BELKIN®

OmniView™

Remote IP Console

User Manual

F1DE101N

ENTERPRISE Series

TABLE OF CONTENTS

INTRODUCTION

Congratulations on your purchase of this Belkin OmniView ENTERPRISE Series Remote IP Console (the Unit). 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 anywhere around the world through any web browser, the Unit can be easily configured to accommodate your existing LAN setup, large or small.

Belkin has designed and developed the Unit 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 Unit, from installation to operation and troubleshooting, in the unlikely event of a problem.

Thank you for purchasing the OmniView ENTERPRISE 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

- 1 OmniView ENTERPRISE Series Remote IP Console
- 1 User Manual
- 1 Quick Installation Guide
- 1 IEC Power Supply Cord
- 1 PS/2 KVM Cable Kit
- Rack-Mount Brackets with Screws
- Registration Card

GLOSSARY

SSL Secure Sockets Layer Protocol—used for managing the security of a message transmission on the Internet.

SNMP Simple Network Management Protocol—governs network management and the monitoring of network devices and their functions.

ICMP Internet Control Message Protocol—used for message control and error reporting between a host server and a gateway to the Internet.

DHCP Dynamic Host Configuration Protocol—automatically configures the TCP/IP settings of every computer in your network.

TCP/IP Transmission Control Protocol/Internet Protocol—used for data transmission over the Internet.

SMTP Simple Mail Transfer Protocol—used in sending and receiving e-mail.

UDP User Datagram Protocol—offers a limited amount of service when messages are exchanged between computers in a network that uses the IP.

HTTPS Hyper Text Transfer Protocol over Secure socket layer—encrypts and decrypts user page requests as well as the pages that are returned by the web server.

Static IP A number that is in a sequence of four decimal numbers, separated by dots, assigned by an Internet Service Provider to be its permanent address on the Internet.

Dynamic IP A number that is in a sequence of four decimal numbers, separated by dots, assigned by your DHCP.

OVERVIEW

The Unit allows you to access the connected computer or KVM switch through the Internet by using a web browser. Using the latest compression technology, the Unit compresses the console signals and sends it through the network via TCP/IP protocols. The Unit automatically monitors server activities and notifies you if problems exist so you can resolve them quickly and inexpensively. It overcomes inherent limitations in current remote server administration methods. For example, the Unit enables you to reset the hardware, access BIOS, and reset power. The Unit does not require any additional software and supports multiple operating systems with PS/2 platforms.

For local control and monitoring, the Unit has one local port for connection of a separate mouse, keyboard, and monitor. The local port allows you to directly access and view the connected computer or KVM switch.

The Unit senses the controlled computer's video mode, and digitizes and compresses the video using a proprietary compression algorithm. It then sends the video to the local and remote consoles. From the remote console, the mouse and keyboard data is encrypted using 128-bit SSL, and is sent over the TCP/IP network back to the Unit where it decodes the data before sending it to the controlled server. The Unit performs hardware emulation of the mouse and keyboard so that the absence of a keyboard and mouse doesn't register as an error on the controlled server.

The Unit has two RS232 serial ports that are used for multiple applications. The first serial port is a modem-compatible port and the second is a 3-wire RS232 port with additional pins that can be used to control contact closure devices such as power bars.

FEATURES

- Complete keyboard, video, and mouse control of a server or KVM switch over a TCP/IP network
- Hardware management: hardware reset and BIOS access
- Keep-alive emulation: PS/2 keyboard and mouse, and VGA video emulation even at power off
- Remote power management to remotely power on/off of a server
- Standard web browser for console interface
- Supports free client software (Virtual Network Computing (VNC) for console interface
- One local port for direct keyboard, video, and mouse access to your server
- 128-bit SSL encryption
- 3 levels of security: Relaxed, Stealth, and Turtle modes
- IntelliView On-Screen Display (OSD)
- Flash upgradeability
- 10 user passwords
- Automatic server monitoring and notification
- Serial-port monitoring and switching capability for serial devices
- SNMP-compliant
- 1U 19" rack-mount
- 100% true hardware solution for remote console management
- Operating system-independent
- Supports: Windows® NT®, 95, 98, 2000, Me, MS-DOS, CPM, Linux®, FreeBSD, UNIX®, and more

FEATURES (CONTINUED)

AUTOMATIC MONITORING AND NOTIFICATION

Monitors server functions and notifies users if the system becomes nonresponsive, loses power, has sudden video changes, or other signs of distress. It can either reset the computer automatically or notify the administrator via e-mail of any trouble.

ACCESS AND COMPATIBILITY

The interface is browser-based, so it can be used from any computer that is connected to the Internet or an intranet. No additional software is required, so it is operating system-neutral. It works equally well with Windows NT, 95, 98, 2000, Me, MS-DOS, CPM, Linux, FreeBSD, UNIX, and more.

CONTROL AND SECURITY

You can remotely reset the power of the system to recover from a lockup where Ctrl-Alt-Del doesn't work, as well as access BIOS and make adjustments. Security is guarded by multiple users/passwords, SSL encryption, secure web control interface, and public key certificate support for authentication (optional in addition to passwords). For use on the public Internet, a number of specialized security features include:

- Up to 10 unique passwords/users
- Stealth mode: prevents port scans and other network probes
- Turtle mode: unit will self-disable when attacked
- Idle time-out for automatic user logout

NETWORK PROTOCOLS

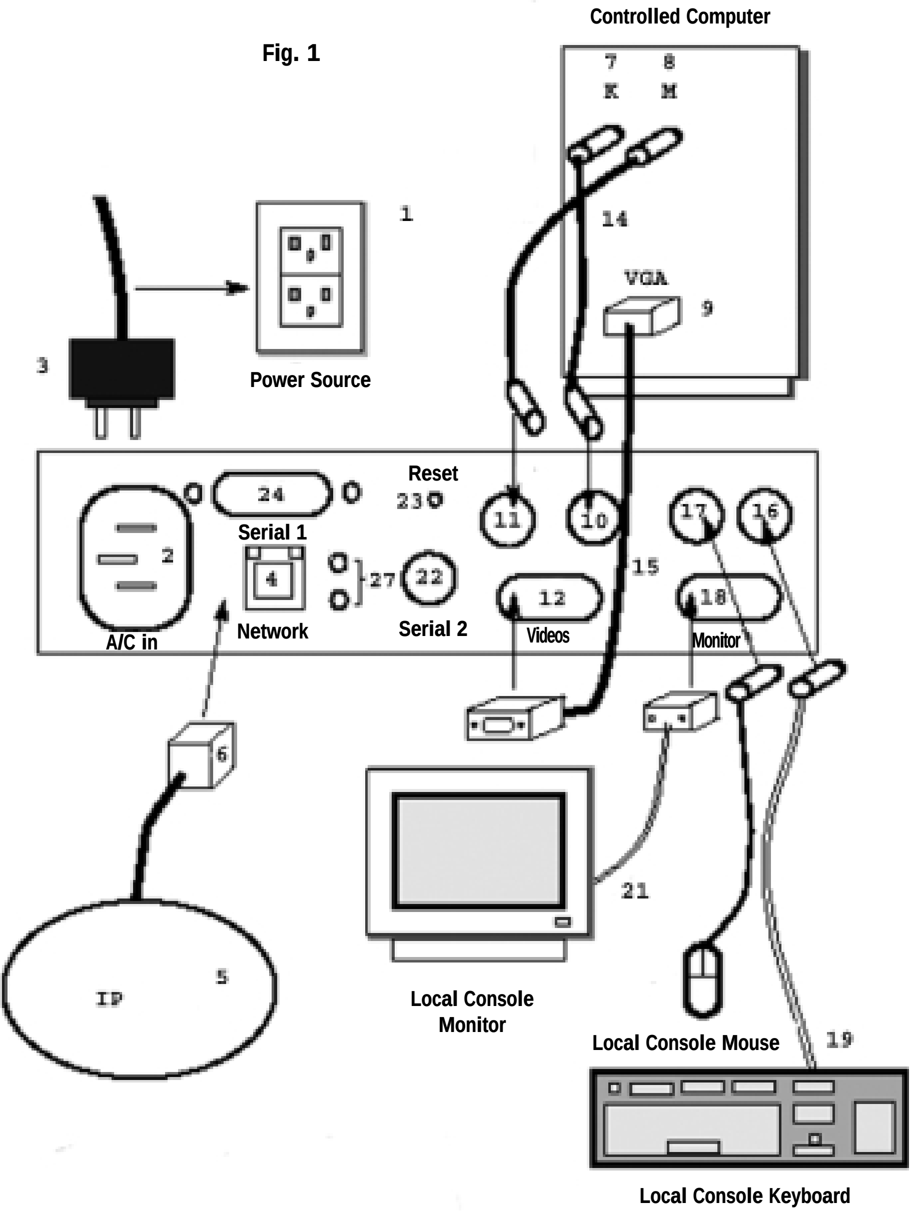
- HTTP/1.1 and HTTPS (secure) web server used for control and setup
- VNC server (implements RFB 3.3 protocol with Hextile encoding)
- Requires one dedicated IP address
- TCP/IP port numbers for all services may be changed to confuse attackers
- SMTP is used to deliver e-mail notifications
- Does not require a DNS server (Domain Name Server) so that it will continue to operate in the face of this network failure

