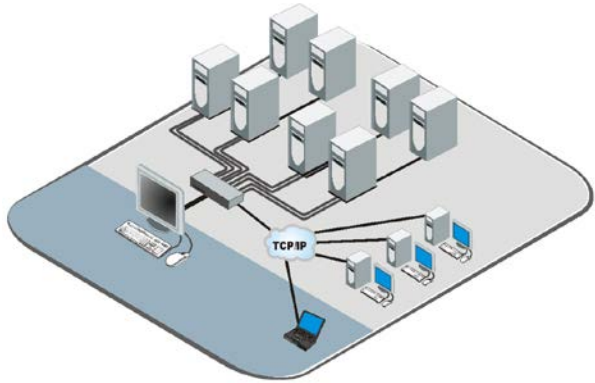


Vista Remote 2

SINGLE USER REMOTE KVM ACCESS OVER IP

INSTALLATION AND OPERATIONS MANUAL



ROSE.COM



LIMITED WARRANTY

Rose Electronics® warrants Vista Remote 2™ to be in good working order for one year from the date of purchase from Rose Electronics or an authorized dealer. Should this product fail to be in good working order at any time during this one-year warranty period, Rose Electronics will, at its option, repair or replace the Unit as set forth below. Repair parts and replacement units will be either reconditioned or new. All replaced parts become the property of Rose Electronics. This limited warranty does not include service to repair damage to the Unit resulting from accident, disaster, abuse, or unauthorized modification of the Unit, including static discharge and power surges.

Limited Warranty service may be obtained by delivering this unit during the one-year warranty period to Rose Electronics or an authorized repair center providing a proof of purchase date. If this Unit is delivered by mail, you agree to insure the Unit or assume the risk of loss or damage in transit, to prepay shipping charges to the warranty service location, and to use the original shipping container or its equivalent. You must call for a return authorization number first. Under no circumstances will a unit be accepted without a return authorization number. Contact an authorized repair center or Rose Electronics for further information.

ALL EXPRESS AND IMPLIED WARRANTIES FOR THIS PRODUCT INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO A PERIOD OF ONE YEAR FROM THE DATE OF PURCHASE, AND NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WILL APPLY AFTER THIS PERIOD. SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF THIS PRODUCT IS NOT IN GOOD WORKING ORDER AS WARRANTED ABOVE, YOUR SOLE REMEDY SHALL BE REPLACEMENT OR REPAIR AS PROVIDED ABOVE. IN NO EVENT WILL ROSE ELECTRONICS BE LIABLE TO YOU FOR ANY DAMAGES INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR THE INABILITY TO USE SUCH PRODUCT, EVEN IF ROSE ELECTRONICS OR AN AUTHORIZED DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

IBM, AT, and PS/2 are trademarks of International Business Machines Corp. Microsoft and Microsoft Windows are registered trademarks of Microsoft Corp. Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owner.

Copyright Rose Electronics 2008. All rights reserved.

No part of this manual may be reproduced, stored in a retrieval system, or transcribed in any form or any means, electronic or mechanical, including photocopying and recording, without the prior written permission of Rose Electronics.

FCC / IC STATEMENTS, EU DECLARATION OF CONFORMITY

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO-FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses and can radiate radio frequency energy and if not installed and used properly, that is in strict accordance with the manufacturer's instructions may cause interference to radio communication. It has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment complies with the requirements of the European EMC directive 89/336/EEC in respect of EN55022 (Class B), EN50082-1 and EN60555-2 standards and the Low Voltage Directive.

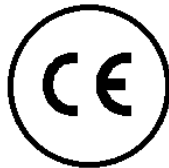


TABLE of CONTENTS

Contents	Page #
System Introduction.....	1
Features	2
Package contents	2
Rose Electronics web site	3
Product Registration.....	3
System Overview	4
Vista Remote 2 Models	5
Vista Remote 2 Installation	6
Connecting the KVM station.....	6
Connecting the Computers	7
Connecting to the network	7
Configuring the Vista Remote 2 IP Input module.....	8
Connecting Remotely	13
Remote Configuration.....	14
User Accounts	15
Unit Configuration.....	16
Unit Advanced Configuration	17
Time and Date Configuration.....	19
Network Configuration	20
Host Configuration.....	21
Logging and Status	22
KVM Switch Module Configuration	24
Change the computer names.....	25
Configure appearance	26
Configure security	28
Configure mouse type.....	29
Configure keyboard type.....	30
Configure miscellaneous.....	31
Save	32
Exit	32
Remote System Operation	33
Connecting using a web browser	33
VNC Viewer Toolbar.....	34
Controls Tab.....	35
Host Tab.....	37
Keyboard Commands.....	39
Keyboard command description.....	40
Troubleshooting.....	42
Maintenance and Repair.....	45
Technical Support	45

