BELKIN®

OmniView® SMB
Remote IP Device

User Manual

F1DP101M

Table of Contents

Table of Contents

Introduction

Congratulations and thank you for purchasing the Belkin OmniView SMB Remote IP Device (the IP Device). This IP Device provides a simple, easy-to-use, remote server management solution for small- to medium-size businesses. When connected to a KVM switch or server, the IP Device allows you to access and control your servers over the Internet via a standard web browser. This round-the-clock access enables you to troubleshoot servers faster and more efficiently, reducing server downtime and service costs.

This User Manual provides all the details you'll need to install and operate your new IP Device, in addition to expert troubleshooting advice—in the unlikely event of a problem. For quick and easy installation, please refer to the Quick Installation Guide included in your packaging.

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

OmniView SMB Remote IP Device

Rack-Mount Brackets with Screws

One 5V DC, 2A Power Supply

PS/2 Cable Kit

RS232 Cross Cable

User Manual

Quick Installation Guide

Overview

Features

• **High-Performance Remote Access**
The IP Device allows you to access and control a KVM switch configuration
and all connected servers from any remote console over a TCP/IP connection.
The IP Device can also be set up to provide remote access to an individual
computer or server. The IP Device provides superior video quality and mouse
control, giving you the same user experience as if you were accessing your
servers locally.

• **Web-Browser Based**
The IP Device allows you to access your KVM switch and all connected servers
from any computer connected to the LAN, WAN, or Internet using Microsoft
Internet Explorer version 6.0 or higher.

• **Universal Compatibility**
The IP Device seamlessly adds remote, out-of-band access to any KVM switch
or individual server with PS/2-console connections. When connected to a
daisy-chained KVM configuration, the IP Device provides remote access to all
connected servers.

• **BIOS-Level Access**
The IP Device allows you to remotely access the basic input/output system
(BIOS) of your servers to make changes and perform reboots, regardless of
network connectivity or server condition.

• **User-Friendly Interface**
The web-based interface allows you to set up and change the IP Device's
functions quickly and easily through your web browser, without having to install
additional software onto your servers.

• **Remote Serial Access**
The IP Device provides support for one serial device, such as a managed
power distribution unit (PDU), so you can remotely perform hard reboots of
your servers.

• **Enhanced Security**
The IP Device provides 128-bit Secure Sockets Layer (SSL) encryption and
password protection to prevent unauthorized access to your servers and
protect data transferred over the Internet.

Overview

- **Digital Collaboration**
  The IP Device enables one user to access and control servers remotely over the Internet. Up to eight users can also simultaneously view remote sessions to share technical expertise and troubleshoot servers collaboratively.

- **Video Resolution**
  The IP Device supports video resolutions of up to 1600x1200@75Hz for both local and remote consoles.

- **Firmware Updates**
  Flash upgrades allow you to obtain the latest firmware updates for your IP Device. These firmware updates ensure that the IP Device is compatible with the latest devices and hardware and are free for the life of the IP Device. Visit www.belkin.com for upgrade information and support.

Equipment Requirements

Cables

To connect the IP Device to your KVM switch or individual server, the included PS/2 KVM Cable Kit is required.
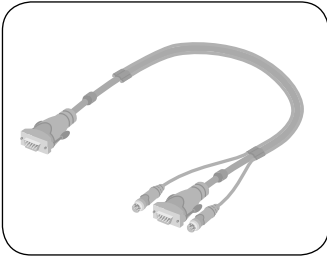
To connect the IP Device to your local area network, you will need to locate a network cable with an RJ45 connector.

System Requirements

Host Computer Operating-System (OS) Platforms

The SMB Remote IP Device is compatible with CPUs running on, but not limited to, the following OS platforms:

• Windows® NT®, 2000, XP, Server 2003, or Vista™

• Microsoft® DOS 5.x and above

• Red Hat® Linux® 8.x and above

• Sun™*

• Novell® 5.x

• Solaris™ 8.x and above*

*Adapters may be required.

KVM Switches

The IP Device is compatible with the following Belkin KVM Switches:

• OmniView Quad-Bus Series

• OmniView SMB Series

• OmniView PRO2 Series

• OmniView SE Plus Series

The IP Device is also compatible with KVM switches with PS/2-console ports from other manufacturers including, but not limited to, the following:

• Avocent® Corporation	• Daxten
• ATEN	• Tripp Lite
• Raritan®	• NTI
• Black Box®	• Adder
• Compaq®	• D-Link®
• HP®	• CCC Networks
• IBM®	• Rextron
• Minicom	• Emine
• Cybex	• KVM Partnership
• Rose	

System Requirements

Keyboards

• PS/2-compatible

Mice

• PS/2-compatible with 2, 3, 4, or 5 buttons

• PS/2-compatible wireless and optical mice

Monitors

• CRT and LCD (with VGA support)

Remote-Console Software

The SMB Remote IP Device may be accessed remotely over a TCP/IP connection from computers using the following web browsers and OS platforms:
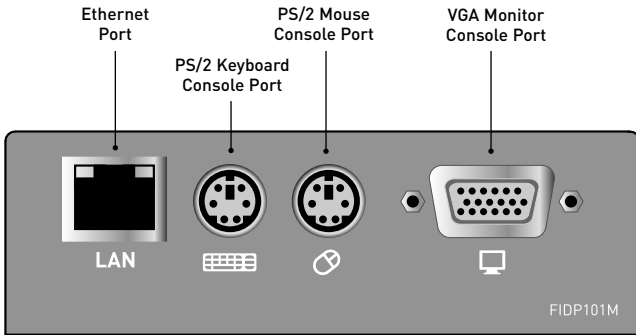
• Microsoft Internet Explorer 6.0 and above with ActiveX® support

• Windows 2000, XP, or Server 2003

• Windows Vista**

**Internet Explorer® must be run under administrator mode due to extra security for ActiveX plug-ins under Windows Vista.