CONNECTION DIAGRAM

LIST OF ITEMS IN CONNECTION DIAGRAM (Fig. 1)

1. A/C grounded power source, 100–240VAC @ 50/60Hz 1A
2. The Unit's power connector
3. Power cord with ground (supplied)
4. RJ45 network connector
5. Company network through which remote (VNC or Java) client communicates with the Unit
6. RJ45 Category 5 network cable
7. PS/2 connector for keyboard 6-pin miniDIN female on server
8. PS/2 connector for mouse 6-pin miniDIN female on server
9. VGA connector for monitor HDDB15 female on server
10. PS/2 connector for keyboard 6-pin miniDIN female on the Unit
11. PS/2 connector for mouse 6-pin miniDIN female on the Unit
12. VGA connector for monitor HDDB15 female on the Unit
13. PS/2 cable for keyboard port 6-pin miniDIN male/male
14. PS/2 cable for mouse port 6-pin miniDIN male/male
15. VGA cable for monitor port HDDB15 male/male with thumbscrews
16. PS/2 connector for keyboard 6-pin miniDIN female on the Unit for local console keyboard
17. PS/2 connector for mouse 6-pin miniDIN female on the Unit for local console mouse
18. VGA connector for monitor HDDB15 female on the Unit for local console monitor
19. Local Console Keyboard
20. Local Console Mouse
21. Local Console Monitor
22. Serial port 2—used for power control (relay module) or secondary serial port
23. Reset button—use a paperclip (or similar) to reset hardware of the Unit; will not affect controlled computer
24. Primary serial port—RS232C DCE connection; connect using a male/female, 9-pin, straight-through cable to any computer
25. 10/100 speed light: Green—100Base-T connection; Orange—10Base-T
26. Link/Activity Light—"On" indicates good link connection, "Off" indicates no link, "blinking" indicates is that there is network traffic
27. Red and green indicator lights that should alternate when the unit is well

CONNECTION DIAGRAM (CONTINUED)



SYSTEM REQUIREMENTS

Hardware

- Compatible with all PS/2 platform-based computers
- Compatible with all KVM switches
- Supports HDDB15 VGA video

Software

- Works with Windows NT, 95, 98, 2000, Me, MS-DOS, CPM, Linux, FreeBSD, UNIX, and more
- Compatible with both import and export browsers
- Proprietary software, with published open standard-based interfaces
- Web browser: Netscape® 4+ or Microsoft® Internet Explorer 4+
- Optional VNC viewer: supports version 3.3 of RFB protocol
- An SMTP server is required for e-mail notification feature
- Telnet client required for serial port terminal server access
- Public keys/encryption
- Supports X.509 certificates
- True hardware RNG (Random Number Generator) used to create session keys and seed values
- 128-bit or 56-bit encryption for SSL v2
- Supports RC4 and DES algorithms

SPECIFICATION

Part No.: F1DE101N
Power: 100–240VAC @ 50/60Hz 1A
Max. Number of Servers: 256 Servers (with KVM)
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: 1280x1024@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: 1.7 x 5.7 x 16 inches (43.1mm x 144.7mm x 406.4mm)
Weight: 2.6 lbs. (1088.6g)
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.

INSTALLING THE UNIT INTO A SERVER RACK

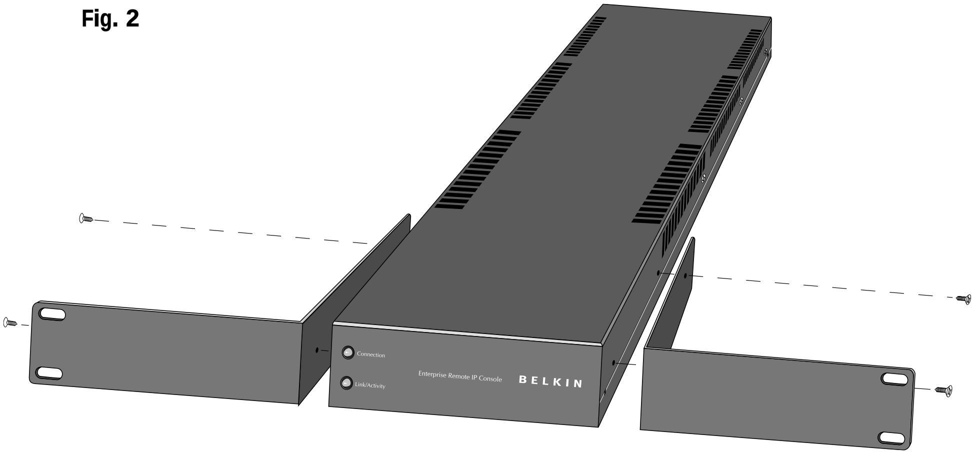
The Unit includes mounting brackets for installation in 19-inch racks.

1. Remove the first two Phillips screws located on the left and right side of the Unit.

2. Attach the two included brackets to the side of the Unit with the provided Phillips screws (Fig. 2).

3. Mount the Unit to the rack rail assembly.

Fig. 2



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 Unit or your computer(s), please ensure that everything is powered off. Belkin Components is not responsible for damage caused in this way.

HARDWARE INSTALLATION (CONTINUED)

CONNECTING THE CONSOLE

Power down your server or KVM switch.

Connect your PS/2-type keyboard and mouse to the “CONSOLE” ports.

Take the video cable that is attached to your monitor and connect it to the “CONSOLE” video port (Fig. 3).

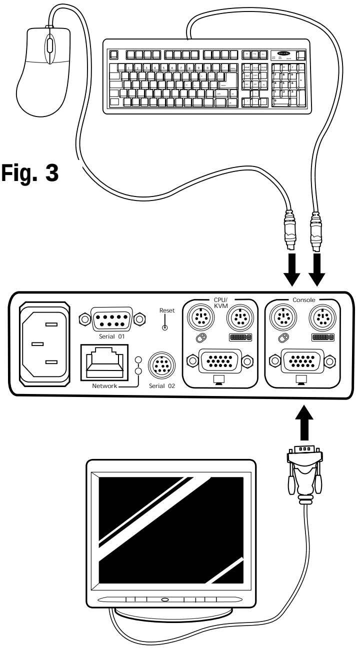


Fig. 3

CONNECTING THE SERVER TO THE UNIT

Using the provided PS/2 KVM 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 Unit (Fig. 4).

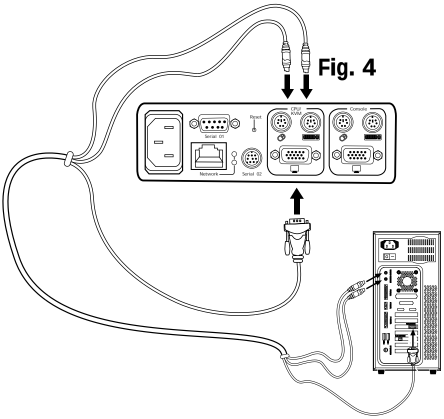
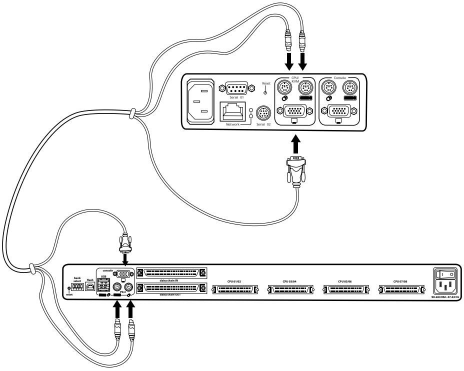


Fig. 4

CONNECTING THE KVM SWITCH TO THE UNIT

Using the provided PS/2 KVM Cable Kit, connect one end of the VGA and PS/2 cables to the Console ports on the KVM switch. Connect the other end to the "CPU/KVM" ports on the back of the Unit (Fig. 5).