Figures	Page #
Figure 1. Vista Remote 2 Models	5
Figure 2. Connecting a KVM.....	6
Figure 3. Connecting Computers	7
Figure 4. Connecting to the Network.....	7
Figure 5. Configuration OSD.....	8
Figure 6. Unit Configuration OSD.....	8
Figure 7. Network Configuration.....	10
Figure 8. Secure Key calculation.....	11
Figure 9. Standard Logon screen.....	11
Figure 10. Control menu	12
Figure 11. Remote Configuration Menu	14
Figure 12. User Accounts	15
Figure 13. Unit Advanced Configuration.....	17
Figure 14. Time and Date Configuration	19
Figure 15. Configure Network	20
Figure 16. Configure Host.....	21
Figure 17. KVM Switch Module OSD	24
Figure 18. Change computer names.....	25
Figure 19. Change appearance	26
Figure 20. Switch module security settings	28
Figure 21. Configure mouse type.....	29
Figure 22. Configure Keyboard.....	30
Figure 23. Configure Misc.....	31
Figure 24. Save Switch settings.....	32
Figure 25. VNC Viewer Toolbar	34

Tables	Page #
Table 1. Keyboard Commands	40

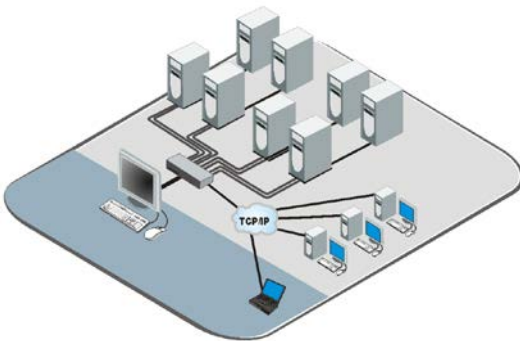
Appendices	Page #
Appendix A – General specifications.....	48
Appendix B – Part Numbers.....	48
Appendix C – RackMount	49
Appendix D – IP Access Control	50
Appendix E – VNC Viewer connection options.....	52
Appendix E – VNC viewer window options.....	58
Appendix F – Browser viewer options	59
Appendix G – Supported video modes.....	61
Appendix H – Typematic Rate	62

System Introduction

Thank you for choosing Vista Remote™ 2 from Rose Electronics for your network access solutions. This intelligent and innovative product is the result of Rose Electronics commitment to providing state of the art, economical switching solutions for today's demanding workplace. Vista Remote 2, when installed and connected to your network, allows you full access and control of the connected computers from the built in viewer client or any web browser from almost anywhere. This flexible and powerful product uses the Real VNC client software that is designed for very secure, encrypted, and password protected exchange of information between the computers and the remote viewer. The Vista Remote 2 sets a new standard for an easy and very secure way to remotely manage The Vista Remote 2 is available in a 4 port or 8 port model.

The Vista Remote 2 is different in the way it manages remote access to your systems. All of the computers that will be remotely connected remain completely unchanged and can run their usual operating system normally. They only need to be connected to the Vista Remote 2 unit. Being totally operating system independent, a user can remotely connect to different computers with no problem.

Whatever your remote accessing needs are, the versatility of the Vista Remote 2 from Rose Electronics can fulfill those needs. It can be installed at any network level and connected to computers running most operating system.



Installing the Vista Remote 2 consists of:

1. Configuring the unit to be compatible and accessible with your network
2. Connecting the unit to a local KVM station
3. Connecting your computers to access and
4. Connecting to the network

Once installed and configured you have full control of the selected computer provided your security profile permits it.