Unit Display Diagrams

Front View

Ethernet
Port

PS/2 Keyboard
Console Port

PS/2 Mouse
Console Port

VGA Monitor
Console Port

LAN

FIDP101M

Back View

KVM/Server
Port

Serial-Device Port

Power
Jack

Go Local/
Reset Button

KVM In

Serial

⊕-ⓒ-⊖
3.3V/2A

Go Local

Power

Power
Status LED

Overview
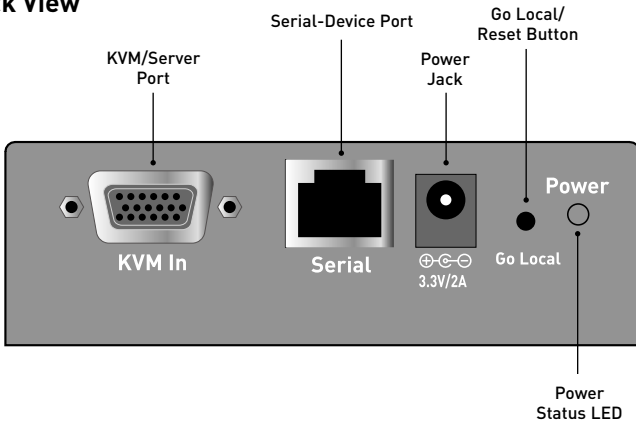
Specifications

|	
Part No.:	F1DP101M
No. of Users Supported:	1 digital or 1 local
Enclosure:	Aluminum
Power Requirements:	3.3V DC, 1.3A power adapter (center-pin negative)
Video-Resolution Support:	Local analog port: Up to 1600x1200 @ 75Hz
	Digital port: Up to 1600x1200 @ 75Hz
Console Keyboard Emulation:	PS/2
Console Mouse Emulation:	PS/2
Console Keyboard Input:	MiniDIN6 (PS/2)
Console Mouse Input:	MiniDIN6 (PS/2)
Console Monitor Port:	HDDB15 female (VGA)
KVM/Server Port:	HDDB15 female*
Ethernet Port:	RJ45 (10/100Base-T connection)
Security:	128-bit SSL encryption
Typical Bandwidth:	0.31Mbps**
Serial-Device Port:	RJ45
Power Connection:	IEC
Port Selectors:	8 and 16 respectively for 8- and 16-port models
LED Indicators:	8 and 16 respectively for 8- and 16-port models
Dimensions:	1.1 x 4.1 x 3.1 in. (28 x 104 x 79mm)
Weight:	0.5 lbs. (0.2kg)
Operating Temp:	32° to 104° F (0° to 40° C)
Storage Temp:	-40° to 158° F (-40° to 70° C)
Humidity:	0-80% RH, non-condensing
Warranty:	2 years

*The IP Device may be connected to any KVM switch or individual server with PS/2 keyboard and mouse console ports.

**Typical bandwidth is defined as typical "non-intensive" administrative use at 16-bit color, 1024x768 resolution.

Note: Specifications are subject to change without notice.

Hardware Installation

Pre-Configuration
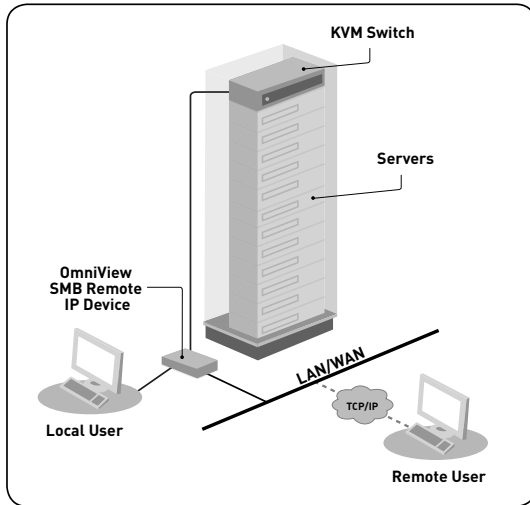
(Typical configuration)

Where to place the IP Device:

The IP Device includes a mounting bracket and is designed for stand-alone or 0U rack-mount installation.

Consider the following when deciding where to place the Switch:

• whether or not you intend to use the included bracket

• the lengths of the cables attached to your keyboard, monitor, and mouse

• the location of your KVM switch or server in relation to your console

• the lengths of the cables you use to connect your IP Device to the KVM switch or server

Warning: Avoid placing cables near fluorescent lights, air-conditioning equipment, or machines that create electrical noise (e.g., vacuum cleaners).

You are now ready to begin installation of your IP Device. The following sections (pages 10–14) provide complete instructions for the hardware setup of the IP Device to a KVM switch or individual server.

Hardware Installation

Step 1   Mounting the IP Device (optional)

Note: Before you begin, locate the MAC address and device number on the bottom of the IP Device. You will need these numbers later in the installation process, so it is highly recommended that you record these numbers below before mounting the IP Device to your rack.

MAC Address	Device Number

1.1   Attach the included mounting bracket to either side of the IP Device. (Refer to diagram below.)

1.2   Mount the IP Device to the rear post of your rack. (Refer to diagram below.)

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

Step 2   Connecting the Console to the IP Device

2.1 Connect your monitor VGA cable to the monitor port on the front of the IP Device labeled "▯." (Refer to diagram below.)

2.2 Connect your keyboard and mouse PS/2 cables to the keyboard and mouse ports on the front of the IP Device. (Refer to diagram below.)

Hardware Installation

2.3 Locate and connect a cable from your local area network to the RJ45 Ethernet port on the back of the IP Device. (Refer to diagram below.)

Step 3   Connecting the KVM Switch or Server to the IP Device

3.1 Make sure your KVM switch and all connected servers are powered off.

3.2 Using the included KVM cable kit, connect the single DB15 connector to the "KVM In" port on the back of the IP Device. (Refer to diagram below.)

3.3 Using the other end of the cable kit, connect the VGA and PS/2 cables to the console monitor, keyboard, and mouse ports on your KVM switch or server. (Refer to diagrams below.)
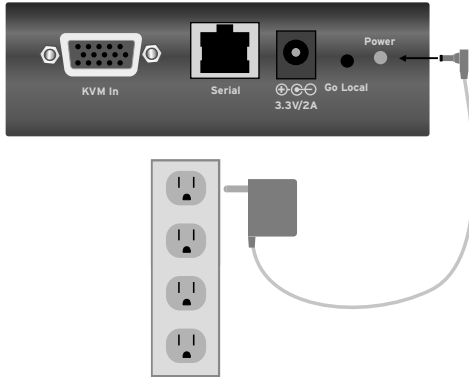
Connecting to a KVM Switch

Connecting to a Server

Step 4   Powering Up the Systems

4.1 Attach the power adapter to the IP Device and connect it to a
power source to power up the IP Device. (Refer to diagram below.)

