniView ENTERPRISE Quad-Bus Series Remote IP Console
- One PS/2 cable kit
- One 5V DC, 2000mA power supply
- User Manual
- Quick Installation Guide
- Registration Card
- Rack-mount bracket with screws
- One DB9 cable

Feature Overview
Capacity for one digital user support
Allows one digital user access to control a computer or KVM via web browser.
Web-browser compatibility
The RIPC can be accessed from any computer that is running Microsoft® Internet Explorer Version 5.5 or higher. No proprietary software is needed.
0U rack-mountable
The RIPC is compact enough to position on your desktop, behind another device, or attached to the side of your

server rack to take up 0U space.

User-defined hot keys

User-defined hot keys simulate keystrokes on the remote system that cannot be generated locally.

Flash upgrades

Flash upgrades allow you to obtain the latest firmware updates for your RIPC. These updates ensure that your RIPC continues to work with the latest devices and computers. Firmware upgrades are free for the life of the RIPC. Visit **belkin.com** for upgrade information and support.

LED display

Located on the face of the RIPC, the LED display provides an easy way for you to monitor the status of your connection, link, and activity.

Video resolution

With an 117MHz bandwidth, the RIPC is able to support video resolutions of up to 1280×1024@60Hz. To preserve signal integrity and obtain the best results, use Belkin video cables.

Web-based advanced user interface

You can set up the RIPC's functions easily through your web browser, without having to install additional software onto the computer. There are no disks to install or keep track of and you can make changes and perform setup functions from any computer on the network, quickly and easily.

Equipment Requirements
Hardware Requirements

- OmniView ENTERPRISE Quad-Bus Series Remote IP Console (included)

- PS/2 cable kit (included)

- 5V DC, 2000mA power supply (included)

- Keyboard, monitor, and mouse

- Connection to network using 10/100Base-T Ethernet port (RJ45)

- CAT5e crossover cable

- CAT5e straight-through cable

- Rack-mount bracket with screws (included, for rack-mount install option)

Software Requirements

- Microsoft Internet Explorer 5.5 and above

- Servers running Windows® NT®, 2000, and XP

Specifications
Part Number: F1DE101G
Power: 5V DC, 2000mA
Network Connection: 10/100Base-T connection (standard RJ45 connector)
Keyboard Emulation: PS/2
Mouse Emulation: PS/2
Monitors Supported: Supports all VESA graphics modes, and text modes
Max. Resolution: 1280×1024@60Hz
Bandwidth: 117MHz
Keyboard Input: 6-pin miniDIN (PS/2)
Mouse Input: 6-pin miniDIN (PS/2)
Computer/**KVM** Ports: 1
VGA Port: 15-pin HDDB type
LED Indicators: 2
Enclosure: Metal enclosure
Dimensions: 1.75 x 5.7 x 7 inches (43.1 x 144.7 x 177mm)
Weight: 1.8 lbs. (800g)
Operating Temp: 32° to 104° F (0~40° C)
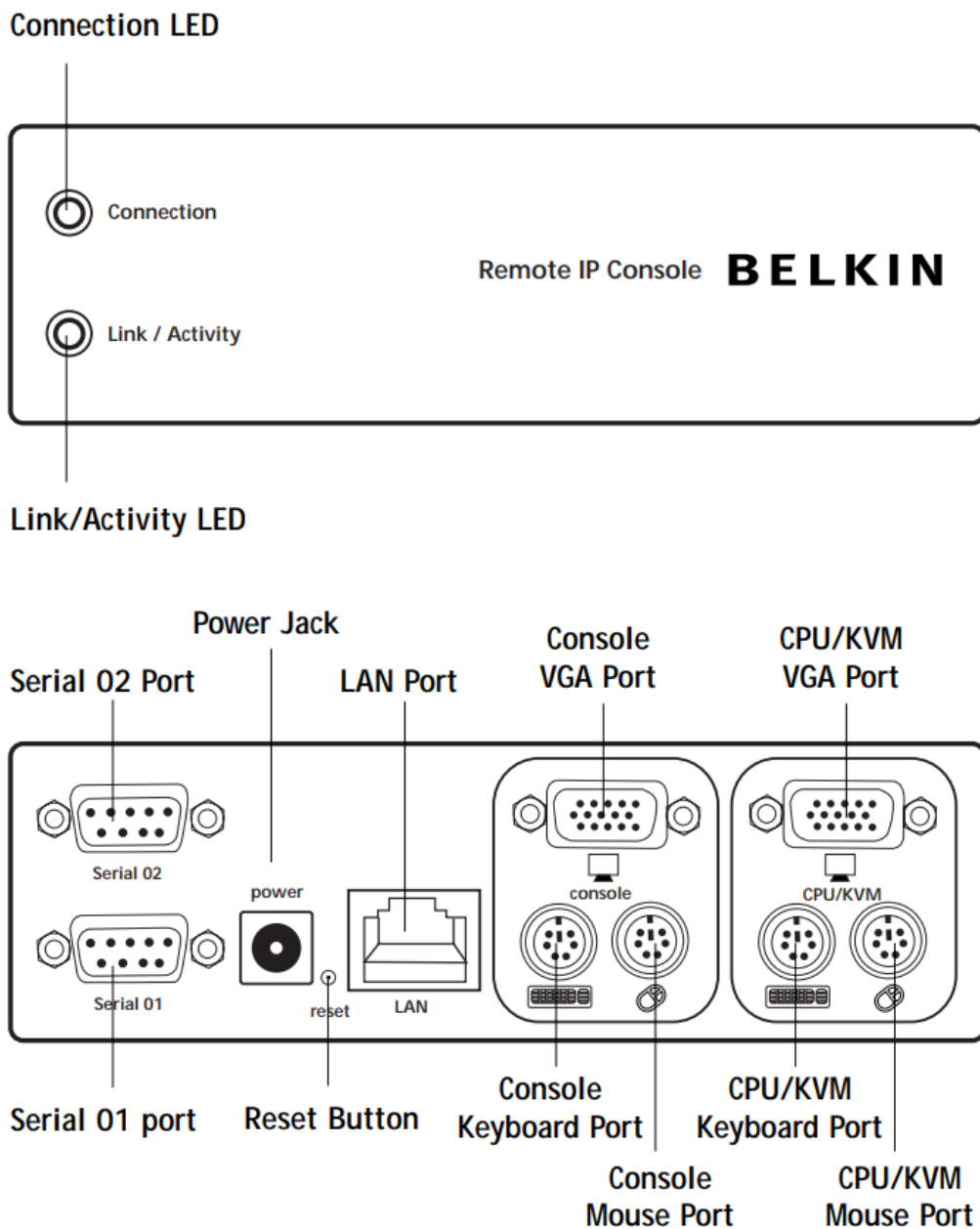
Storage Temp: 104° to 167° F (40~75° C)
Humidity: 0-80% RH, non-condensing
Maximum Altitude: 10,000 feet
Warranty: 1 year

Note: Specifications are subject to change without notice.