The Vista Remote 2 consists of an IP input module and a KVM switch module. Each module serves a unique purpose in access control and KVM switching control. The IP input module controls the accessibility, security, and state-of-the-art encryption to the unit. It can be accessed locally, remotely over your network, or from any workstation connected to the internet. All access methods require a user ID and password to gain access to the units IP input module. Access to the units IP input module from any remote user is via any supported web browser. The Vista Remote 2 is further enhanced by the use of Real VNC that allows for the creation of ciphered user communications. Additionally, an optional user ID and password and other set-up parameters can be set-up to gain access and use the KVM switch module. This additional user ID can be set-up for each user needing access to the KVM switch module.

Features

- Models available:
 - 4-port model
 - 8-port model
- Solid-state embedded unit, has no disk drive for maximum reliability
- Remote application (Real VNC or Java applet) can be installed directly from the unit
- Local KVM port for configuring and direct access to the connected computers
- Connect to the unit directly, from a network workstation, or over IP using any supported web browser.
- Access remote computers by simple keyboard commands or an on-screen list of computers
- Supports video resolution up to 1600 x 1200 @ 75hz
- Password security prevents unauthorized configuration and Unit access
- Remote access requires a user ID and password.
- IP lockout feature for incorrect login (IP address shown as "Blacklisted" in log file)
- All transmissions to and from a remote user are encrypted with the latest AES 128 bit encryption technology.
- Up to 16 remote user accounts can be set-up each with separate access permission levels.
- Scan function sequences through the connected computers at rates of 1 to 999 seconds
- Four different screen savers are available
- Rack mount kits available for 19", 23", or 24" racks

Package contents

The package contents consist of the following:

- The Vista Remote 2 unit
- RJ12 Serial Cable
- +5VDC Power Adapter / Power cord
- Installation and operations manual CD
- Quick Start Guide

Cables are usually ordered separately. If the package contents are not correct, contact Rose Electronics or your reseller so the problem can be quickly resolved.

Rose Electronics web site

Visit our web site at www.rose.com for additional information on Vista Remote 2 and other products offered by Rose Electronics that are designed for data center applications, classroom environments, and many other access and switching applications.

Product Registration

Take advantage of the following when you register your Rose Electronics products online at <http://www.rose.com/htm/online-registrationform.htm>:

- Rose Standard Warranty *Plus...*
- Free Lifetime Firmware Updates
- Free Lifetime Technical Support
- 30 Day Money Back Guarantee
- Priority “First-in-Line” Status for Tech Support

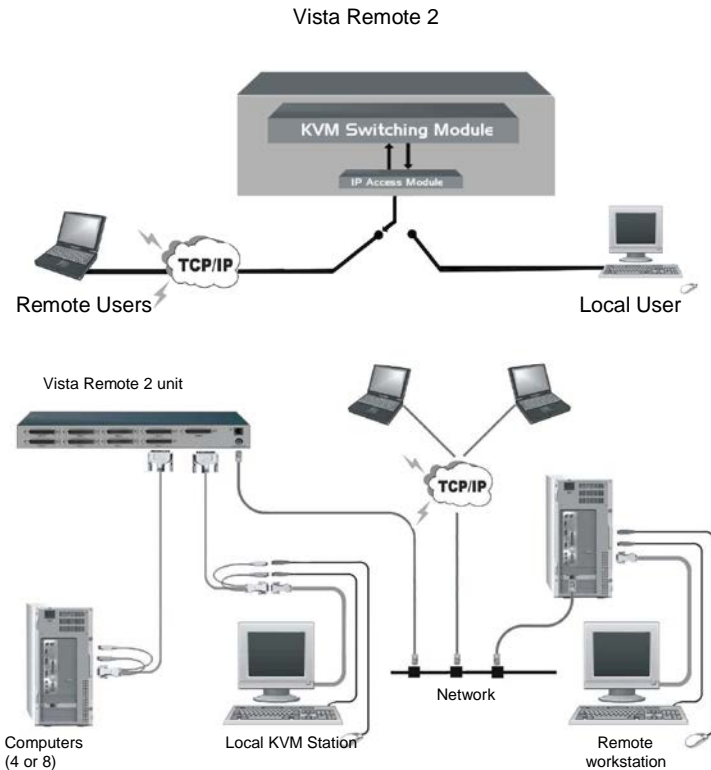
System Overview

Vista Remote 2 is a versatile and powerful product that can extend the range of access to your computers from anywhere in the world. It is designed to provide seamless and trouble-free access from any workstation on your network or any remote user to any connected computer. You can connect to and control any of the connected computers by simple keyboard commands or an on-screen list of computers. Each computer can be assigned a unique name that makes sense for your system. Names like sales, production, and administration make it easy to recognize and connect to.