4.2 Power on the KVM switch or server connected to the IP Device. The IP
Device emulates both a mouse and a keyboard on each port, and allows
your KVM switch or server to boot normally.

4.3 Power on all servers connected to your KVM switch.

4.4 Check that the local keyboard, monitor, and mouse are
working normally.

1

2

3

section

4

5

6

7

8

9

Remote Installation

Initial Settings

The following section provides instructions for setting the IP address for the OmniView SMB Remote IP Device.

Step 1   Identifying the IP Address

Once your IP Device has been connected to your network and is powered up, a Dynamic Host Configuration Protocol (DHCP) server on your network will automatically assign the IP Device an IP address, gateway address, and subnet mask.

To identify the IP address on your network, use the MAC address or unique device number located on the back of the IP Device. If no DHCP server is found on your network, the IP Device will boot with the following static IP address: 192.168.2.155.

If you want to connect more than one IP Device to the same network and there is no DHCP server available, connect each IP Device to your network one at a time and change the static IP address of each unit before connecting the next unit.

Note: If a DHCP server later becomes available on your network, the IP Device will take a new IP address from the DHCP server. To keep the original static IP address, you will need to disable DHCP (see page 19).

Remote Installation

Step 2   Logging into the Web Interface

To log into the web interface:

1. Open your web browser (Internet Explorer version 6.0 or above is required). **If you are using Windows Vista, you must run Internet Explorer in administrator mode. In order to run Internet Explorer in administrator mode, right-click on Internet Explorer and select "Run as Administrator".**

2. Type in the IP Device's IP address in the address field, using this format: **https://192.168.2.155/config**. The login page will appear (see Fig. 1). Bookmark the page for easy reference.

    Note: HTTPS is used for communication over an encrypted secure socket layer (SSL) mechanism.

BELKIN   Configuration

Username   admin

Password   •••••••••

Login

Fig. 1 Login Page

3. Type in the following default user name and password (case-sensitive):

User	Password
admin	SMBremote

Remote Installation

4. Click [Login]. The web interface will open at the Network-Configuration page (see Fig. 2).

Fig. 2 Network-Configuration Page

Remote Installation
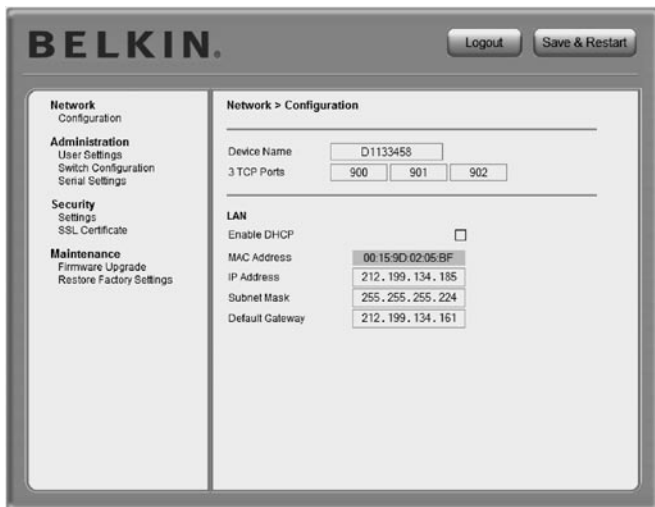
Step 3   Network Configuration

When first connecting to the IP Device's HTTPS configuration page, two browser security warnings may appear. Click "Yes" on both warnings.

Note: The first security warning only occurs once per client machine. This is when the Belkin root certificate is installed. The second warning can be avoided by adding a line to your Windows "hosts" file (typically at **\winnt\system32\ drivers\etc\hosts**—edit using Notepad). The line format should be "IP address-any-name.kvm.net".
(For example: **192.168.2.155 BelkinSMB.kvm.net**.)

Device Name	D1133458		
3 TCP Ports	900	901	902

Device Name

Type in a name you would like to assign the IP Device. The default device name consists of the letter "D" followed by the 7-digit device number located on the back of the IP Device.

Three TCP Ports

Choose three Transmission Control Protocol (TCP) ports, and type in the provided fields. The default ports are 900, 901, and 902. This is suitable for the majority of installations. However, you can enter any value for TCP ports, from 800 up to 65535. This applies to all three fields.

Note: Your firewall or router security access list must enable inbound communication through the selected TCP ports for the IP Device's address. Ports 80 and 443 are used for standard Web communication and should be open. For client-computer access from a secured LAN, the selected ports should be open for outbound communication.

Remote Installation

LAN	
Enable DHCP	☐
MAC Address	00:15:9D:02:01:51
IP Address	212.199.134.184
Subnet Mask	255.255.255.224
Default Gateway	212.199.134.161

Enable DHCP

When this box is checked (default setting), a DHCP server on your network is enabled to assign an IP address to the IP Device. When this box is not checked (recommended), you can assign a static IP address to the IP Device.

Set a Static IP

If you choose not to use DHCP, uncheck the "Enable DHCP" box, then enter the IP address, subnet mask, and default gateway for LAN, as provided by your network administrator.

Note: If you enter a static IP address without unchecking the "Enable DHCP" box, the static IP address will not work and DHCP will remain enabled.

Note: Where you have access to the server, your configured (or default) device name will appear on the DHCP server's list, making it easy to locate.