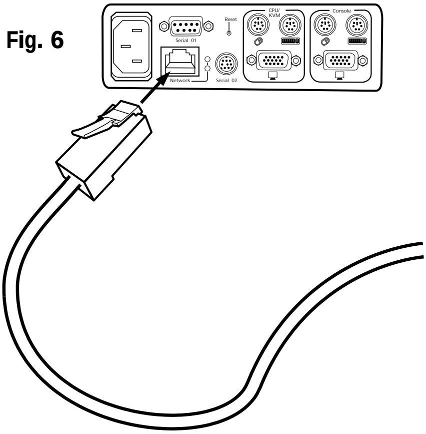
Fig. 5



CONNECTING THE UNIT TO THE NETWORK

Connect the Unit to the network using RJ45 Category 5 network cable (Fig. 6).

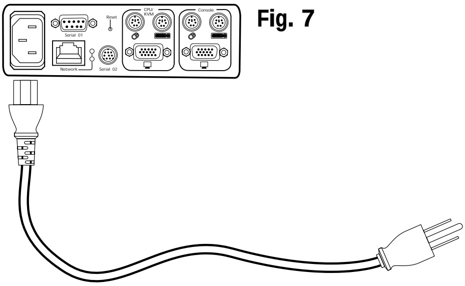
Fig. 6



POWERING UP THE UNIT

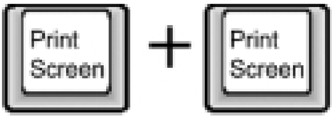
Attach the IEC power cable to the power connector located on the rear of the Unit (Fig. 7).

Fig. 7

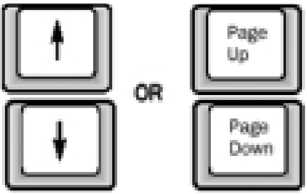


Basic Configuration from Local Console for On-Screen Display (OSD) Menu Commands

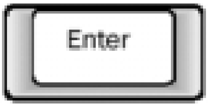
Press “Print Screen” twice quickly to gain access to the local On-Screen Display.



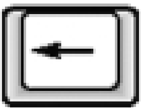
Use the arrow or “Page Up/Down” keys to navigate through the menu.



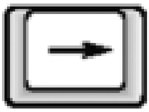
Press “Enter” to change a value.



Use the left-arrow key to return to the root menu.



Use the right-arrow key to advance to a sub-menu.



Single Server Mode

The Unit can be connected directly to a single computer as shown in Fig. 8. To configure the Unit, you must connect a keyboard, monitor, and a mouse to the Unit’s local ports. After setup, you may leave the local port connected or unconnected.

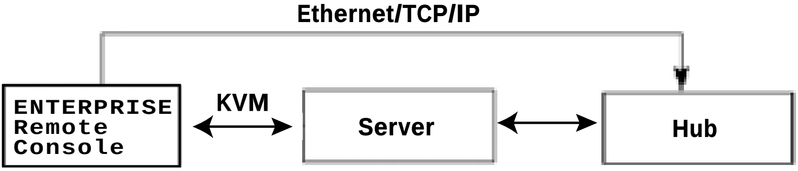


Fig. 8

Multiple Servers Mode

The Unit can be connected to a KVM switch. During initial setup, the user must connect a keyboard, monitor, and a mouse to the local port to set up the Unit. After the initial setup is complete, the user can leave the keyboard, monitor, and the mouse connected to the local port for local monitoring.

Ethernet Configurations

We recommend connecting the Unit as shown below. In this example, the Unit will continue to monitor the servers even if the firewall fails or the connection to the firewall goes down as shown in Fig. 9.

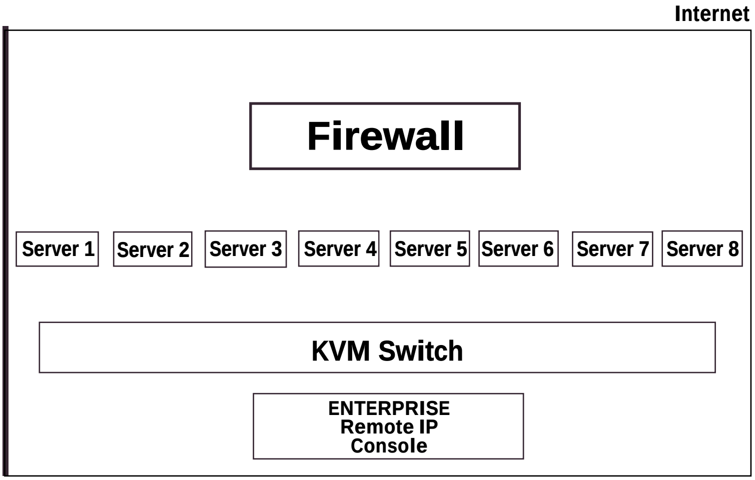


Fig. 9

The Unit and server connected to different hubs as shown in Fig. 10.

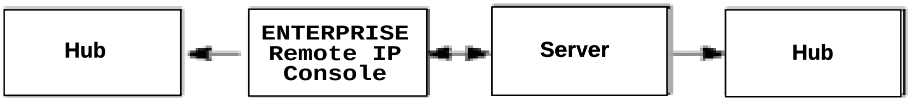


Fig. 10

Another application for the Unit would be to connect a computer that does not have a network connection on the Web, as shown in Fig. 11.

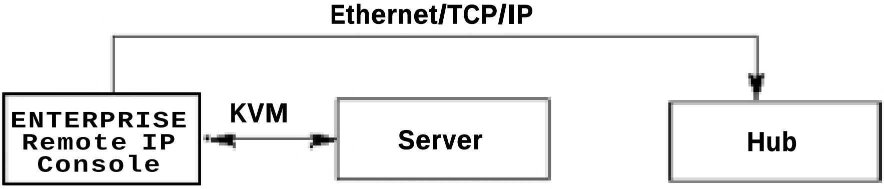
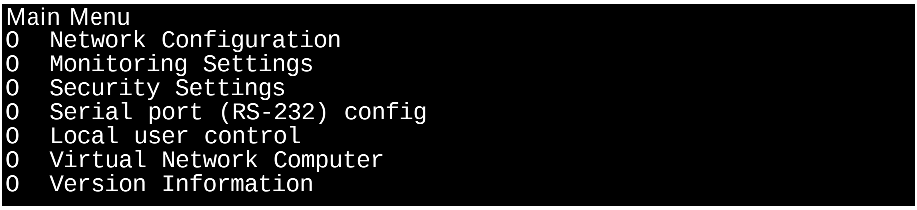


Fig. 11

NETWORK SETUP

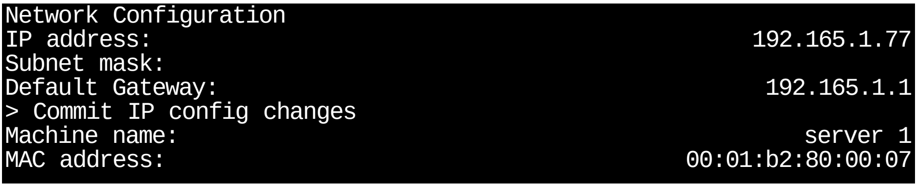
Call up the main menu by hitting the appropriate hot key combination (the default is “Print Screen” + “Print Screen”).



```
Main Menu
O  Network Configuration
O  Monitoring Settings
O  Security Settings
O  Serial port (RS-232) config
O  Local user control
O  Virtual Network Computer
O  Version Information
```

Fig. 12

Select “Network Configuration” to view the following menu:



```
Network Configuration
IP address:                                             192.165.1.77
Subnet mask:
Default Gateway:                                         192.165.1.1
> Commit IP config changes
Machine name:                                               server 1
MAC address:                                       00:01:b2:80:00:07
```

Fig. 13

NETWORK CONFIGURATION MENU

1. Addressing and Routing
   From this screen, you can configure the network details for the Unit.

Note: When you make changes to any of the above, your changes will take effect after the next reset or power cycle. If you want the new values to be in effect immediately, select “Commit IP config changes”.

2. Changing the Machine Name
   This simple text string identifies this machine. To change the machine name, type in a new name up to 15 characters long.