RIPC Diagrams

INSTALLATION

Hardware Installation
Installing the RIPC into a Server Rack
The RIPC includes mounting brackets for installation in 19-inch racks.

1. Attach the included bracket to the top or bottom of the RIPC with the provided Phillips screws.

2. Mount the RIPC to the rack.

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

Before attempting to connect anything to the RIPC 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.
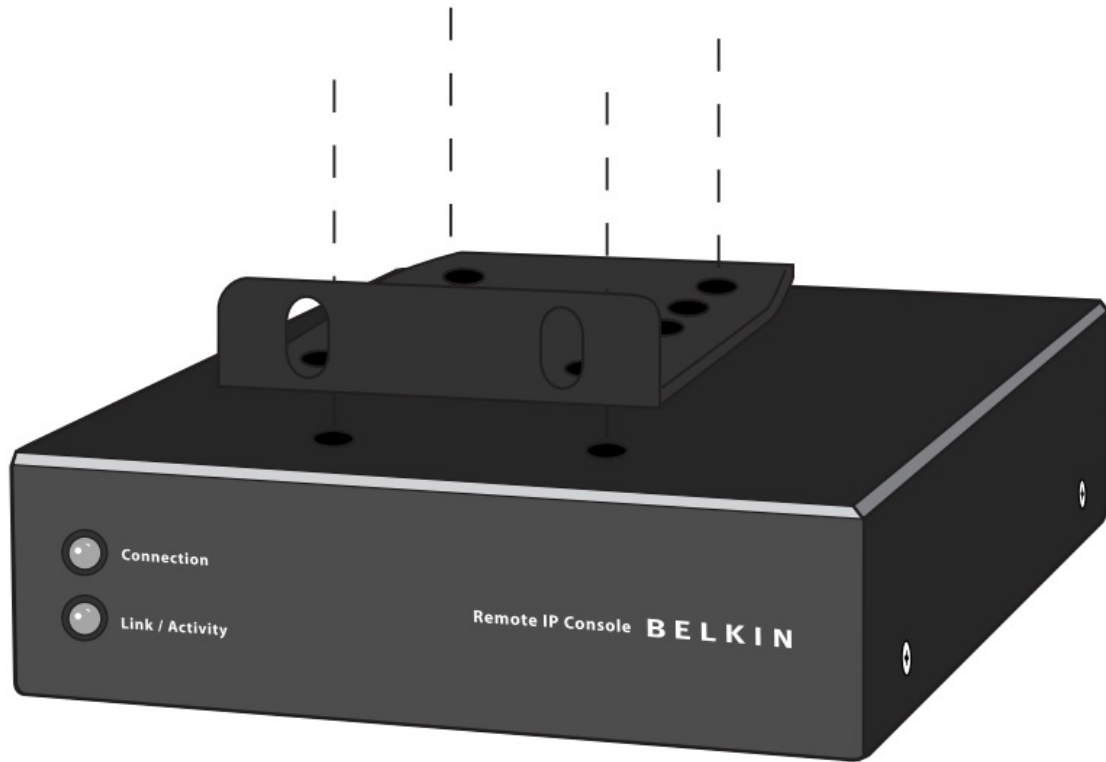

1. Power down your server or KVM Switch.
2. Connect your PS/2 type keyboard and mouse to the appropriate PS/2 "Console" ports.
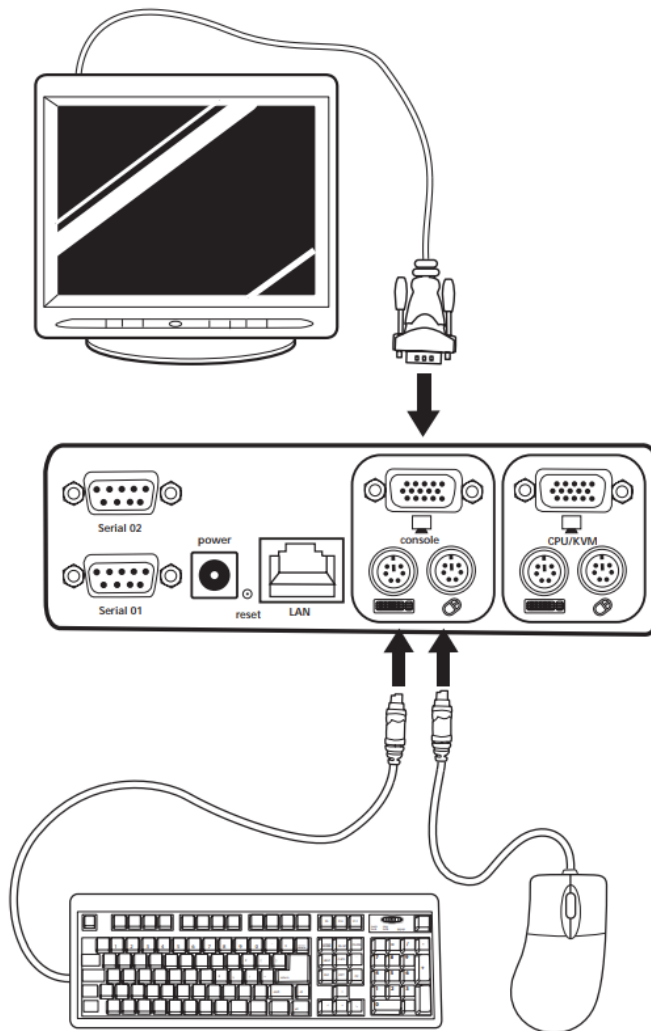
3. Take the video cable that is attached to your VGA monitor and connect it to the "Console" port.