Remote Installation

Step 4   User Settings

In the User-Profile page, you can create and edit up to 25 different user accounts. To open the page, click "User Settings" under "Administration" in the far-left menu (see Fig. 3).
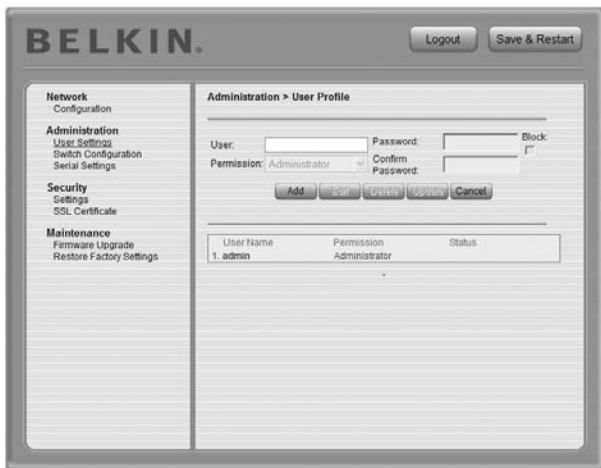
Fig. 3 User-Profile Page

There are three levels of user access:

Administrator

An administrator has unrestricted access to all windows and settings and can "take over" any active session (see page 30 for more details). An administrator can change the name and password of all users.

User

A user can access and control target servers, but cannot use or have access to the following:

• Advanced mouse settings

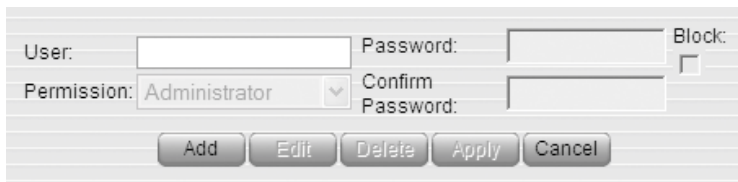• Web configuration interface (found at https://*IP Address*/config)

Remote Installation

View Only

A "view only" user is only allowed to view the screen of the target server without keyboard and mouse control. Only limited options appear, such as "disconnect". A View Only icon will appear on the viewer's local mouse pointer to indicate this status.

Note: Only one administrator can log in to the Configuration page at a time. The IP Device can support up to eight simultaneous viewers to a remote session, but only the administrator can take control of the server.


To add a new user:

1. Click [Add] and type in a user name and password. The password must be at least six characters (letter or numbers) and must not include the user name, even if other characters are added. Depending on the security level chosen, the user name and password parameters are different. (See page 26 for more details.)

2. Select the permission type from the Permission box.

3. Click [Apply] to save the changes. The new user will appear in the list of users.

Remote Installation

To edit a user:

1. Select the user from the list.

2. Click [Edit]. You can now change all the available parameters—user name, permission type, and password.

3. Click [Apply] to save the changes.

Note: For security, you should change the password for the default "admin" user name.

To delete a user:

1. Select the user from the list.

2. Click [Delete].

3. Click [Apply] to save the changes.

Blocking a standard user and "View Only" user

An alternative to deleting a user is "blocking." This means that the user's name and password remained stored, but the user is unable to access the system.

To block a user:

1. Select the user from the list.

2. Check the "Block" box.

3. Click [Apply] to save the changes.

Note: For security purposes, we recommend that you delete administrator accounts and not use this blocking feature.

Step 5   Switch Configuration

When a KVM switch is connected to the IP Device, you must specify the manufacturer and model of the switch in the "Switch Configuration" section.

The Switch-Configuration page allows you to specify the KVM Switches attached to the IP Device. To open the page, click "Switch Configuration" under "Administration" in the far-left column (see Fig. 4).


Fig. 4 Switch-Configuration Page

Note: By default, the Switch-Configuration page assumes that the IP Device is connected to a single server. The page displays a single server-name field.

Remote Installation

To specify and name servers:

1. Click ⧉ next to the "Manufacturer" and "Model" fields field and select the KVM-switch configuration that best suits your configuration.

2. Click [Apply]. The number of possible connected servers will appear in the Server Name section.

3. Change the name of each connected server by highlighting the server and typing in a new name.

4. Click [Apply]. to save the changes.

Note: You will need to change the name of every server you want to access. Server names left as "**UNUSED**" cannot be accessed.

Installing new Switch-Definition Files (SDFs)

If your KVM switch-configuration type is not listed in the drop-down list, contact Belkin Technical Support at (800) 282-2355 to request an updated SDF with the desired KVM-configuration list.

To install the SDF:

1. Load the file onto the client computer.

2. Click [Browse...] to locate the new SDF.

3. Click "Install" to update the Switch with the new file.

Note: If you change the hot-key sequence in the KVM Switch to "Print Screen", "Ctrl", or "F12", you must load a new switch-definition file (SDF) for the corresponding hot key. The SDF can be downloaded from www.belkin.com/support.

Step 6   Serial Settings

The SMB Remote IP Device supports one serial device, which can be attached using the included serial cable. The serial device can be accessed remotely via the IP Device's VT100 serial terminal emulation.

If you have a serial device connected to the Switch, such as a power distribution unit (PDU), you must configure the serial (RS232) settings. To open the Serial-Settings page, click "Serial Settings" under "Administration" in the far-left menu (see Fig. 5).

Fig. 5 Serial-Settings Page

To configure your serial device:

1.   Type in the name of the serial device.

2.   Using the drop-down menus, select the correct baud rate, parity, and data-and stop-bit parameters for the device.

3.   Check the "Show" box. This will make the serial device appear in the list of servers and devices that can be accessed through the quick-access toolbar.

Remote Installation

Step 7   Security Settings

The Security-Settings page allows you to configure security features for the IP Device. To open the Security-Settings page, click "Settings" under "Security" in the far-left menu (see Fig. 6).

Fig. 6 Security-Settings Page

You can configure the following security features:

Account Blocking

Specify the number of invalid login attempts allowed before the user is locked out.

Password Policy

Choose between a standard- or high-security password policy. The table below shows the parameters of the two options available. Check the box to enable the high-security password policy, or leave unchecked to enable the standard-security policy.

Standard-Security Password	High-Security Password
6 characters or more	8 characters or more; must include at least 1 digit and 1 uppercase letter, and 1 of the following "special" characters: !@#$%^&*()_-+={}]"':;?/><
Must not include the user name	Must not include the user name

Remote Installation

Idle Timeout

Select the maximum time allowed for inactivity before the user is disconnected from the remote session. Choose "No Timeout" to disable the Idle Timeout feature. By default, the timeout inactivity period is set to 10 minutes.

SSL Certificate

You can install your company's own SSL certificate to protect data transferred over the Internet between your servers and remote console. To open the SSL-Certificate page, click "SSL Certificate" under "Security" in the far-left menu (see Fig. 7).