3. Accessing the Ethernet Address (MAC Address)
   This is the hardware address of the Ethernet interface on the Unit. It is assigned by the factory to uniquely identify this Unit and it cannot be changed. You may need this number to configure other software on your network, such as DHCP servers, hubs, or monitoring software.

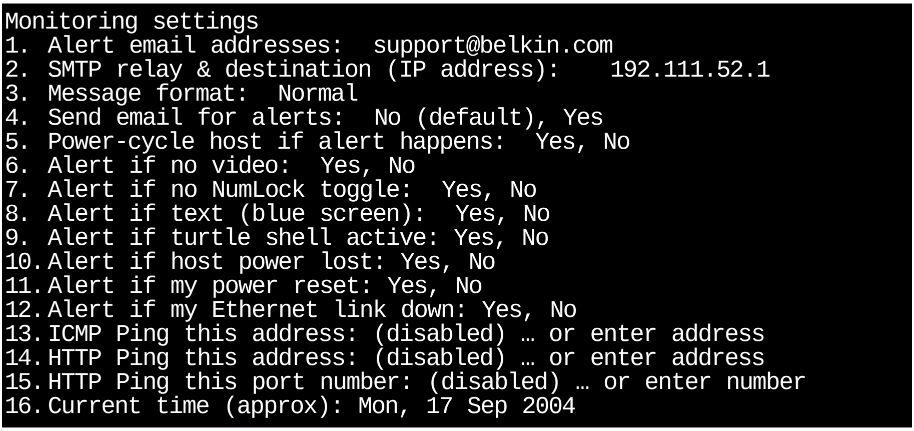
SERVER MONITORING

The Unit may be configured here to detect certain common failure modes. Once enabled, the Unit will continuously monitor for a failure and, if it occurs, will log the event. It can also be configured to send out an e-mail to alert you to the problem. For completely autonomous monitoring, it is also possible to reset the power to the controlled computer.

CONFIGURING ALERT ACTIONS

You can configure what you would like the Unit to do when an error condition occurs. All error conditions are logged when they happen whether e-mail is enabled or not.

To access the "Monitoring Settings" menu (Fig. 14), call up the main menu by hitting the appropriate hot key combination (the default is "Print Screen" + "Print Screen") and selecting "Monitoring Settings":



```
Monitoring settings
1.  Alert email addresses:  support@belkin.com
2.  SMTP relay & destination (IP address):    192.111.52.1
3.  Message format:  Normal
4.  Send email for alerts:  No (default), Yes
5.  Power-cycle host if alert happens:  Yes, No
6.  Alert if no video:  Yes, No
7.  Alert if no NumLock toggle:  Yes, No
8.  Alert if text (blue screen):  Yes, No
9.  Alert if turtle shell active: Yes, No
10. Alert if host power lost: Yes, No
11. Alert if my power reset: Yes, No
12. Alert if my Ethernet link down: Yes, No
13. ICMP Ping this address: (disabled) … or enter address
14. HTTP Ping this address: (disabled) … or enter address
15. HTTP Ping this port number: (disabled) … or enter number
16. Current time (approx): Mon, 17 Sep 2004
```

Fig. 14

1. Setting Alert E-mail Addresses
This is the e-mail address used in outgoing e-mail when the monitoring function detects a failure.

2. SMTP Relay/Destination (IP Address)
The SMTP relay/destination is the IP address (numeric) for the SMTP server to use to send the e-mail. This server must be willing to relay to the above e-mail address, or else be the mail server for that domain. Disable this by setting address to 0.0.0.0.

3. Message Format
   You can choose the type of e-mail message to send in the event of a failure. The default message length is normal; the short format is appropriate for messages sent to cell phones and pagers that have a limited display.

4. Send E-mail for Alerts
   This control must be enabled before any e-mail will be sent. You can use this to turn off e-mail without losing your other settings.

5. Power-Cycle Host If Alert Happens
   You can enable the Unit to reset the controlled computer to be automatically turned off (via power cycle) when an error condition occurs.

Note: This option carries a certain risk to it, because there is a possibility of false positives with all of the failure tests.

6. Alert If No Video
   Enabling “Alert if no video” will cause a notification if no graphics or text video signal is coming from the controlled computer. Please note that power-saving screen savers (DPMS) may trigger this falsely. To enable, select “Yes”. To disable, select “No”.

7. Alert If No NumLock Toggle
   If this is enabled, then the Unit will simulate the “Num Lock” key being pressed regularly (every few seconds). If at any time, the “Num Lock” light does not toggle in response to a “Num Lock” key-press, then the software on the controlled computer is assumed to have crashed and this error condition will be active. To enable, select “Yes”. To disable, select “No”.

8. Alert If Text (Blue Screen)
   “Alert if text (blue screen)” occurs when the machine is rebooting (BIOS screen) or displays “Blue Screen of Death”. This can be useful for detecting self-initiated reboots. To enable, select “Yes”. To disable, select “No”.

9. Alert If Turtle Shell Active
   “Alert if turtle shell active” occurs if turtle mode is activated by too many bad login attempts over a certain period. To enable, select “Yes”. To disable, select “No”.

10. Alert If Host Power Lost
    The alert is activated when the power supply fails to the controlled computer; this condition is considered active. To enable, select “Yes”. To disable, select “No”.

11. Alert If Power Is Reset
If the Unit is reset or powered-off for any reason, this condition is activated when power is restored. This might be used in combination with other controls above. To enable, select “Yes”. To disable, select “No”.

12. Alert If My Ethernet Link Down
If the Ethernet link signal to the Unit is lost, then this condition is activated. There can be some difficulty sending e-mail if this condition occurs, because the Unit is off the Net in this situation. The event is still logged, however. To enable, select “Yes”. To disable, select “No”.

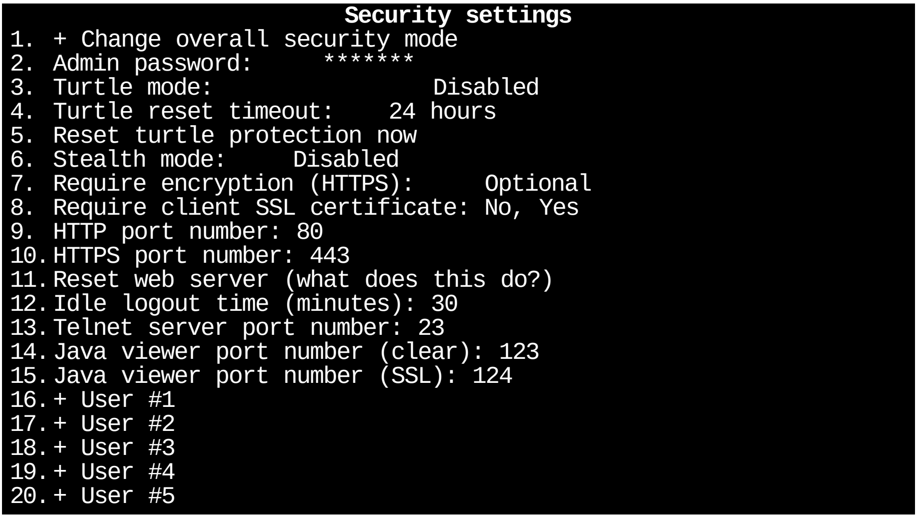
13. Designating an ICMP Ping
The ICMP Ping address should be an IP address that will be pinged continuously. If more than half of the packets are lost during a short interval, then the error condition is triggered. This IP address does not need to be the controlled computer, but might be a border router or other important component of your network. To enable, enter an IP address to ping. To disable, use 0.0.0.0.

14. HTTP Ping This Address
The number designated for HTTP pings of addresses should be an IP address of a web (HTTP) server. The server will be asked to get the root page. If nothing is returned (zero length) or the connection fails, then this error condition is considered active. To disable, use 0.0.0.0.

15. HTTP Ping This Port Number
The number designated for HTTP pings of ports should be an IP address of a web (HTTP) server. The server will be asked to get the root page. If nothing is returned (zero length) or the connection fails, then this error condition is considered active. To disable, use 0.0.0.0.

16. Current Time (Approx)
The value “Current time (approx)” is a Web-only value and cannot be changed from the local console. You must use the web interface instead.