Access control for the users can be set-up to provide access restrictions to the configuration menus and the unit. The installation and configuration section explains all the features and functions of the Vista Remote 2 and how to customize it to fit your business needs.

The Vista Remote 2 is designed with the highest regard for security. Remote access requires a user ID and password. All transmissions, to and from a remote workstation and Vista Remote 2 uses the versatile and very secure RealVNC viewer and are encrypted with the latest encryption technology. Login, time-out, User ID and password add to the security of the system.

The UltraView Remote 2 consists of an IP input module and a KVM switch module. Each module serves a unique purpose in access control and KVM switching control. The IP input module controls the accessibility, security, and state-of-the-art encryption to the unit. The KVM switching module controls and manages the CPU port switching.



Typical connection diagram

Vista Remote 2 Models

 <p>(Part Number KVL-1R4UA/OV/2)</p>	<table border="1"> <thead> <tr> <th>Connector</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>Power Adapter</td> <td></td> </tr> <tr> <td>CPU (4)</td> <td>DB25F</td> </tr> <tr> <td>KVM (1)</td> <td>DB25F</td> </tr> <tr> <td>RS232</td> <td>RJ11F</td> </tr> <tr> <td>LINK</td> <td>RJ45F</td> </tr> </tbody> </table>	Connector	Type	Power Adapter		CPU (4)	DB25F	KVM (1)	DB25F	RS232	RJ11F	LINK	RJ45F
Connector	Type												
Power Adapter													
CPU (4)	DB25F												
KVM (1)	DB25F												
RS232	RJ11F												
LINK	RJ45F												

 <p>(Part Number KVL-1R8UA/OV/2)</p>	<table border="1"> <thead> <tr> <th>Connector</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>Power Adapter</td> <td></td> </tr> <tr> <td>CPU (8)</td> <td>DB25F</td> </tr> <tr> <td>KVM (1)</td> <td>DB25F</td> </tr> <tr> <td>RS232</td> <td>RJ11F</td> </tr> <tr> <td>LINK</td> <td>RJ45F</td> </tr> </tbody> </table>	Connector	Type	Power Adapter		CPU (8)	DB25F	KVM (1)	DB25F	RS232	RJ11F	LINK	RJ45F
Connector	Type												
Power Adapter													
CPU (8)	DB25F												
KVM (1)	DB25F												
RS232	RJ11F												
LINK	RJ45F												

Figure 1. Vista Remote 2 Models

Vista Remote 2 Installation

Installing the Vista Remote 2 is a very easy process and should be performed by a designated administrator. The administrator will install, configure, and set-up user access profiles. A network administrator will need to assign an IP address to the unit (if needed) and set-up firewall and network access to the unit.

The following installation procedure is a guide to properly install and configure the Vista Remote 2. The following items are needed to install the Vista Remote 2:

1. A valid IP address to assign to the unit (if not using DHCP feature)
2. VGA monitor
3. PS/2 keyboard
4. PS/2 mouse
5. RJ45 network cable
6. KVM Adapter cable (DB25M to PS/2F-PS/2F-HD15F)
7. CPU Adapter cable(s) (DB25M to PS/2M-PS/2M-HD15M)

Connecting the KVM station

Connect the KVM stations PS/2 keyboard, video monitor and PS/2 mouse cables to the corresponding connectors on the KVM adapter cable as shown in Figure 2. The KVM station's video monitor should be equal or better than any of the connected computers. Connect the DB25M end of the KVM cable to the KVM DB25F port on the rear panel of the Vista Remote 2 unit.