Fig. 7 SSL-Certificate Page

To install an SSL certificate:

1. Click Browse... next to the Certificate-File field to locate the *.cer file.

2. Click Browse... next to the Private-File field to locate the private-key file.

3. Type the "private key" password in the Key-Password field.

4. Click Save & Restart to complete and upload the files.

Maintenance

Firmware Upgrade

You can upgrade the IP Device's firmware to take advantage of new features or fixes as they become available. Visit www.belkin.com/support to check for firmware updates.

To upgrade firmware:

1. Download and save the firmware file on the client computer.

2. Select "Firmware Upgrade" under "Maintenance" in the far-left menu of the web interface. The Firmware-Upgrade page will appear (see Fig. 8).

3. Click Browse to locate and install the firmware file.

4. Click "Start Upgrade".

5. Once the upgrade is complete, click "Reboot" immediately. The unit should reboot. After about 30 seconds, the Login page should appear.

Fig. 8 Firmware-Upgrade Page

Note: Depending on the type of firmware upgrade, the following settings may be erased: user settings, switch-configuration settings, mouse and video adjustments, and RS232 serial-device settings. For more information, refer to the firmware release notes. The network settings will remain intact.

Restore Factory Settings

You can restore the IP Device to its original factory settings. This restores the original parameters, resetting all the information added by the administrators, including: network settings, servers, switches, users, and passwords. You also have the option to preserve network settings, as explained below.

WARNING! Once data has been reset, it cannot be retrieved.

To restore factory settings:

1. Select "Restore Factory Settings" in the far-left menu. The Restore-Factory-Settings page will appear (see Fig. 9).

2. Check the Preserve-Network-Settings box if you would like to preserve the network settings.

3. Click Restore .

Fig. 9 Restore-Factory-Settings Page

Logging Out

To exit the Configuration page and close the session, click Logout .

Only one administrator can log into the Configuration area at a time. An idle timeout of 30 minutes terminates the session.

Using the Remote IP Device

Starting a Remote Session

To start a remote session:

1. At a client computer, open Internet Explorer (version 6.0 or above) and type the IP Device's IP address (**https:// IP address**).

Note: If you are using Windows Vista, you must run Internet Explorer in administrator mode. In order to run Internet Explorer in administrator mode, right-click on Internet Explorer and select "Run as administrator".

2. When the Login screen appears, type in your user name and password, and click Login . By default, the user name is "admin" and the password is "SMBremote" (both are case-sensitive).

3. If it is your first time connecting, you will be prompted to install the Belkin certificate and the Microsoft ActiveX control. You must have administrator privileges on your client computer to install the ActiveX control.

4. The screen of the currently selected server on the IP Device's will appear. The quick-access toolbar will also appear on the right side of the screen.

5. If the target server is currently being accessed by another user, a dialog box will appear, giving you the option to "Take Over", "View Only", or "Cancel" (see Fig. 10). Select one of these options. An **administrator** has the option to take control over any server. A **user** only has this option when the current session is run by another user, but not by an **administrator**. The dialog box will not appear for a "**view only**" **user**.

Fig. 10 Server-Access Dialog Box

Full-Screen Mode

You can work on the target server in full-screen mode, just as if you were connected to the server locally.

To work in full-screen mode:

1. Ensure that the client computer has the same screen resolution as the target server.

2. Press "F11". The Internet Explorer window will disappear, leaving the Internet Explorer menu bar at the top.

3. Right-click the Internet Explorer menu bar and check "Auto-Hide". The Internet Explorer menu bar will disappear and you will be in full-screen mode (see Fig. 11).

4. To exit full-screen mode, press "F11", or move your cursor to the top of the window to display the Internet Explorer toolbar and click the "Restore" button.

Fig. 11 Example of Full-Screen Mode

Using the Quick-Access Toolbar

The quick-access toolbar provides an easy method for changing settings and switching servers (see Fig. 12).

Fig. 12 Quick-Access Toolbar

Icon	Function
	Minimize or maximize the toolbar
	Disconnect the remote session
	Configure the mouse and change settings
	Configure the keyboard and change settings
	Adjust the video settings
	Adjust the bandwidth settings
	Select which server to access
	Hide or display the toolbar; right-click to open additional features

Moving or Hiding the Quick-Access Toolbar

The quick-access toolbar can be dragged and placed anywhere on the browser's screen. To hide the toolbar, double-click ▶⊙ or press "F9". To display the toolbar, repeat the same action. To minimize or maximize the toolbar, click ‹ .

Disconnecting the Remote Session

To disconnect the session, click ⊠. You may close the browser after you disconnect.

Mouse Configuration and Settings

Mouse-Pointer Alignment

When working remotely at the client computer, two mouse pointers will appear: one for the client computer and one for the target server. The client computer's mouse pointer will appear on top of the target server's. The mouse pointers should be synchronized (aligned). If they are not synchronized, follow the instructions below.

To align mouse pointers:

1. In the quick-access toolbar, click 🖱.

2. Select "Align" or press "Ctrl+M".
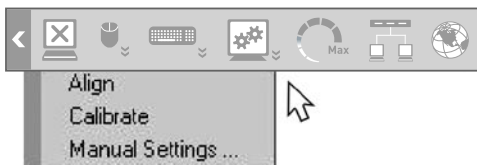
Mouse-Pointer Calibration

(Note: This option is not necessary for Windows operating systems.)

A target server may have a different mouse-pointer speed than the client computer. Calibration automatically discovers the mouse speed of the target server and aligns the two pointers. When you calibrate pointers, the IP Device saves the alignment, so calibration is only needed once per target server.

To calibrate mouse pointers:

1. In the quick-access toolbar, click 🖱.

2. Select "Calibrate".

Note: If the video-noise level is above zero, calibration may not work properly. Go to "Video Adjustment" and try to eliminate the noise by pressing "Audio Video Adjust", or by adjusting the bars in "Manual Video Adjust", then perform the mouse calibration again.

Manual Settings

You must manually synchronize the mouse pointers if:

• the mouse setting on the target server was ever changed, or

• the operating system on the target server is Windows 2000, Linux, Novell®, SCO UNIX, or Sun Solaris™.