Connecting the Computer or KVM
Using the provided PS/2 cable kit, connect one end of the VGA and PS/2 cables to your server. Connect the other end to the "CPU/KVM" ports on the back of the RIPC.
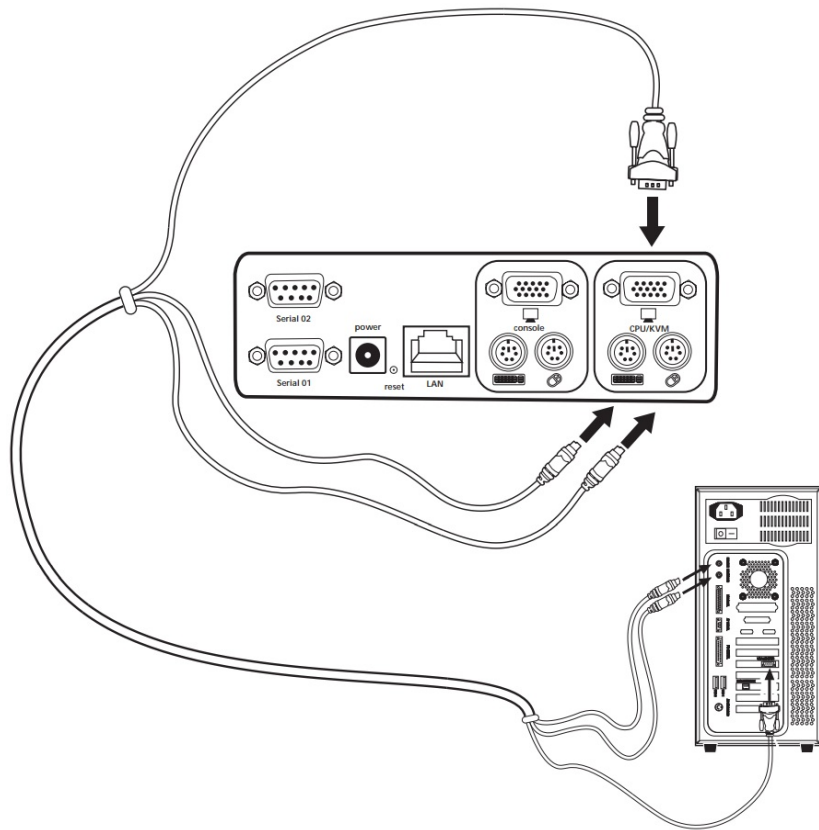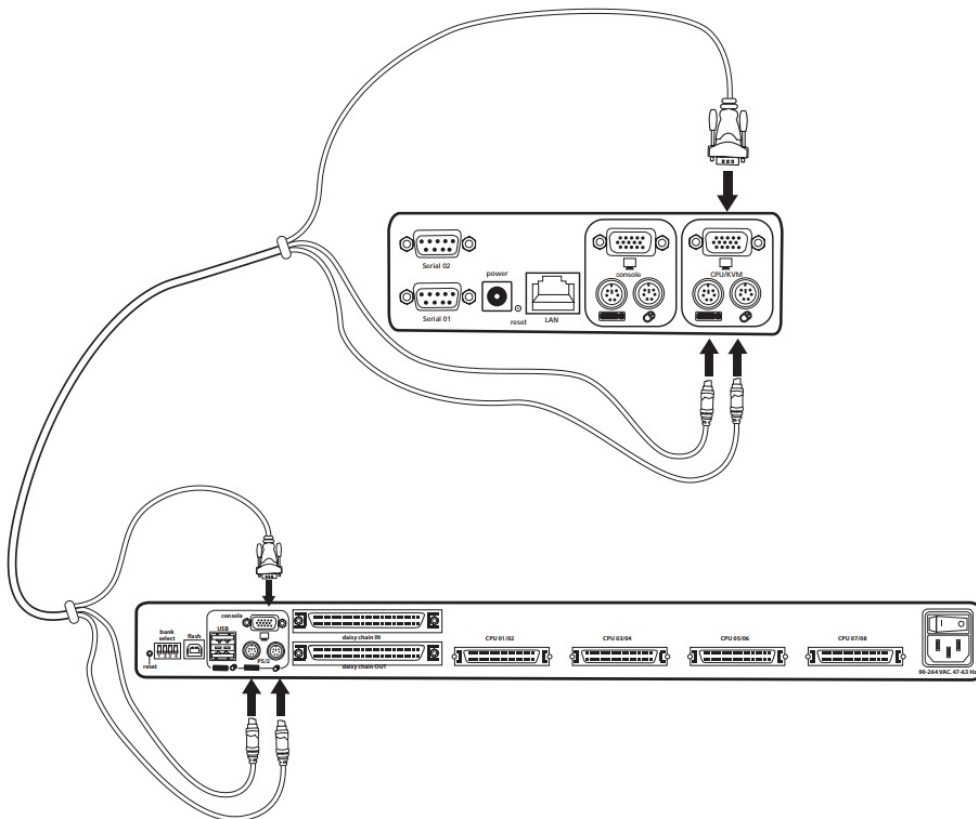
Connecting the Computer or KVM

Using the provided PS/2 cable kit, connect one end of the VGA and PS/2 cables to the RIPC on the KVM Switch. Connect the other end to the "CPU/KVM" ports on the back of the RIPC.

Powering Up the RIPC

1. Connect the included power supply unit into an available power outlet.

2. Attach the barrel plug into the power jack located on the rear of the RIPC to the power unit.
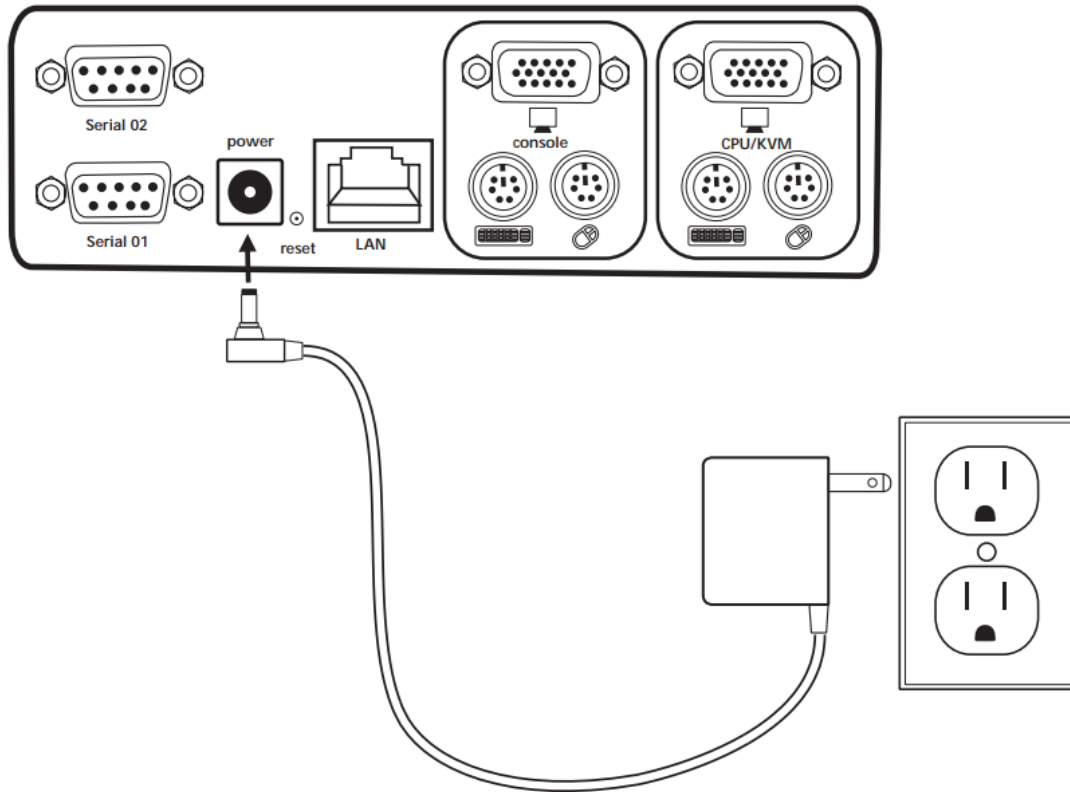
3. Turn on your KVM Switch. If you do not have a KVM Switch, please proceed with powering up your computers.