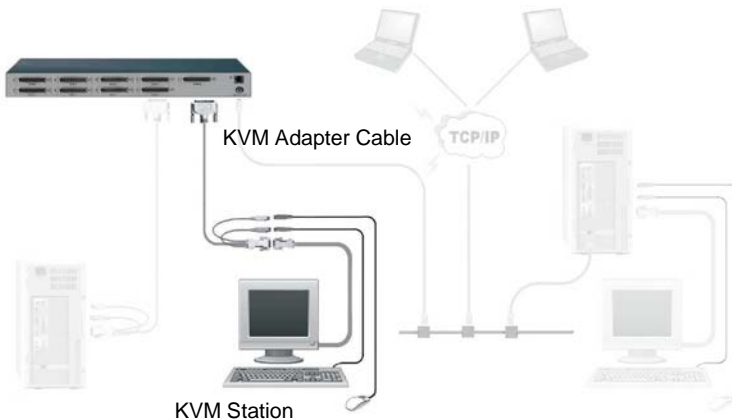


Figure 2. Connecting a KVM

Connecting the Computers

Connect each computer to the Vista Remote 2 using the appropriate CPU adapter cable designed to interface to the type of computer being connected (PS/2, Unix, SUN, DEC, Apple, etc). Connect the DB25M end of the CPU adapter cable to the desired DB25F CPU port on the rear panel of the unit. Connect the other end of the cable to the corresponding ports on the computer (keyboard, monitor, and mouse). Refer to Figure 3.

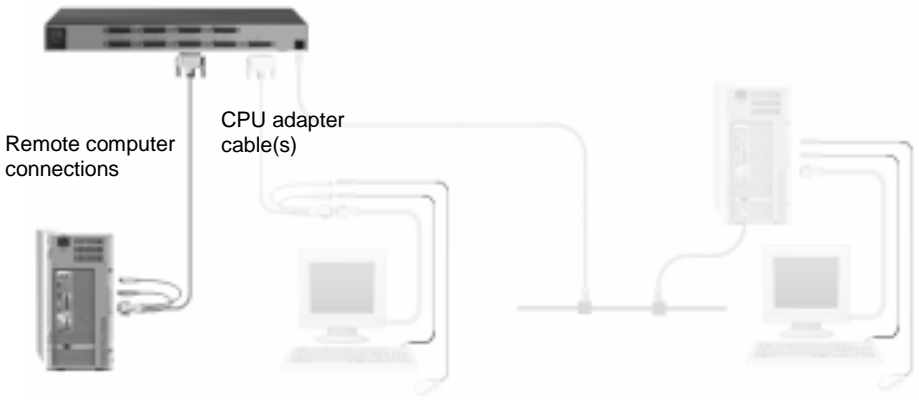


Figure 3. Connecting Computers

Connecting to the network

Connect a network cable from the RJ45 connector on the rear panel of the Vista Remote 2 and to your network (See Figure 4)

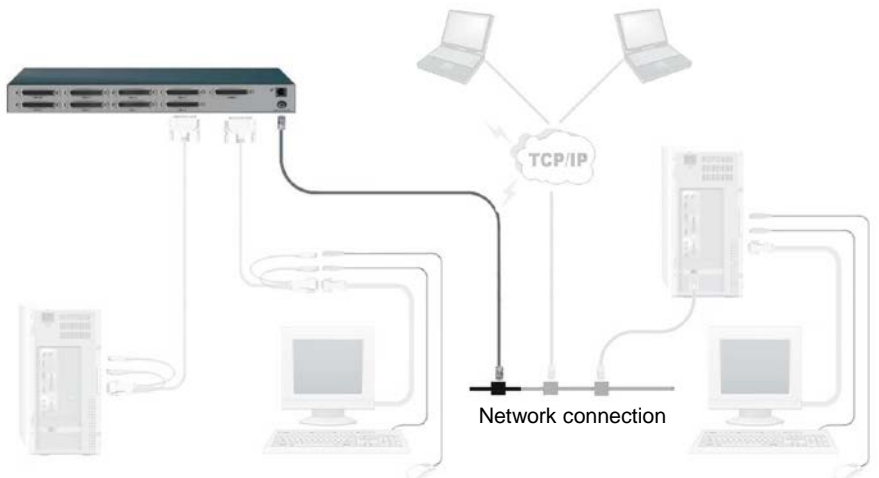


Figure 4. Connecting to the Network

Configuring the Vista Remote 2 IP Input module

When you **locally** connect to Vista Remote 2 unit for the first time the Unit and Network must be configured. Follow the recommended procedure below to configure all models:
Make all cable connections to the KVM station, network, and computers
Apply power to all devices (Computers, Vista Remote 2, and Monitor).
Make sure a computer is connected to CPU port #1 and that computer is powered on.
If no computer is connected to port #1, the OSD menu screens may not sync.
With power applied, a standard login screen will display on the KVM monitor
Login on to the unit using the default user ID, **admin** and no password
After a successful login, the remote computer's video will display on the KVM monitor.
Press the CTRL + ALT + C keys simultaneously to display the configuration menu options as shown below: (Unit connection screen may display after initial connection is made)