To manually synchronize mouse pointers:

1. In the quick-access toolbar, click 🖱.

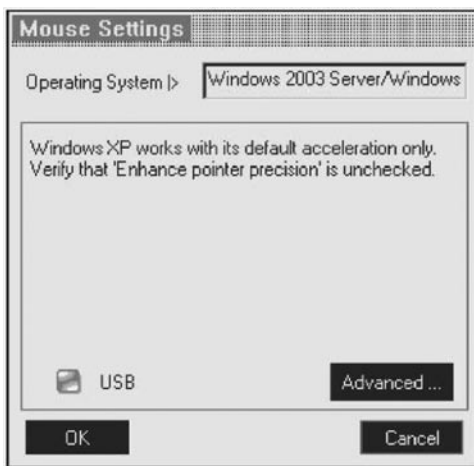**2.** Select "Manual Settings". The Mouse-Settings box will appear (see Fig. 13).

Fig. 13 Mouse-Settings Box

3. Select the target server's operating system and click "OK". Instructions and sliders will appear.

4. Follow the instructions and set any relevant sliders to the same values as set in the target server's mouse properties.

Examples: For servers running on Windows XP, go to the Mouse settings in the Control Panel and uncheck "Enhance pointer precision" (see Fig. 14).
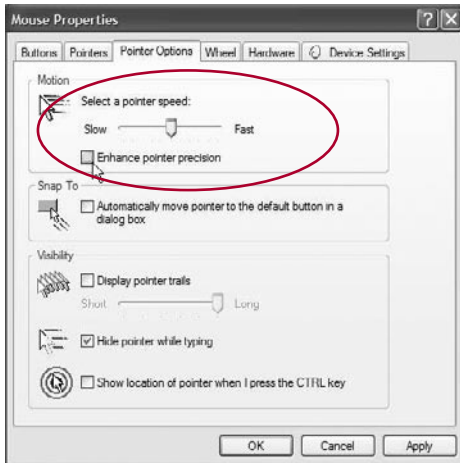

Fig. 14 Mouse-Pointer Options (Windows XP)

For servers running on Windows NT, if mouse properties were ever changed—even if they were returned to their original state—uncheck "Default".

5. Click "OK". The mouse pointers should now be synchronized.

Advanced-Mouse Emulation

In the Advanced-Mouse settings, you can set the type of mouse you would like the IP Device to emulate.

Note: Belkin recommends that you <u>NOT</u> change the advanced settings unless there is erratic mouse behavior (i.e., if the mouse is making random clicks and jumping arbitrarily around the screen).

To change the mouse-emulation settings:

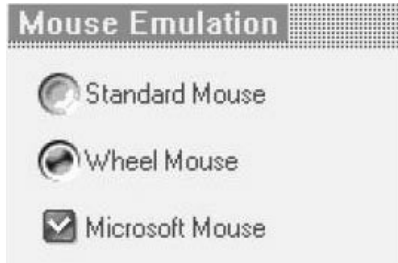**1.** Click Advanced... . The Mouse-Emulation box will appear (see Fig. 15).

Fig. 15 Mouse-Emulation Box

2. Select the type of mouse physically connected to the local console port on the IP Device.

3. In the Max Rate box, choose the maximum mouse-report rate. For Sun Solaris systems, the default rate is 20 in order to support older Sun versions.

4. Click "OK".

1

2

3

4

5 section

6

7

8

9

Keyboard Configuration and Settings

You can define and transmit a keyboard sequence directly to the target server, without affecting the client computer.

To transmit a keyboard sequence:

1. In the quick-access toolbar, click ▭.

2. Select a key sequence to transmit to the target server.

For example, if you select the "Ctrl-Alt-Del" keyboard sequence for the target server, it will allow you to initiate the server's shutdown/login process from your client computer.

To add a keyboard sequence:

1. In the quick-access toolbar, click ▭.

2. Click "Add/Remove". The Special-Key-Manager box will appear (see Fig. 16).
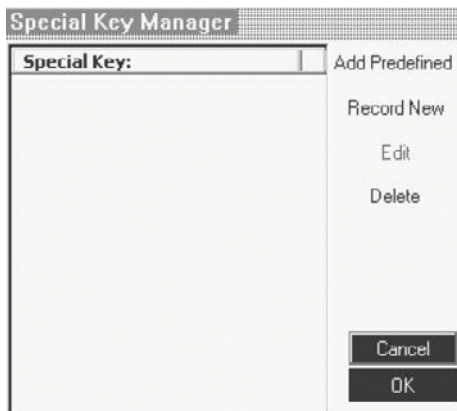
Fig. 16 Special-Key-Manager Box

3. Click "Add Predefined". A list of sequences will appear.

4. Select the desired sequence and click "OK". The sequence will appear in the Special-Key-Manager box.

5. Click "OK". The sequence will now appear in the Keyboard-Key-Sequence list.

To record a keyboard sequence:

1. In the quick-access toolbar, click ⌨.

2. Click "Add/Remove". The Special-Key-Manager box will appear.

3. Click "Record New". The Add-Special-Key box will appear (see Fig. 17).

4. Assign a name to the key sequence in the Label box.

5. Click "Start Recording", then click your mouse cursor on the recording window.

6. Press the desired keys. The keys will appear in the box.

7. Click "Stop Recording".

8. Click "OK" to complete and save the sequence.

Fig. 17 Add-Special-Key Box

Video Configuration and Settings

Refresh

You may need to refresh the video image when changing the display attributes of a target server.

To refresh the video settings:

1. In the quick-access toolbar, click 🖳.

2. Select "Refresh" or press "Crl+R".

Manual Video Adjust

You may want to manually adjust video to fine-tune the target-server video settings, to adapt to a noisy environment or a non-standard VGA signal, or when using a full-screen DOS/CLI mode.

To adjust the video manually:

1. In the quick-access toolbar, click 🖳.

2. Select "Manual video adjust". A slider bar will appear (see Fig. 18). A red frame will also appear around the screen. This represents the screen area according to the server's screen resolution.