Initial Network Configuration

1. Using a RJ45 crossover cable, connect one end to the computer and the other end to the port labeled "Network".
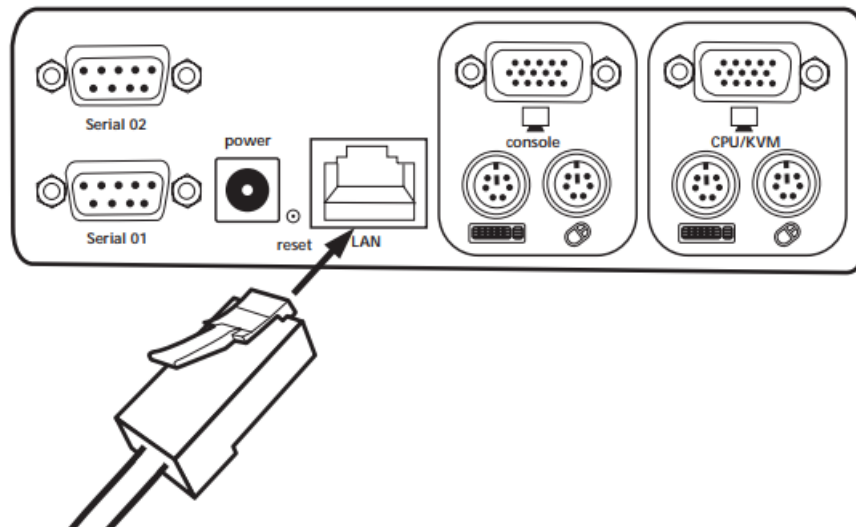
2. Set the IP address on your computer to be in the same range as 1.2.3.4 (example: 1.2.3.6).
3. Open the Microsoft® Internet Explorer web browser.
4. Enter the IP address "1.2.3.4".
5. Enter the default login name "administrator".

6. Enter the default password "belkin".

Initial Network Configuration

7. Under Setting & Configurations, click on "Network". (Note: Uncheck "DHCP" check box.)

8. Enter the desired network settings and click on "Apply Changes" to save new network settings.

9. Reset the local IP address settings on the computer used for configuration of the RIPC.

Connecting the RIPC to the Network
Connect the RIPC to the network using a straight-through RJ45 Category 5 network cable.

Remote Access
Remote Access is a Java™ applet that displays the redirected screen, keyboard, and mouse of the remote host system to which the RIPC is attached. The web browser used for accessing the RIPC must supply a Java Runtime Environment, version 1.1 or higher. Remote Access will perform in much the same way from a remote location as if you were sitting directly in front of the computer itself.
You will be able to use the keyboard and mouse in the usual way, however, the remote system will react to keyboard and mouse actions with a slight delay.
The length of the delay depends on the bandwidth of the line over which you are connected to the RIPC. Open the applet by choosing the appropriate link in the navigation frame of the HTML.

Bottom Part of the Remote Access Applet

The Remote Access Applet offers the following features:
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 RIPC adjusts for the best possible video quality.
Sync
Choose this option in order to synchronize the local with the remote mouse cursor.
Video settings
This opens a new window with elements to control the RIPC's video settings.
You can change some values related to brightness and contrast of the picture displayed, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

Configuration via serial
On a computer that has HyperTerminal Services software installed, connect the provided DB9 serial cable by attaching one end to your computer and the other end to the port labeled "Serial 1" on the RIPC.
Open the HyperTerminal software and use the following parameters:
Serial line parameters

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

You will now be able to set your networking configuration on the RIPC.

USING YOUR RIPC

Prerequisites

The RIPC features an embedded operating system and applications that offer a variety of standard user interfaces. The information following will describe their use in detail. All of the interfaces are accessed using the TCP/IP protocol, and can be used over either the built-in Ethernet adapter or the modem.

The following interfaces are supported:

HTTP/HTTPS: The most complete access is provided by an embedded web server and the RIPC's environment can be controlled by a standard web browser. Depending on the web browser, you can access the RIPC's card using the unsecured HTTP protocol or, if the browser supports it, the encrypted HTTPS protocol. We recommend use of HTTPS whenever possible.

Telnet: A standard telnet client can be used to access an arbitrary device connected to one of the RIPC's serial ports via a terminal mode.

In order to use the Remote Access window of your managed host system, the browser must include a Java Runtime Environment, version 1.1 or higher.

However, even if the used browser has no Java support, such as is the case on small handheld devices, you can still maintain your remote host system using the administration forms displayed by the browser itself.

We recommend the following browsers for an unsecured connection to the RIPC:

Microsoft Internet Explorer version 5.5 or higher on Windows 98, Me, 2000, and XP Netscape® Navigator® 7.0 or Mozilla 1.0 on Windows 98, Me, 2000, XP, Linux® and other UNIX®-like operating systems

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured if you are using key length of 128 bits. Many older browsers do not have a strong 128-bit encryption algorithm due to former export regulations of US authorities. Internet Explorer 5.0, which is included in Windows Me and 2000, supports a key length of only 56 bits. You can read about the key length of Internet Explorer under the menu points "?" and "Info". The dialog box displays a hyperlink that leads you to information on upgrading your browser to a state-of-the-art encryption scheme.

We recommend the following browser for a secured connection to the RIPC:

Microsoft Internet Explorer version 5.5 or higher on Windows 98, Me, 2000, and XP Netscape Navigator 7.0 or Mozilla 1.0 on Windows 98, Windows Me, 2000, XP, Linux, and other UNIX-like operating systems

Internet Explorer Showing the Encryption Length

Log Into the RIPC
Start your web browser and direct it to the address of your RIPC configured during installation.
To establish an unsecured connection, you must enter the following into the address line of your browser:
http://192.168.1.22/
For a secure connection, you must enter: **https://192.168.1.22/**
The RIPC has a built-in administrator-user that has permission to administrate your system:

Login name	administrator
Password	Belkin

Note: Be sure to change the administrator-user password immediately after you have installed and accessed your RIPC for the first time.