To access the "Security Settings" menu (Fig. 15), call up the main menu by hitting the appropriate hot key combination (the default is "Print Screen" + "Print Screen") and selecting "Security Settings":



```
                         Security settings
1. + Change overall security mode
2. Admin password:     *******
3. Turtle mode:                Disabled
4. Turtle reset timeout:    24 hours
5. Reset turtle protection now
6. Stealth mode:     Disabled
7. Require encryption (HTTPS):     Optional
8. Require client SSL certificate: No, Yes
9. HTTP port number: 80
10.HTTPS port number: 443
11.Reset web server (what does this do?)
12.Idle logout time (minutes): 30
13.Telnet server port number: 23
14.Java viewer port number (clear): 123
15.Java viewer port number (SSL): 124
16.+ User #1
17.+ User #2
18.+ User #3
19.+ User #4
20.+ User #5
```

Fig. 15

You may choose one of the following three security policy buttons to configure the Unit for common situations. Once this has been done, you may further fine-tune other security settings, including local settings.

Relaxed Security (Default)

This is the factory default. It requires passwords (where defined) but allows those passwords to be transmitted "in the clear" over the network. This means network sniffers can see the passwords needed to access the Unit. This is the only mode that leaves the telnet server enabled. You might need to use this mode if your browser does not support encryption.

Internal LAN with Snoopers

This is the recommended setting for most office networks. It requires all connections to use encryption. Passwords are not visible to network sniffers but the Unit does not try to conceal its presence on the network.

For Use on the Public Internet

This is the recommended setting if the Unit is outside of a firewall and is visible to the public Internet. Non-standard values are used for web server TCP/IP ports (8888 for HTTP, 4444 for HTTPS), but you should change them from these default values. This mode also enables two proprietary features of the Unit: Turtle mode and Stealth mode.

SECURITY MODES OFFER DIFFERENT LEVELS OF SUPPORT AND CONTROL

Turtle Mode

This optional mode enables the Unit to shut down when it feels that its security may be under attack. For example, if more than five password failures are detected in a certain time frame, the Unit will shut down and disconnect itself from the network. The only way to recover operation of the Unit is to log in from the local control port (the keyboard connected to the “thru” connector) and give the appropriate reset command. Remote access to the Unit is completely locked out. The operation of the attached server is not affected. Clearly, Turtle mode opens the Unit to denial-of-service attacks, which could be rather annoying to legitimate users. Therefore, this mode is not enabled by default. There is an optional Turtle timeout duration (in hours) that by default is set to 24 hours.

Stealth Mode

In Stealth mode, the Unit deliberately violates certain TCP/IP protocol standards in order to conceal its presence on the network. For example, it will not respond to any ICMP ping requests. A TCP/IP connection request (or UDP packet) to any unused port will go unanswered and will not solicit the normal “connection refused” response. The goal is to make the Unit invisible to a “port scan” attack, by acting as if it was not there. For optimum security, the web server port number should be changed from the default as well (user-configurable). Operation of the Unit by legitimate users who know both the IP address and web server port number will be as normal. However, outsiders who might be searching for the Unit will not be able to detect it on the network unless they correctly guess both the IP address and port number.

SECURITY SETTINGS

1. Change Overall Security Mode
There are three security modes to choose from: “Relaxed” (default), “Internal LAN with Snoopers”, and “For Use on the Public Internet”. For an explanation of these modes, please see page 18.

2. Admin Password
The master (or root) password can be changed here. The user name for the master account cannot be changed; the system will accept either “root” or “administrator” as the name of this account.

3. Turtle Mode
To enable Turtle mode, change the default setting of “Disabled” to “Enabled”. For a complete description of this security setting, please see above.

4. Turtle Reset Timeout
Change this value to set the number of hours the Unit stays in Turtle mode after an attack.

5. Reset Turtle Protection Now
The “shell” of protection can be manually reset at the local console.

6. Stealth Mode
To enable Stealth mode, change the default setting of “Disabled” to “Enabled”. For a complete description of this security setting, please see above.

7. Require Encryption (HTTPS): No, Yes
Use this command to require HTTPS encryption for all activities through the Unit.

8. Require Client SSL Certificate: No, Yes
Use this command to require a client SSL certificate for all activities through the Unit.

9. HTTP Port Number: 80
Use this command to change the HTTP port number.

10. HTTPS Port Number: 443
Use this command to change the HTTPS port number.

11. Reset Web Server
Use this command to reset the web server.

12. Idle Logout Time (Minutes): 30
Idle logout time is set in minutes. To change, enter new number of minutes.

13. Telnet Server Port Number: 23
To change, enter new telnet server port number.

14. Java Viewer Port Number (Clear): 123
To change, enter new java viewer port number.

15. Java Viewer Port Number (SSL): 124
To change, enter new java viewer port number.

16.–20. Setting User Passwords (+ User #1, + User #2, etc.)
Choose these options to get to the "User settings" sub-menu (Fig. 16). This process applies to all of the users that you will create for the Unit.

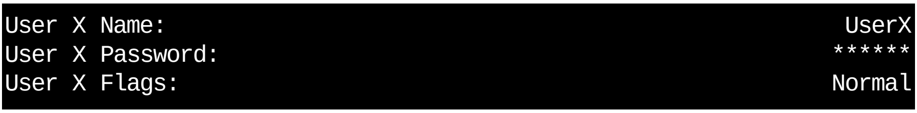
USER SETTINGS SUB-MENU

Flags

Not only is the administrator responsible for assigning user passwords and names, in the "Flags" section, the administrator chooses how much authority to give the user.

Normal

"Normal" means the user can log in and use the Unit with full privileges.



```
User X Name:                                                      UserX
User X Password:                                                 ******
User X Flags:                                                    Normal
```

Fig. 16

View Only

"View only" means the user can watch what the server is doing but cannot send keyboard and mouse commands.

Disabled

In the "Disabled" mode, the Unit will not accept the login name or user ID.

To enable the new user name, you must change the value to "Normal" or "View Only".

The Unit has two serial ports. Each may be used for four different purposes:

1. ENTERPRISE Series Remote IP Console Log—outputs log from the Unit's serial port. The following is an example of format of the log output:

```
"@ Tue, 14 Aug 2001 15:34:37 -400 INFO:
System startup. (Previously up at: Tue, 14 Aug 2001 15:32:32 -400)
@ Tue, 14 Aug 2001 15:34:22 -400 INFO:
Random words are 76/160 (47%) ones (passed test)."
```

   The Unit's log can also be read from the web interface.

2. Telnet—allows remote telnet user to connect to serial device. The user must connect the serial cable to the serial device, configure the serial port, and start "Telnet" to the device through the Unit. The Unit is transparent in this mode and allows bidirectional link.

3. Watchdog—detects and logs the presence or absence of a string.

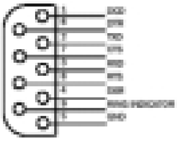
   Watchdog pattern (string): Each line of input (to the Unit) will be matched against this simple string. Only lines that contain this string will be logged in Watchdog mode. If this field is empty, then all lines will be logged.
   Watchdog mode: Choose what to do with lines that match the pattern. See "Monitoring Settings" section to configure what happens with the alert.

   Watchdog timeout: Period of time during which a matching string must be seen, before an error condition is considered to have occurred. Used only with Watchdog mode "Alert if missing".

4. Power Control—connects to a serial device to turn off/on power to the controlled device. This feature is ideal for controlling power bars with serial protocol capabilities. Choose the make and model from the web browser interface and click to reset the power to target.

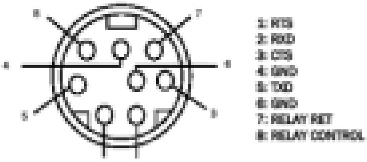
Serial Port Configuration

Fig. 17



Serial Port 1 (DB9 Female)
This port has all the signals of a typical RS232 serial port (Fig. 18). This port can be fully configured from the web interface in the serial interface configuration menu.

Fig. 18



Serial Port 2 (8-pin miniDIN)
Port 2 is an RS232 port with minimum handshaking support (see Fig. 19). Port 2 also has an added capability to control contact closure power bars as well as serial protocol-capable power bars (see belkin.com for list of supported devices). A breakout cable can connect to the rear-panel 8-pin miniDIN while providing a DB9 and an RJ11 on the other end. The DB9 provides the RS232 output and the RJ11 provides the necessary connections to control contact closure power bars. See Fig. 19 of the breakout cable.

SERIAL PORT FUNCTIONS (CONTINUED)

Port 2 has the same menu options as Port 1. The user must configure each port separately. Each port can be configured for different functions. When both ports are configured for the same functions, then the outputs of each port are identical. For example, if each port is set to “Telnet” function and a telnet command is sent to the Unit, then both ports will output the same command. Port 1 and Port 2 can operate at different baud rates.