3. Move the sliders to adjust and change the displayed image. Click in the area of the sliders for fine-tuning.

- **Brightness/Contrast**—adjusts the brightness and contrast of the displayed image
- **Horizontal Offset**—defines the starting position of each line on the displayed image
- **Vertical Offset**—defines the vertical starting position of the display image
- **Phase**—defines the point at which each pixel is sampled
- **Noise Level**—represents the video noise when a static screen is displayed
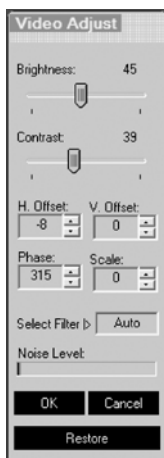
Fig. 18 Manual Video-Adjust Bar

Auto Video Adjust

To adjust the video automatically:

1. Open Internet Explorer (or similar) in the background.

2. In the quick-access toolbar, click [icon].

3. Select "Auto video adjust".

The process will take a few seconds. If the process runs for more than three seconds, there may be an abnormal noise level. Check the video cable and verify that no dynamic-video application is running on the target server's desktop.

Perform this procedure where necessary for each target server or new screen resolution.

1

2

3

4

5 section

6

7

8

9

Performance Settings (Bandwidth)

You can adjust the bandwidth settings on the IP Device to give you the desired compression and color-support levels for your remote sessions.

To change the bandwidth settings:

1. In the quick-access toolbar, click on ⬤. The Performance-Settings box will appear (see Fig. 19).
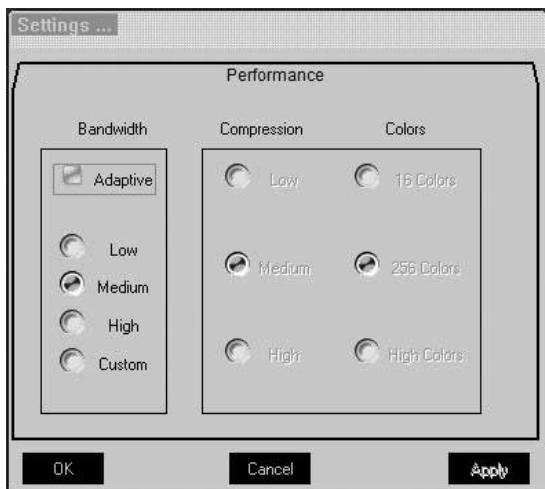
Fig. 19 Performance-Settings Box

2. Select one of the following bandwidth options:
   • **Adaptive—** Automatically adapts to the best compression and colors based on activity.
   • **Low—** Provides high compression and 16-color support.
   • **Medium—** Provides medium compression and 256-color support. Medium is recommended when accessing the Switch over an Internet connection.
   • **High—** Provides low compression and high, 16-bit color support. This setting provides optimal performance when working on a LAN.
   • **Custom—** Allows you to select your own compression and color-support levels. Choose between Low, Medium, and High compression, and 16-, 256-, and High (16-bit) color support.
3. When finished, click "OK" to save the setting. The screen of the last accessed target server will appear.

Selecting a Server

The quick-access toolbar allows you to easily select and switch to any server connected to the Switch or daisy-chain configuration.

To connect to a different server:

1. In the quick-access toolbar, click 🖥 or right-click. A list of connected servers will appear (see Fig. 20). If a serial device is connected to the IP Device, it will also appear on the list.

2. Select the desired server or serial device. The screen of the server or the serial-device window will appear.
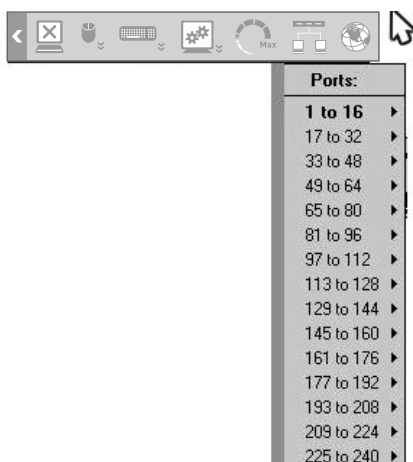
Fig. 20 Server-Selection Menu

Note: If security is enabled on the KVM switch, remote switching will not be allowed through the quick-access toolbar.

Additional Features

When you right-click [icon] in the quick-access toolbar, a menu will appear. From this menu you can access your connected servers. The menu also provides the following features:

- **Disconnect—**Disconnects the remote session.

- **About—**Verifies the current version of software/firmware of your IP Device.

- **Local Settings—**Opens the Client-Configuration box.

- **Pointer Type—**Lets you change the client-computer mouse pointer to appear as a dot, or to not appear at all.

- **Hide Toolbar—**Hides the quick-access toolbar starting with the next remote session. To toggle the toolbar on and off, press "F9".

- **Full-Screen Mode—**Makes the screen appear in full-screen mode starting with the next remote session. To toggle the full-screen mode on and off, press "F11".

Using the Remote IP Device

Restoring Factory Defaults

The "Restore Factory Settings" section on page 29 explains how to restore factory settings from the web interface. When you cannot access the system (you have forgotten the user name, IP address, or password), you can restore factory defaults from the IP Device.

To restore factory defaults:

1. Press and hold down the "Go-Local" button on the back of the IP Device for five seconds while powering up the IP Device. The IP Device will boot up in safe mode.

2. Wait 30 seconds for the IP Device to reboot.

3. Log in with the default IP address of the unit:
    http://192.168.2.155/config
    The blank login screen will appear (no background picture).

    Note: Do not start the IP address with **https**.

4. Type in the following default user name and password (case-sensitive), and click "Login". This user name and password only work immediately after the reset procedure described above.

Safe-Mode User	Safe-Mode Password
admin	SAFEmode

5. From the menu, select "Restore Factory Settings". A warning will appear advising you that all device data will be erased.

6. Click "Restore". The factory defaults will be restored. When the process finishes, you will be prompted to reboot.

7. Click "Reboot" to restart the IP Device.

Frequently Asked Questions

What operating systems does the IP Device support?

The IP Device will support operating systems that run on a PS/2 platform. Operating systems include, but are not limited to, DOS; Windows 2000, NT, XP, 2003 Server; Sun; Solaris; Novell; and Linux.

Does the Switch support Microsoft IntelliMouse®?

The IP Device supports mice from Microsoft, Logitech®, Kensington®, etc., and Belkin. Please contact Belkin Technical Support for compatibility issues you may experience.