Main Screen
After a successful login, the RIPC will present its main screen frames (see Figure below).
The home button brings you instantly to the home page from one of the administration menu points. The logout button logs you out of the RIPC; it terminates the current session and will require you to re-enter your user name and password to log in again later.
Note: The RIPC will prompt you for a password automatically if there is no administration activity for 30 minutes.

The RIPC's Home Menu Window

Log Out from the RIPC
This link logs out the current user and presents a new login screen. An automatic logout will occur if there is no admin activity for a period of 30 minutes—following a prompt for re-entry of the password.

Control Host Remote Access
The Remote Access is the redirected screen, keyboard, and mouse of the remote host system the RIPC controls. Initiating Remote Access causes a pop-up window to appear that replicates the screen of your host system. Remote Access will perform in much the same way from a remote location as if you were sitting directly in front of the computer itself. You will be able to use the keyboard and mouse in the usual way, however, the remote system will react to keyboard and mouse actions with a slight delay. The length of the delay depends on the bandwidth of the line over which you are connected to the RIPC.

Remote Access Window Showing a Windows 2000 Desktop Screen

Note: You can circumvent communication issues between the local and remote keyboards by adjusting the keyboard of your remote system to the same mapping as that of your local one.
For example, if you are using a German administration system but your host system uses a U.S. English keyboard layout, special keys on the German keyboard will no longer function according to the local program, but will recreate that of their U.S. English counterpart.
The Remote Access Java applet tries to establish its own TCP connection to the RIPC. Its protocol is not HTTP or HTTPS, but another protocol called RFB (Remote Frame Buffer Protocol). Currently RFB tries to establish a connection to port number 443. Your local network environment must allow this connection to be made, i.e. if you are working over a private internal network your NAT (Network Address Translation) firewall settings must be configured accordingly. In other words, if the RIPC is connected to your local network environment and your connection to the Internet is over a proxy server only, failure to configure NAT correctly will make it very unlikely that the Remote Access will be able to establish the connection. This is because web proxies are not capable of relaying the RFB protocol.
If you are unsure about this issue, please consult your network administrator for an appropriate network environment.
Remote Access window attempts to display the remote screen at its optimal size, so that it may resize to match the remote screen initially, as well as following a change of the remote screen's resolution. You can always resize the Remote Access window using your local window system.
A control bar on the lower part of the Remote Access window houses a control bar that displays Remote Access status and lets you adjust its settings. The following table defines the Remote Access control options:

Control	Description
Options ➤ Scaling	Allows you to scale down the Remote Access. You can still use the mouse and keyboard, however, the scaling algorithm will not preserve all display details.
Options ➤ Mouse Handling	The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointers.
Options ➤ Video Settings	Opens a panel for changing the RIPC's video settings.
Hot Keys	Special button keys to send the defined key combinations to the remote system.
KVM Keys	If defined in KVM Port Settings, you can switch the current KVM port by sending the appropriate hot key to the KVM switch.
Read Option	Toggles the read-only mode on and off. If the Monitor mode chec box is selected, the Remote Access will not accept any local inpu for either keyboard or mouse. The symbol indicates whether or no monitor mode is currently active.
Auto Adjust	Starts the auto adjustment procedure to determine the settings for best visual quality of the current image being displayed on the RIPC.

Remote Access Options

The Remote Access title bar displays information about the incoming (In:) and outgoing (Out:) network traffic. If you are using the compressed encoding, both compressed and uncompressed incoming traffic will be indicated.

Remote Access Title Bar

Power Management Unit

This provides a Java applet that enables the telnet protocol to open a connection to the RIPC. Its main use is the pass-through option for serial port 1, however, it also allows you to connect with a standard Telnet client. Telnet access must be enabled in the security settings.

RIPC Mouse Synchronization

The RIPC addresses a common KVM-device challenge, which is the synchronization between the local and remote mouse cursors. To do so, it uses an intelligent synchronization algorithm.

There are three ways to re-synchronize local and remote mouse signals:

Fast Sync

The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Access options menu or, if you defined a mouse synchronization hot key sequence, use it.

Sync Detect

If the sync doesn't work, or if the mouse settings have been changed on the host system, use the intelligent re-synchronization. This method takes longer than the fast synchronization and can be accessed with the appropriate item in the Remote Access option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto-adjustment function or the manual correction in the Video Settings panel to set up the picture.

Single (Direct) Mouse Mode

If all synchronization options fail, it is still possible to work with the remote mouse by selecting the single-mouse mode, using the image button. If activated, all mouse movements are transmitted directly to the host, so you can adjust the host mouse settings to less extreme values, or work in this mode if mouse acceleration is turned off. In this mode all synchronization options perform a fast sync.

Limitations of the Mouse Synchronization

While the intelligent algorithm works fine for common cases, there are some special limitations, which may prevent the synchronization from working properly:

Special Mouse Driver

These are mouse drivers that influence the synchronization process leading to desynchronized mouse pointers. If this happens, make sure you don't use a special vendor-specific mouse driver on your host system.

Badly Adjusted Picture

For intelligent sync to work, a correctly adjusted picture is necessary. Use the auto-adjustment function or the manual correction in the Video Settings panel to set up the picture.

Active Desktop

Check to see whether you have the Active Desktop feature of Microsoft Windows enabled. If so, do not use a plain background; be sure to use some kind of wallpaper. You can also disable the Active Desktop entirely.

Video Settings

The RIPC features a panel to set up the following video options, available in the Remote Access Options menu.
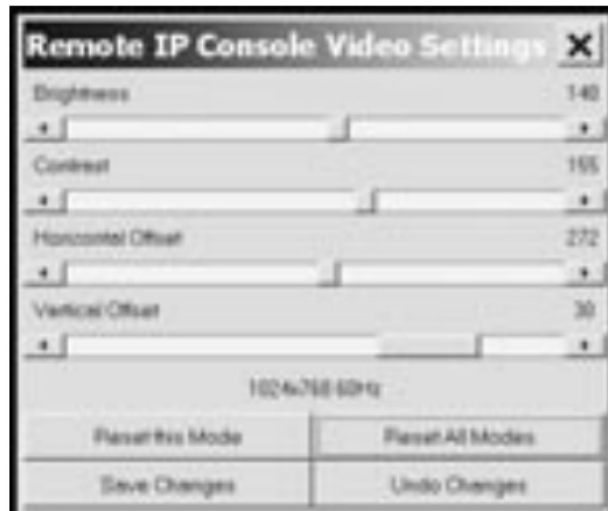
Video Settings Panel

Note: Brightness and contrast controls affect all modes and KVM ports globally; the other settings are changed specifically for each mode on each KVM port.