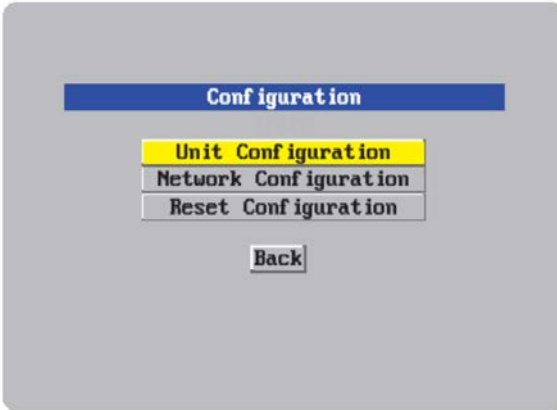


Figure 5. Configuration OSD

Select "Unit Configuration" and the below screen will display



Figure 6. Unit Configuration OSD

Hardware

The hardware version level is displayed in this field.

Firmware

The Vista Remote 2 firmware version is displayed in this field

Keyboard Layout

Using the left and right arrow keys, select the keyboard type expected from the host computers.

Admin password

Enter an administrator password of at least six characters that has a mix of letters and numerals. The background color provides an indication of password suitability. It is initially red to indicate that the password is not sufficient. When a password with reasonable strength has been entered it changes to blue.

Unit Name

You can assign a unit name to the Vista Remote 2.

Hot Keys

Use the left and right arrow keys to select a different hot key combination. This hot key combination is used to invoke the OSD menu and other keyboard commands

Screen saver

Use the left and right arrow keys to set the time for the screen saver to activate.

Time and Date

Set the time and date to the correct values. Use the 24 hour base inputs. All entries in the activity log are time stamped using this information.

Encryption

Arrange this setting according to your security requirements.

When all items have been updated, click on "Next" to configure the network information. The network information entered (IP Address, Net Mask, and Gateway) must be compatible with the network Vista Remote 2 will be connected to.

Configuring the Network

The screenshot shows a 'Network Config' window with the following fields and values:

MAC Address	0040A4:100023
Use DHCP	No
IP Address	192.168.1.42
Net Mask	255.255.255.0
Gateway	192.168.1.2
UNC Port	5900
HTTP Port	80

At the bottom of the window, it says 'Screen 2 of 4' and has a 'Next' button.

Figure 7. Network Configuration

MAC address

Media Access Control Address – this is the unique and unchangeable code that was hard coded within your Vista Remote 2 unit when it was built. It consists of two 6-digit hexadecimal (base 16) numbers separated by colons. A section of the MAC address identifies the manufacturer, while the remainder is effectively the unique electronic serial number of your particular unit

Use DHCP/IP address/Net Mask/Gateway/VNC port/HTTP Port

1. You need to either set the DHCP option to 'Yes' or manually enter a valid IP address, Net mask and Gateway. If you set the option to use DHCP, remote users must be informed of the IP address assigned so they can remotely access the unit.
2. Change the IP Address to the IP address assigned to the unit by your network administrator that is compatible with your network.
3. Change the Net Mask and Gateway addresses if needed.
4. The VNC and HTTP ports should remain set to 5900 and 80, respectively, unless they clash with an existing setup within the network.
5. When all network information has been entered, click on "Next" to calculate a "Secure Key".

Screen #3 is a secure keys screen that will display after the network information has been entered.



Figure 8. Secure Key calculation

This screen uses mouse movements and keyboard inputs to create random data. This unpredictable information is then combined with several other factors to develop the basis of the encryption keys that are used to establish secure remote links.

With every mouse move and key press the single dash will move across the progression bar (unless the same key is pressed repeatedly). Periodically, a new star character will be added to the bar as the random data are accepted as part of the new encryption key. When the bar is full, the final encryption keys for your Vista Remote 2 will be created – this process takes roughly 30 to 40 seconds.

Once the secure key has been calculated, the Vista Remote 2 will restart and present a standard logon screen as shown below. Logon to the unit with the correct Username and password.