What is the maximum video resolution that the IP Device supports?

The advanced video circuit in the IP Device supports a maximum resolution of up to 1600x1200@75Hz. Increasing the cable length from your IP Device to your KVM switch or server will result in lower resolution support.

Do I have to install any software to use the IP Device?

No, the IP Device does not require any drivers or software to be installed in your servers. Simply connect the IP Device to your KVM switch or server using the included PS/2 cable kit, and then attach one keyboard, monitor, and mouse to the console ports, and it is ready for use.

Does the IP Device support Linux?

Yes, the IP Device works with Red Hat and other Linux distributions configured for PS/2 or USB support.

Frequently Asked Questions

What communication ports does the IP Device use so it can be accessed remotely?

Five ports have to be open to remotely connect to the IP Device. Ports 80 and 443 are used for standard web communication. Three consecutive ports are used to send the remote video. These can be user-defined. By default, ports 900, 901, and 902 are used.

Hz→	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		X	
720x400					x					X	
800x600	x	x				x		x		X	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

Troubleshooting

Problem:

The Remote console login page will not display on my browser.

Solution:

• Verify that you are using Microsoft Internet Explorer 6.0 or higher.

• Verify that the ActiveX plug-in is installed and enabled for the web browser.

• A firewall may prevent access to the remote console. Verify that default ports 900, 901, and 902 for both HTTP and HTTPS are open. If you have selected your own ports, verify that the three consecutive ports are open based on the first port number you selected.

Problem:

The mouse does not sync after I align the mouse using the quick-access toolbar.

Solution:

• In the quick-access toolbar, click the "mouse" icon and select "Manual Settings". Check that the correct operating system and mouse settings are selected. Refer to page 34.

• Use the quick-access toolbar and select "Auto video adjust" under "Video Settings". Refer to page 39.

Problem:

I can't switch to a different server using the server list on the quick-access toolbar.

Solution:

• If you have changed the hot key in the KVM switch, make sure to upload a new switch-definition file (SDF). Refer to page 24.

• Make sure you have named the server in the Switch-Configuration page. Refer to page 23.

Troubleshooting

Problem:

The video quality is bad and/or grainy.

Solution:

• Use the quick-access toolbar to refresh the video screen.

• Use the quick-access toolbar and select "Automated adjust" under "Manual video adjust". Refer to page 39.

Problem:

The video performance and/or mouse performance is slow.

Solution:

• Use the quick-access toolbar to refresh the video screen.

• Use the quick-access toolbar and select "Automated adjust" under "Manual video adjust". Refer to page 39.

Problem:

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

Solution:

• Refer to the "Restoring Factory Defaults" section on page 44.

Problem:

I changed the LAN settings to a static IP address, but I cannot get into the web interface through the new IP address.

Solution:

• Make sure you uncheck the "Enable DHCP" box.

• Check whether the computer you are using to access the web interface has an IP address in the same domain as the new IP address to which you set your IP Device.

• Refresh your browser or clear your browser's cache.

Glossary

The following definitions are used throughout this User Manual.

Client Computer: The computer being used to access the Switch remotely over a TCP/IP connection.

Console: The all-in-one term for the keyboard, video monitor, and mouse connected to a KVM switch.

Console Port: Receptors for the console to connect to the KVM switch.

Control: When discussing switching between ports, control means that the console is capable of sending input to the server. Control requires that the console also has focus on the port, and is viewing it.

DDC: Short for Display Data Channel, a VESA standard for communication between a monitor and a video adapter. Using DDC, a monitor can inform a computer's video card about its properties, such as maximum resolution and color depth, to ensure that the user is presented with valid options for configuring the display.

DHCP: Dynamic Host Configuration Protocol. An Internet protocol that allows nodes to dynamically acquire ("lease") network addresses for periods of time rather than having to pre-configure them. DHCP greatly simplifies the administration of large networks, and networks in which nodes frequently join and depart.

Daisy-Chain: A configuration of multiple KVM switches that are connected one to another in a series. A KVM-switch daisy-chain uses common settings to allow seamless, complex interactions between multiple consoles for control over many servers.

Host Computer: The computer connected directly (locally) to the IP Device.

Glossary

KVM: Literally "Keyboard Video Mouse", this term refers to technology that allows two or more computers to be controlled by one keyboard, video monitor, and mouse; some switches that use KVM technology enable sharing of other peripherals such as audio speakers, microphones, and printers.

KVM Switch: A device that allows a user to access and control multiple servers from a single console. It has at least one console port and multiple server ports.

MAC: Media Access Control. In computer networking, a MAC address is a unique identifier attached to most forms of networking equipment.

Port: An interface receptor on a server through which you can attach a device or plug in a device cable.

SSL: Secure Sockets Layer. Cryptographic protocols that provide secure communications on the Internet for such things as email and Internet banking.

TCP/IP: Transmission Control Protocol/Internet Protocol. Shorthand for the suite of rules defining the format devices use to communicate over the Internet.

Target Server: The server currently being accessed and controlled by the user from a local or remote console.

Information

FCC Statement

Declaration of Conformity with FCC Rules for Electromagnetic Compatibility

We, Belkin International, Inc., of 501 West Walnut Street, Compton CA 90220, declare under our sole responsibility that the products:

F1DP101M

to which this declaration relates:

Comply 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 International, Inc., declare under our sole responsibility that the products F1DP101M, to which this declaration relates, are 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 International, Inc., Limited 2-Year Product Warranty

What this warranty covers.
Belkin International Inc. ("Belkin") 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 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 for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin 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.

Information

How to get service.

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

1. Contact Belkin, 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.

Belkin reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin 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, 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 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. 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 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.

BELKIN®

www.belkin.com

Belkin Tech Support
US: 800-223-5546 ext. 2263
    310-898-1100 ext. 2263
UK: 0845 607 77 87
Australia: 1800 235 546
New Zealand: 0800 235 546
Singapore: 65 64857620
Europe: www.belkin.com/support

Belkin International, Inc.
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 Ltd.
4 Pioneer Avenue
Tuggerah Business Park
Tuggerah, NSW 2259, Australia
+61 (0) 2 4350 4600
+61 (0) 2 4350 4700 fax

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

P75437

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com