Horizontal Offset: Use the left and right buttons to move the picture in a horizontaldirection while this option is selected.

Vertical Offset: Use the left and right buttons to move the picture in a verticaldirection while this option is selected.

Reset this Mode: Resets mode-specific settings to their factory defaults.

Reset all Modes: Resets all settings to their factory defaults.

Save Changes: Saves changes permanently.

Undo Changes: Restores last settings.

SECURITY

Ports & Protocols

Force HTTPS

If this option is enabled, access to the Web front-end is only possible using an HTTPS connection. The RIPC won't work on the HTTP port for incoming connections.

HTTPS Port

Port number at which the HTTPS server is set to. If left unused or open, the default value will be used.

HTTP Port

Port number at which the RIPC's HTTP server is set to. If left unused or open, the default value will be used.

Telnet Port

Port number at which the RIPC's Telnet server is set to. If left unused or open, the default value will be used.

Remote access & HTTPS port >   (Default: 443)

HTTP port >   (Default: 80)

TELNET port >   (Default: 23)

More Info

(Clear changes) (Apply changes)

Firewall
IP access control parameters

Parameter	Description
Enable Firewall	Enables access control based on IP source addresses.
Default Policy	This option controls arriving IP packets that don't match any of the configured rules. They can be accepted or dropped. *Note: If you set this to DROP and you have no ACCEPT rules configured, acce to the We b over LAN is disabled. To enable access again, you can change th security settings via m odem or ISDN dial-in or by temporarily disabling IP access control with the initial configura tion procedure.*
Rule Number	This should contain the number of a rule for which the following commands will apply. This field will be ignored, in case of appending a new rule.
IP/Mask	Specifies the IP address or IP address range for which the rule applies. Examples (the nu mber concatenated to an IP address with a '/' is the number of valid bits that will be used o f the given IP address): 192.168.1.22 or 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 19 2.168.1.255 0.0.0.0/0 matches any IP packet

Firewall Settings Menu

Enable Firewall >   ☐

Default policy >   ACCEPT ▾

Rule #	IP / Mask	Policy
		ACCEPT ▾

Append   **Insert**   **Replace**   **Delete**

More Info

Apply

Certificate Management

The RIPC uses the SSL protocol for any encrypted network traffic between itself and a connected client. During connection establishment, the RIPC has to expose its identity to a client using a cryptographic certificate.

Common name >

Organizational unit >

Organization >

Locality/City >

State/Province >

Country (ISO code) >

Email >

Challenge password >

Confirm Challenge password >

Key length (bits) >

More Info

Create CSR

SSL Certificate Request

Parameter	Description
Common name	This is the network name of the RIPC once it is installed in the user's network.
Organizational unit	This field is used for specifying to which department within an organization the RIPC belongs.
Organization	The name of the organization to which the RIPC belongs.
Locality/City	The city where the organization is located.
State/Province	The state or province where the organization is located.
Country	The country where the organization is located. This is the two-letter ISO code, e.g. US for the USA.
Challenge Password	Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of th certificate). The minimal length of this password is four character
Confirm Challenge Password	Confirmation of the Challenge Password.
E-mail	The e-mail address of a security contact person that is responsib for the RIPC.
Key length	This is the length of the generated key in bits. 1024 bits are suppos to be sufficient for most cases. Larger keys may result in slower response time of the RIPC during connection establishment.

Certificate Request Required Information
However, it is possible to generate and install a new certificate that is unique for a particular card. In order to do that, the RIPC is able to generate a new cryptographic key and the associated Certificate Signing Request that needs to be certified by a certification authority (CA). A certification authority verifies that you are who you claim you are and signs and issues a SSL certificate to you.
The following steps are necessary to create and install the RIPC's SSL certificate:

1. Create a SSL Certificate Signing Request using the panel shown in the Figure below (Security Settings ➤ SSL Settings ➤ Create your own SSL certificate). Fill out a number of fields that are explained in the table above. Once this is done, click "Create CSR" which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the "Download CSR" button (see Figure below).

2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a traditional authentication process.

3. Upload the certificate to the RIPC using the Upload panel as shown in the Figure below.

The following CSR is pending >

countryName = bl
stateOrProvinceName = test
localityName = test
organizationName = test
organizationalUnitName = test
commonName = test
emailAddress = test@test.com

(Download CSR) (Delete CSR)

More Info

SSL Certificate Upload >

SSL Certificate File [   ] [Browse...]

(Upload)

SSL Certificate Signing Request
Note: If you destroy the CSR on the RIPC, there is no way to get it back! If you delete it by mistake, repeat the three steps.
Settings & Configuration Network

Network Settings Parameters

Parameter	Description
IP address	IP address in the usual dot notation.
Subnet mask	The net mask of the local network.
Gateway IP address	The gateway of the network.
1. DNS Server IP	IP address of the primary Domain Name Server in dot notation. This option may be left empty, however, the RIPC won't be able to perform name resolution.
2. DNS Server IP	IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server can't be contacted.
Enable Power Management Unit	If this option is enabled, access over the Power Management Unit is possible. For this reason, to ensure the best level of security, we recommend you disable this parameter.

(Note: Changing the network settings of the RIPC might result in lost connections.
If you change the settings remotely, be sure all the values are correct so that you will still be able to access the RIPC.)

NETWORK SETTINGS MENU

Remote Access Settings
While some parameters can be changed while Remote Access is running, others must be set in the Remote Access settings prior to activating it.

Remote Access Settings

Remote Access Options Table

Control	Description
Transmission Encoding	The Transmission Encoding setting allows you to change the image-encoding algorithm that is used to transmit the video data to the Remote Access window. With these settings, it is possible to optimize the speed of the remote screen depending on the number of parallel users and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.). Normal: The Standard Encoding algorithm, well-suited for many parallel users in a LAN environment. Typical applications generate traffic of up to 15Kbps. Compressed: The data stream between the RIPC and the Remote Access window will be additionally compressed to save bandwidth. The compression encoding is suited for a modem or ISDN environment. However, since the compression takes processing time on the RIPC itself, this encoding shouldn't be used when many parallel users want to access the RIPC at the same time.
Use Sun's Java Browser Plug-In	Instructs the web browser of your administration system to use the JVM (Java Virtual Machine) of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Access 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 already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with "YES". The download volume is around 11MB. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Access software is optimized for this JVM version and offers wider range of functionality when run in Sun's JVM. (Hint: If you are connected over a slow connection to the Internet, you can also pre-install the JVM on your administration machine. The software is available on the CD that is delivered along with the RIPC.)
Mouse Hot Key	Allows specifying a hot key combination that starts either the mouse synchronization process if pressed in Remote Access, or is used to leave the single mouse mode. The key codes are listed in Appendix C.
User-Defined Hot Keys	User-defined hot keys simulate keystrokes on the remote system that cannot be generated locally.