Note: Port 2 does not support hardware flow control.

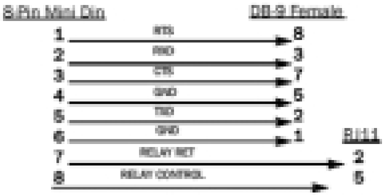
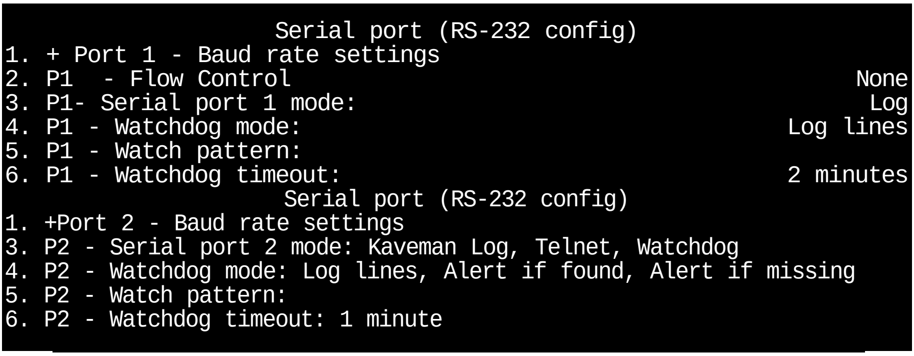


Fig. 19
Breakout Cable

SERIAL PORT CONFIGURATION

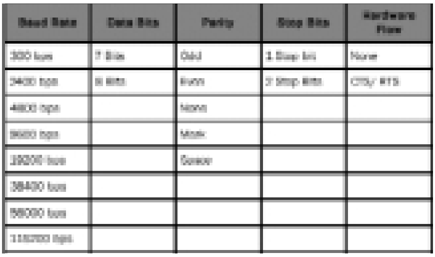
To access the “Serial port (RS-232 config)” menu (Fig. 20), call up the main menu by hitting the appropriate hot key combination (the default is “Print Screen” + “Print Screen”) and selecting “Serial Port (RS-232 config)”:



```
                    Serial port (RS-232 config)
1. + Port 1 - Baud rate settings
2. P1  - Flow Control                                        None
3. P1- Serial port 1 mode:                                    Log
4. P1 - Watchdog mode:                                  Log lines
5. P1 - Watch pattern:
6. P1 - Watchdog timeout:                               2 minutes
                    Serial port (RS-232 config)
1. +Port 2 - Baud rate settings
3. P2 - Serial port 2 mode: Kaveman Log, Telnet, Watchdog
4. P2 - Watchdog mode: Log lines, Alert if found, Alert if missing
5. P2 - Watch pattern:
6. P2 - Watchdog timeout: 1 minute
```

Fig. 20

To configure the serial port, choose the desired baud rate, parity, data bits, stop bits, and hardware flow control configuration (Fig. 21).

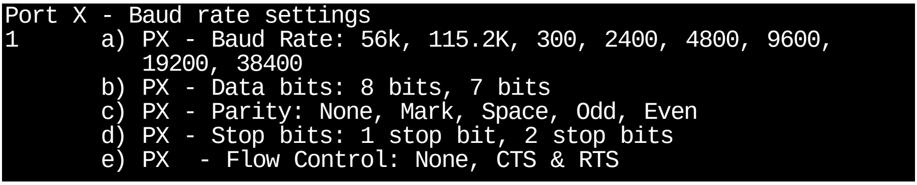


Baud Rate	Data Bits	Parity	Stop Bits	Hardware Flow
300 bps	7 Bits	Odd	1 Stop bit	None
2400 bps	8 Bits	Even	2 Stop Bits	CTS/ RTS
4800 bps		None		
9600 bps		Mark		
19200 bps		Space		
38400 bps				
57600 bps				
115200 bps				

Fig. 21

Note: The settings for P1 and P2 are identical, except for the flow control setting, which only applies to P1. Accordingly, from this point forward, ports will be referred to as PX or Port X (Fig. 22).

Port X - Baud Rate Settings



```
Port X - Baud rate settings
1      a) PX - Baud Rate: 56k, 115.2K, 300, 2400, 4800, 9600,
          19200, 38400
       b) PX - Data bits: 8 bits, 7 bits
       c) PX - Parity: None, Mark, Space, Odd, Even
       d) PX - Stop bits: 1 stop bit, 2 stop bits
       e) PX  - Flow Control: None, CTS & RTS
```

Fig. 22

2. PX - Flow Control (Port 1 Only)
Options: None, CTS, and RTS.

3. Serial Port X Mode
Options: ENTERPRISE Series Remote IP Console Log, Telnet, Watchdog, Power Control (Port 1 only). For an explanation of these functions, please see page 21.

4. PX - Watchdog Mode
Use this function to choose what to do with lines that match the pattern. Your options are to "Log lines", "Alert if found", or "Alert if missing". For more information on configuring what happens when there is an alert, see the "Monitoring Settings".

5. PX - Watch Pattern:
Each line of input (to the Unit) will be matched against this simple string. Only lines that contain this string will be logged in Watchdog mode. If this field is empty, then all lines will be logged.

6. PX - Watchdog Timeout:
This is the period of time during which a matching string must be seen, before an error condition is considered to have occurred. It should be used only with Watchdog mode "Alert if missing".

Local User Control

To access the "Local User Control" menu (below), call up the main menu by hitting the appropriate hot key combination (the default is "Print Screen" + "Print Screen") and selecting "Local User Control" (Fig. 23):

Local User Control Menu

1. Reset Local Keyboard and Mouse

2. Resync Mouse Position

3.–4. Mouse Threshold and Acceleration
These two values determine the speed of the local mouse. When the mouse is moved faster than "threshold", its movement will be accelerated by "acceleration" factor. None of this has any impact on remote users via VNC or java viewer.

SERIAL PORT FUNCTIONS (CONTINUED)

5. Local Console Passwords
You can set a password for the local console. This does not affect the passwords used for remote access.

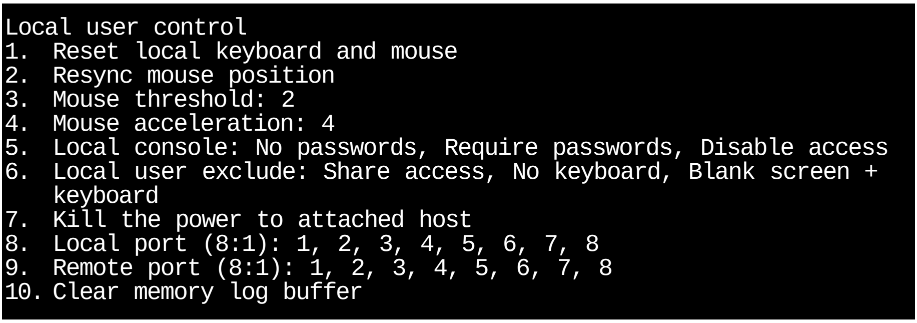
6. Local User Exclude
Options: Share, No Keyboard, and Blank Screen and Keyboard.
When “local user exclude” is set to “Share”, the local user can type when the remote user (VNC, java) is connected and also controlling the same machine. When “local user exclude” is set to “No Keyboard”, the local keyboard is locked out when a remote user connects. When “local user exclude” is set to “Blank Screen and Keyboard”, the local keyboard is locked out AND the screen is blacked out so a local user cannot see the screen when a remote user is logged in.

7. Kill the Power to Attached Host
Turns off and on the relay for the power bar that is connected to the breakout cable RJ11 (dataprobe).

8. Local Port (8:1): 1, 2, 3, 4, 5, 6, 7, 8
Change local port number (1–8).

9. Remote Port (8:1): 1, 2, 3, 4, 5, 6, 7, 8
Change remote port number (1-8).

10. Clear Memory Log Buffer



```
Local user control
1.  Reset local keyboard and mouse
2.  Resync mouse position
3.  Mouse threshold: 2
4.  Mouse acceleration: 4
5.  Local console: No passwords, Require passwords, Disable access
6.  Local user exclude: Share access, No keyboard, Blank screen +
    keyboard
7.  Kill the power to attached host
8.  Local port (8:1): 1, 2, 3, 4, 5, 6, 7, 8
9.  Remote port (8:1): 1, 2, 3, 4, 5, 6, 7, 8
10. Clear memory log buffer
```

Fig. 23

VIRTUAL NETWORK COMPUTER

To access the “Virtual Network Computer (VNC)” configuration menu (Fig. 24), call up the main menu by hitting the appropriate hot key combination (the default is “Print Screen” + “Print Screen”) and selecting “Virtual Network Computer”.