Users & Passwords

Upon delivery, each RIPC is pre-configured with a supervisor user called "administrator" having the password "belkin". IMPORTANT: Be sure to change the administrator-user password immediately after you have installed and initially accessed your RIPC.

User & Passwords Panel

The Figure above shows the User & Passwords panel of the RIPC's front end. Its use will be described in the table below and in the following text.

Description Users & Passwords Table

Field	Description
Existing Users	Select an existing user for modification or deletion. Once a user has been selected, click the "Lookup User" button to see complete user information.
New User Name	In order to create a new user, enter a new login name in this field. Th new name must not already exist as user. If it does, an error message will be displayed on top of the panel.
Full User Name	This is the full name of the login user.
Password	The password for the user name. It must be at least four characters lon
Confirm Password	Confirmation of the password above.
Group	Assign this user to one of the following groups: super ➤ users in this group have every possible permission to control the host system and the RIPC; administrators ➤ users assigned to this group can control the host system; and users ➤ this group has view permissions only.

The user management of the RIPC allows 25 different users. The following sections will describe how to add, delete, and modify users.

Add User
Fill out the fields "New user name", "Full user name", "Password", and "Confirm Password" as shown in the Users & Passwords panel. Alternatively, select the group of which the new user should become a member. Click the "Create User" button.

Delete User
Select a user in the "Existing users" field. Click the "Lookup" button. The complete user information will be shown. Click the "Delete User" button.

Modify User
Select a user in the "Existing users" field. Click the "Lookup" button to get all the user's information. All fields can

be modified as required. The old password is not displayed, but can be modified. If all changes are done, click the "Modify User" button.

Serial Port

The RIPC's Serial Settings allow you to specify which devices are connected to the serial port and how to use them. The options are listed and described in the table below.

Serial Port Settings Table

Function	Description
Modem	Allows access to the RIPC via modem; see Modem Settings below, for details.
Port Access 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 unit or a standard Telnet client to connect to the RIPC.

Serial Port Settings Menu

Modem Settings

The RIPC offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the RIPC's serial interface.

Logically, connecting to the RIPC using a telephone line means nothing more than building up a dedicated point-to-point connection from your RIPC computer to the RIPC. In other words, the RIPC acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the RIPC, be sure to configure your RIPC computer accordingly. For example, on Windows operating systems, you can configure a dial-up network connection, which defaults to the right settings like PPP. The modem settings are part of the Serial Settings panel (see Serial Port Settings Menu).

Modem Options Table

Parameter	Description
Serial Line Speed	The speed at which the RIPC communicates with the modem. Most modems today support the default value of 115200bps. If you are using an old modem and experience problems, try to reduce this speed.
Modem Init String	The initialization string used by the RIPC to initialize the modem. The default value will work with all current standard modems directly connected to a telephone line. If you have a special modem or the 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 giving a new string. Refer to the modem's manual about the AT command syntax.
Client IP Address	This IP address will be assigned to your RIPC computer during the PPP handshake. Since it is a point-to-point IP connection, virtually every IP address is possible but you must make sure it is not interferin with the IP settings of the RIPC and your RIPC computer. The default value will work in most cases.

Keyboard/Mouse Settings

The RIPC supports different keyboard and mouse models. The panel shown in the Keyboard/Mouse Settings Menu is used to adjust settings (see table below).

Keyboard/Mouse Options Table

Control	Description
Targeted KVM Port	Selects the KVM port to which the settings made belo will be applied. Choosing "Update" will display the current values for this port and select it for alteration of its settings.
Keyboard Model	Selects the keyboard model used on the remote host system.
Mouse Mode	Automatic ➤ uses the automatic mouse synchronization process; 1: n ➤ enacts direct scaling of mouse movements between the local and the remote pointer, so you can move the mouse even if it's not entirely synchronous
Reset Mouse/ Keyboard Emulation	This option will reset the RIPC's keyboard and mouse emulation for the host system. Use it if the keyboard or mouse seem to react irrationally. It's just like pulling out the keyboard and mouse connectors and plugging them in again.

Keyboard/Mouse Settings Menu

KVM Switches

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 RIPC, key combinations have to be defined for the ports.

The syntax to define a new hot key is as follows:

< keycode > [+| – [_] < keycode >]*

For example: Ctrl-Ctrl-A-Enter

or Ctrl+A-*1-Enter

Multiple key codes can be concatenated with a + or a – sign. The + sign builds key combinations; all keys will be pressed until a – sign or the end of the combination is encountered. In this case, all pressed keys will be released in reversed sequence. So the – sign builds single, separate key presses and releases. The _ (underscore) inserts a pause of user-definable length; more than one _ (underscore) may be concatenated. The duration of a single pause is set in milliseconds, using the appropriate option on the KVM settings page.

See Hot Key Table for a list of key codes that can be used as hot keys.

If the settings are correct, the KVM port can be switched using the KVM switching matrix on the RIPC's home page. The RIPC uses separate mouse synchronization settings and video settings for each port.

Note: It is still possible to apply KVM key combinations through Remote Access for switching KVM ports, however, in this case video and mouse synchronization settings will be shared among the ports and may unintentionally be exchanged for one of those ports.

Firmware

This section contains a summary of information about this RIPC and its current firmware, and allows you to reset the RIPC. This information is made available under the Maintenance Panel Menu.

APPENDIX A

Update Firmware

Flash upgrades allow you to obtain the latest firmware updates for your RIPC.

These updates ensure that your RIPC continues to work with the latest devices and computers. Firmware upgrades are free for the life of the RIPC. Visit **belkin.com** for upgrade information and support.

Firmware Upload Menu

RIPC Video Modes

Table B.1 lists the video modes the RIPC supports. Please use only these modes, and do not use custom video settings. If you do, your RIPC may not be able to detect them.

Table B.1 Unit Video Modes

Resolution (x,y)	Refresh Rates (Hz)
640×350	70, 85
640×400	56, 70, 85
640×480	60, 67, 72, 75, 85, 90, 100, 120
720×400	70, 85
800×600	56, 60, 70, 72, 75, 85, 90, 100
832×624	75
1024×768	60, 70, 72, 75, 85, 90, 100
1152×864	75
1152×870	75
1152×900	66, 76
1280×960	60
1280×1024	60

The Hot Key Table shows the key codes used to defines keystrokes. Please note that these key codes do not necessarily represent key characters that are used on international keyboards. They name a key on a standard 104-key PC keyboard with U.S. English language mapping. However, most modifier keys and other alphanumeric keys used for hot key purposes in application programs are on an identical position, no matter what language mapping you are using.