1. VNC Server Port Number: 5900
Normally, this is 5900, which is the default port for the first VNC display on a VNC server. It is easy to specify a different port number from the VNC client, just append it after the host name with a colon (target: 123, for example).

2. VNC Bandwidth Goal: Min, Medium, Max
This influences the trade-off between speed and compression. On the “Min” setting, the maximum amount of video compression is performed, but that consumes some time. In the “Max” mode, the video is not compressed at all, it’s just set as quickly as possible. “Max” mode is useful on local area networks. Of course, “Medium” is a compromise that does some compression. We recommend “Max” for local area networks (10Mb and above), and “Min” for links with less than 256Kbps bandwidth. Everything else should be used with “Medium”.

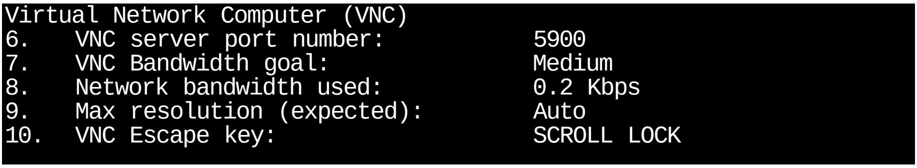
VIRTUAL NETWORK COMPUTER (VNC)

3. Network Bandwidth Used: 0.2Kbps (This is a read-only value.)

4. Max Resolution (Expected)
The initial size of the VNC client window is controlled here. Most users will want to leave this control at “auto”, which picks the highest resolution the Unit has ever observed from the server.

5. VNC Escape Key:

The VNC escape key cannot be changed from the local console. You must use the web interface instead. This key is used to “escape” normal operation and get into the menu system. Over a VNC connection, the same key (again, pressed twice quickly) is used to pull up a small menu of useful functions while online. The default keyboard exit key is “Scroll Lock”.



```
Virtual Network Computer (VNC)
6.   VNC server port number:          5900
7.   VNC Bandwidth goal:              Medium
8.   Network bandwidth used:          0.2 Kbps
9.   Max resolution (expected):       Auto
10.  VNC Escape key:                  SCROLL LOCK
```

Fig. 24

BROWSER-BASED OPERATION

Accessing the Target Computer
Enter the Unit’s address into the address bar in your browser. When you have connected to the Unit, you will arrive at the Unit’s home page.

The Unit’s Home Page Items

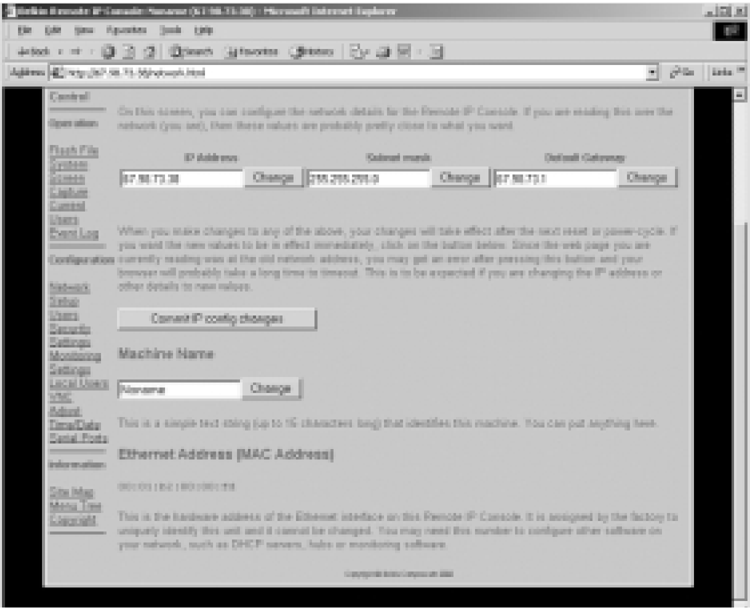
Host Status
See “Remote Administration” on page 29.

Host Control
See “Remote Administration” on page 29.

Setup and Configuration
Network Setup
Users
Adjust Time/Date
Security Settings
Monitoring Settings
Serial Ports
Local Users/VNC

Network Setup

On this screen, you can configure the network details for the Unit (Fig. 25).



On this screen, you can configure the network details for the Remote IP Console. If you are reading this over the network (you are), then these values are probably pretty close to what you want.

IP Address		Subnet mask		Default Gateway	
[illegible]	Change	255.255.255.0	Change	[illegible]	Change

When you make changes to any of the above, your changes will take effect after the next reset or power-cycle. If you want the new values to be in effect immediately, click on the button below. Since the web page you are currently reading was at the old network address, you may get an error after pressing this button and your browser will probably take a long time to timeout. This is to be expected if you are changing the IP address or other details to new values.

Commit IP config changes

Machine Name

Noname | Change

This is a simple text string (up to 15 characters long) that identifies this machine. You can put anything here.

Ethernet Address (MAC Address)

[illegible]

This is the hardware address of the Ethernet interface on this Remote IP Console. It is assigned by the factory to uniquely identify this unit and it cannot be changed. You may need this number to configure other software on your network, such as DHCP servers, hubs or monitoring software.

Fig. 25

Note: When you make changes to any of the above, your changes will take effect after the next reset or power cycle. If you want the new values to be in effect immediately, click on the button “Commit IP config changes” below. Since the web page you are currently reading was at the old network address, you may get an error after pressing this button and your browser will probably take a long time to time out. This is to be expected if you are changing the IP address or other details to new values.

Changing the Machine Name

This simple text string identifies this machine. To change the machine name, type in a new name up to 15 characters long.

Accessing the Ethernet Address (MAC Address)

This is the hardware address of the Ethernet interface on the Unit. It is assigned by the factory to uniquely identify this Unit and it cannot be changed. You may need this number to configure other software on your network, such as DHCP servers, hubs, or monitoring software.

USERS

Changing the Master Account Password

The master (or root) password can be changed here. The user name for the master account cannot be changed. The system will accept either “root” or “administrator” as the name of this account.

Defining User Names and Passwords for User Accounts

Here you may define user names and passwords for up to five regular users. You must enable the account in order to permit logins.

Below, find a step-by-step example of how to define a new user.

Step 1: Defining the User Name

a) Select the user name that you would like to define from the "Users and Passwords" table.

b) User1Name is currently set to "User1". This value is a text string up to 15 characters long. The default value is "User1".

c) Type in new user name and press "Change".

Step 2: Changing User Passwords

You will see the current password. This value is a secret password up to 15 characters long. Enter twice to confirm value. The default value is "[none/empty]".

Step 3: Setting User Permissions (Flags)

Not only is the administrator responsible for assigning user passwords and names, in the "Flags" section, the administrator chooses how much authority to give the user.

There are three display values: 0: Disabled; 1: Normal; and 2: View Only.

Normal
"Normal" means the user can log in and use the Unit with full privileges.

View Only
"View Only" means the user can watch what the server is doing but cannot send keyboard and mouse commands.

Disabled
In the "Disabled" mode, the Unit will not accept the login name or user ID.

To enable the new user name, you must change the value to
"Normal" or "View Only".

Adjust Time/Date

Date and time is stored internally in UTC (Coordinated Universal Time, sometimes called GMT or Zulu time). When times are shown in logs or over the Web, a time zone offset is applied to convert that time into local time. No provision is made for daylight saving time.

Synchronizing the Time/Date with Your Computer
If the computer you are using to view this page knows the correct time, just press the button labeled "Set date, time and time zone" to set the time and zone of the Unit to the same time as your browser.

Current Time
This section indicates when the page was sent. For example:

Wed, 15 Aug 2004 10:23:16 –400

Time Zone Offset (from UTC)

This is the number of minutes the Unit is offset from UTC. Most time zones are on 1-hour boundaries. If you take the UTC time (the time in Greenwich) and add this (signed) value to it, you should get your current local time.

Security Settings

There are a number of controls provided for the local console as well. The master password may always be used to change any settings of the system from the local console. You may restrict regular users as follows:

Local Console Passwords

You can set a password for the local console. This does not affect the passwords used for remote access.

For instructions on creating remote access user names and passwords, see page 26.

Local User Exclude

Explanation of Settings:

0: Share access—local user can type when the remote user is connected and also controlling the same machine.

1: No keyboard—local keyboard is locked out when remote user connects.

2: Blank screen + keyboard—local keyboard is locked out and the screen is blacked out so a local user cannot see the screen when a remote user is connected.

Accessing the Target Computer

Enter the Unit's address into the address bar in your web browser. When you have connected to the Unit, you will arrive at the Unit's home page.

Checking the Host Status

From the home page, you can immediately check the status of the host's screen and power. You can also access a log of recent activity.

The Event Log

The log will appear indicating the time, level, and a brief description of all failed log-in attempts (Fig. 26).

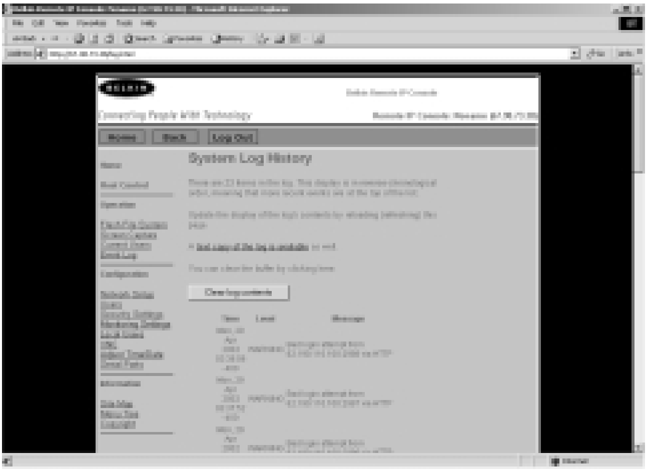


Fig. 26

Taking Control of the Target Computer

Follow the instructions on the Unit's home page to view the current screen contents and take control of the host's keyboard and mouse. You can open a new window to view the screen contents or start a new full-screen browser window. You may need to use Alt-F4 to get out of that special window (Fig. 27).

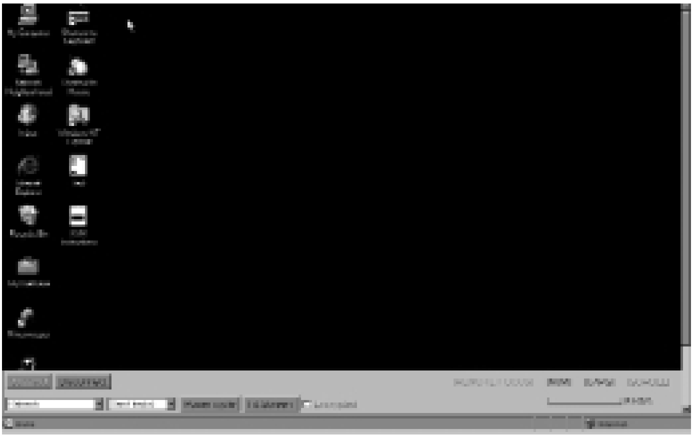


Fig. 27

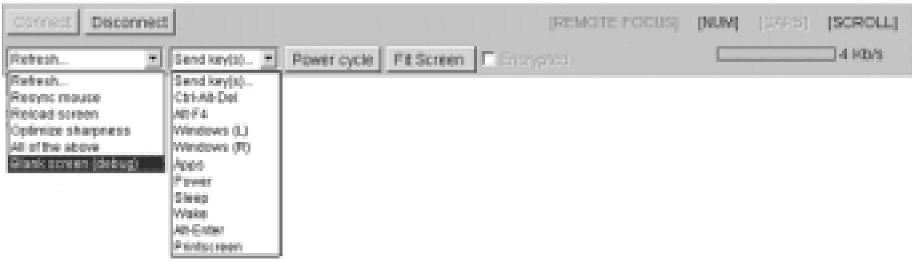


Fig. 28

Menu Items - Screen Contents Viewer

Connecting To/Disconnecting from the Target Computer
Press these buttons to connect to/disconnect from the target computer.

Refresh Menu
Resync mouse—the Unit re-syncs the mouse position.
Reload screen—the Unit reloads the screen of the target computer.
Optimize sharpness—the Unit automatically tunes the video picture for sharpness.

Send Key(s)...
Use this menu to send key combinations/commands to the target computer. If you press any of these key combinations on the computer running the browser, the computer will process the commands locally instead of sending them to the target computer.

Power Cycle
Controls a relay of a power bar connected to the server, using an optional breakout cable connected to the Unit's serial port.

Fit Screen/Full Screen
Adjusts screen size to fit into browser window.

How do I reduce the steady-state network traffic generated by VNC?

1. Improve video quality first. Any video noise is sent over the network.

2. Reduce resolution to 1024x768 or lower.

How do I reduce the overall network traffic generated by VNC?

1. Use a flat-color desktop background rather than a picture of your family or corporate leader. This data must be sent every time a window is moved, so it is best if it is a single color that will compress down to almost nothing.

2. Improve video quality so no analog noise is sent.

How do I maximize the video quality?

1. Use the highest-quality, shortest VGA cables possible. If you see any "ghosts" or "shadows" to the right of sharp edges, then your video cables are causing problems and poor-quality video is being delivered to the Unit.

2. From VNC, use the "optimize video" command:

a) Press "Print Screen" twice quickly.
b) Press: A.
c) Wait a second or two for screen re-draw.

This tunes the video settings to what is currently coming from the computer. Changing the video cables will affect this tuning. This tuning operation is performed automatically whenever the video mode changes, so performing this operation manually may not help.

1. Reduce vertical refresh rate to no higher than 60Hz. There is no benefit to using a higher refresh rate with the Unit. If someone is using the computer locally, and he or she is using a CRT display (as opposed to LCD), that person should be consulted to check if a lower refresh rate is more ergonomically acceptable.

2. Use the minimum resolution needed for your application. Lower resolutions (and lower refresh rates) use lower-frequency electrical signals and, therefore, stress the performance of your cables and video card less.

The mouse is always in the wrong position, by a small, fixed amount. This persists even after a "mouse resync" operation.

1. There is a screen position error, so the Unit's idea of the mouse position is offset by the width of the black bars/or missing area. See the next question and apply it.

There is a black bar to the left and/or top of my screen. Part of the image is cut off, from the left or top edges of the screen.

1. This should not occur in any VESA-standard video mode. Switch to a typical video mode (1024x768@60Hz, for example). However, some video cards do not generate VESA modes precisely, so this may not help.

2. If using a non-standard VESA mode, or an unknown video source, correct the position error manually:

a) Start VNC and get into the VNC menu by pressing "Print Screen" twice.

b) Use the arrow keys to move the screen around.

If black bars: move left (or up) until the first non-black area touches the edge of the VNC window.

If cut-off screen: move the window right (or down) repeatedly (the edge will smear). Press "ESC" to quit the menu (which causes a re-draw) and start the process over.

Press "ESC" at any time to re-draw the whole screen and check the result. The screen drawn by VNC is only an approximation of what the new position will look like.

1. You can fine-tune the position by observing the remote mouse position relative to the VNC local cursor (small box). When they are precisely aligned on top of each other, you should have the optimal screen position. The new X, Y position will be remembered automatically on this Unit. This process may need to be repeated for other video modes.

When I connect to the Unit with the browser and open a session window, I get black video and the "Connect, Disconnect" options keep toggling. I am able to connect locally, through VNC and via telnet. What do I do?

1. The problem could be a configuration issue. Check the "Java Viewer port number (clear)" and "Java viewer port number (SSL)". These numbers must be different port numbers from the web server whose default is 80 and 443. Reset the two ports to 19900 and 19901, respectively, which are the factory defaults.

When I try to upload my firmware, I receive a message that the file is not found.

1. Some versions of Internet Explorer cannot upload the firmware image (or any other file) if any part of the file path contains a space. This is a problem, for example, if the file "Image.frm" is stored as "C:\My Document\Image.frm". The solution is to use Netscape, or move the file to be uploaded into another directory that does not contain spaces in its file path.

For additional technical support, contact Belkin technical support at
1.800.223.5546 ext. 2263.

FCC Statement

DECLARATION OF CONFORMITY WITH FCC RULES FOR ELECTROMAGNETIC COMPATIBILITY

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

F1DE101N

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 Components, declare under our sole responsibility that the F1DE101N 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 Components Limited One-Year Product Warranty
Belkin Components 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, INCLUDING, 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 Components

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 Components, Ltd.

7 Bowen Cresent • West Gosford
NSW 2250 • Australia
Tel: +61 (2) 4372 8600
Fax: +61 (2) 4325 4277

P74045