Some of the keys have aliases also, meaning they can be named by two key codes (separated by comma in the table).

Hot Key Table

For these commands…	…type these characters
Tilde	TILDE
Minus	– or MINUS
Equals	=or EQUALS
Semicolon	;
Apostrophe	'
Less than	<or LESS
Comma	,
Period	.
Slash	/ or SLASH
Backspace	BACK SPACE
Tab	TAB
Left bracket	[

Right bracket	]
Enter	ENTER
Caps Lock	CAPS LOCK
Back slash	\ or BACK SLASH
Left Shift, Shift	LSHIFT or SHIFT
Right Control	RCTRL
Right Shift	RSHIFT
Left Control or Control	LCTRL or CTRL
Left Alt or Alt	LALT or ALT
Space Bar	SPACE
Escape	ESCAPE or ESC
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7
F8	F8
F9	F9
F10	F10
F11	F11
F12	F12
Print Screen	PRINTSCREEN
Scroll Lock	SCROLL LOCK
Break	BREAK
Insert	INSERT
Home	HOME
Page Up	PAGE UP
Delete	DELETE
End	END
Page Down	PAGE DOWN
Up arrow	UP

Left arrow	LEFT
Down arrow	DOWN
Right arrow	RIGHT
Number Lock	NUM LOCK
0 on number pad	NUMPAD0
1 on number pad	NUMPAD1
2 on number pad	NUMPAD2
3 on number pad	NUMPAD3
4 on number pad	NUMPAD4
5 on number pad	NUMPAD5
6 on number pad	NUMPAD6
7 on number pad	NUMPAD7
8 on number pad	NUMPAD8
9 on number pad	NUMPAD9
Addition sign on number pad	NUMPADPLUS or NUMPAD PLUS
Division sign on number pad	NUMPAD/
Multiplication sign on number pad	NUMPADMUL or NUMPAD MUL
Minus sign on number pad	NUMPADMINUS or NUMPAD MINUS
Enter on number pad	NUMPADENTER
Windows	WINDOWS
Menu	MENU

GLOSSARY

ACPI
A specification that enables the operating system to implement power management and system configuration.

ATX
Advanced Technology Extended: A particular specification of a motherboard introduced by Intel® in 1995.

DHCP
Dynamic Host Configuration Protocol: Protocol for dynamically assigning IP configurations in local networks.

DNS
Domain Name System: Protocol used to locate computers on the Internet by their name.

FAQ
Frequently Asked Question

HTTP

Hypertext Transfer Protocol: The protocol used between web browsers and servers.

HTTP
Hypertext Transfer Protocol: The protocol used between web browsers and servers.

HTTPS
Hyper Text Transfer Protocol Secure: Secure version of HTTP.

LED
Light Emitting Diode

MIB
Management Information Base: Describes the structure of the management information that can be accessed via SNM

PS/2
The PS/2 device interface was developed by IBM® and is used by many mice and keyboards.

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

SSL
Secure Socket Layer: Encryption technology for the Internet used to provide secured data transmissions.

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

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

FAQs

Does the RIPC work with Belkin OmniView ENTERPRISE Quad-Bus Series KVM Switches?

Yes, it does.

Does the RIPC work with non-Belkin KVM switches?

Yes, the RIPC works with non-Belkin PS/2 KVM switches, however, be advised that degradation in performance may result if a lesser-quality KVM switch is used.

What operating systems does the RIPC support?

The RIPC supports Windows NT, 2000, and XP.

Can I use my RIPC with operating systems that are not based on Microsoft Windows?

Yes, you can use your RIPC with other platforms, however, only the keyboard and video are supported.

Does the RIPC put any strain on the servers?

No, the RIPC is a 100% hardware solution that does not require any additional software installed on servers.

TROUBLESHOOTING

The remote mouse doesn't work or is not synchronous.
Make sure the mouse settings match the mouse model.
The video quality is bad or the picture is grainy.
Try to correct the brightness and contrast settings until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.
Login fails.
Use the administrator account to log in and make sure your user name and password are correct.
The Remote Access window can't connect to the RIPC.
A firewall may be preventing access. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.
No connection can be established to the RIPC.
Check to ensure that the network connection is working in general (ping the IP address of the RIPC). If not, check network hardware.
Is the RIPC powered on? Check whether the IP address of the RIPC and all other IP-related settings are correct.
Verify that all the IP infrastructure of your LAN, such as routers, etc., is correctly configured. Without a ping functioning, the RIPC will not work.
Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the RIPC's system and not transmitted to the host.
Create a hot key command for this special function.
In the browser the RIPC pages are inconsistent or chaotic.
Make sure your browser cache settings are correct. Be especially careful that the cache settings are NOT set to "never check for newer pages". Otherwise, the RIPC pages may be loading from your browser cache and not from the card.

INFORMATION

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:
F1DE101G 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 F1DE101G, 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 Five-Year Product Warranty
Belkin Corporation warrants this product against defects in materials and workmanship for its warranty period. If a defect is discovered, Belkin will, at its option, repair or replace the product at no charge provided it is returned

during the warranty period, with transportation charges prepaid, to the authorized Belkin dealer from whom you purchased the product. Proof of purchase may be required.

This warranty does not apply if the product has been damaged by accident, abuse, misuse, or misapplication; if the product has been modified without the written permission of Belkin; or if any Belkin serial number has been removed or defaced.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. BELKIN SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, NCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No Belkin dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

BELKIN IS NOT RESPONSIBLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO, LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH BELKIN PRODUCTS.

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

BELKIN

®

belkin.com

Belkin Corporation
501 West Walnut Street
Compton • CA • 90220 • USA
Tel: 310.898.1100
Fax: 310.898.1111

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

Belkin Components B.V.
Starparc Building • Boeing Avenue 333
1119 PH Schiphol-Rijk • The Netherlands
Tel: +31 (0) 20 654 7300
Fax: +31 (0) 20 654 7349

Belkin, Ltd.
7 Bowen Crescent • West Gosford
NSW 2250 • Australia
Tel: +61 (0) 2 4372 8600
Fax: +61 (0) 2 4372 8603

Belkin Tech Support
US: 310.898.1100 ext. 2263
800.223.5546 ext. 2263
Europe: 00 800 223 55 460
Australia: 1800 666 040

P74238-A

https://manual-hub.com/

Documents / Resources

 BELKIN F1DE101G OmniView Remote IP Console [pdf] User Manual
F1DE101G OmniView Remote IP Console, F1DE101G, OmniView Remote IP Console, Remote IP Console, IP Console, Console

References

- 🟢 **Mobile & Computer Accessory Products | Belkin US**
- ᴹᴴ **Search - Manual-Hub.com**