Figure 9. Standard Logon screen

To view the menu options press <CTRL> <ALT> <C>. (If the default hotkeys were altered on the Configure Unit screen, use the new hotkeys plus C)

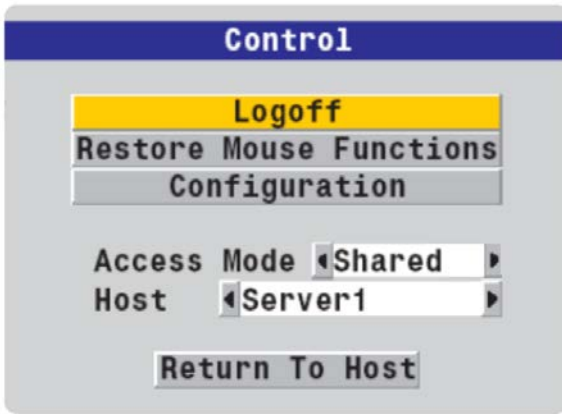


Figure 10. Control menu

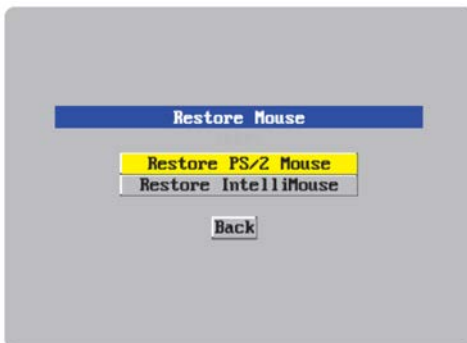
Logoff

Select this option to close your current session and display the screensaver.

Restore mouse functions

Select this tab to revive a mouse that has ceased to function correctly. The Vista Remote 2 provides a feature to reinstate PS/2 mouse communications. (Does not apply if using a USB mouse.)

There are two main types of data formats used by current PC mice; 'PS/2' format and the more recent IntelliMouse® format introduced by Microsoft. These use slightly different data arrangements and it is important to know which type was being used before you hot-plugged the computer to the Vista Remote 2. The previous setting depends both on the type of mouse and the type of driver, as various combinations of PS/2 and IntelliMouse are possible. Using the incorrect restore function may produce unpredictable results and require the computer to be rebooted.



Using a keyboard and monitor directly connected to the Vista Remote 2, log on and then press the hotkey sequence <Ctrl> <Alt> <C> to view the options menu.

1. Select the 'Restore mouse functions' option to display:
2. Select one of the following options:
3. *Restore Standard Mouse* – if PS/2 mode is required, or *Restore IntelliMouse* – if IntelliMouse mode is required.
4. Select "Back" to return to the Control menu.

Configuration

Select the “Configuration” tab to gain access to the Unit and Network configuration menus. You can also reset the Vista Remote 2 to its initial state.

Access mode

Allows you to choose between the Shared mode (where all other logged on users can see your operations) and the Private mode (where the screens of all other users are blanked).

Host

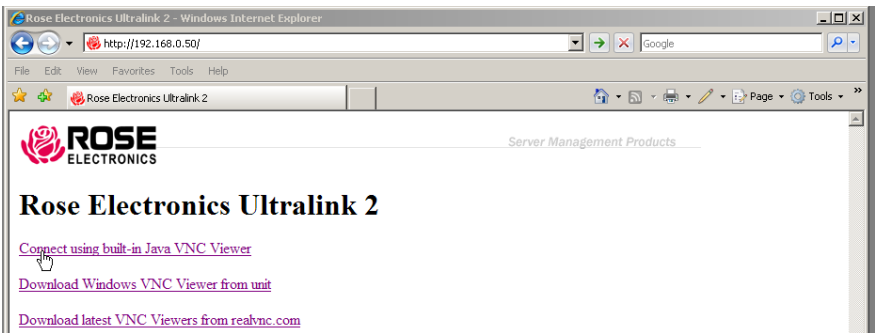
Indicates the currently selected host computer and allows you to select others. This item will be blank unless host details have been set-up.

Return to host

Quits the menu and returns to the host screen.

Connecting Remotely

With the Unit and the Network configured properly, start a web browser like IE or Netscape from any workstation connected to the same network your Vista Remote 2 is connected to. Type in the Vista Remote 2’s assigned IP address (Example (<http://168.192.0.41>) in the URL field. The Vista Remote 2 will respond with the below screen. There may be initial login and connect screens displayed.



(NOTE: See Appendix E for additional VNC Viewer options)

Click on the “Connect using built-in Java VNC viewer” option and the Vista Remote 2 will install a temporary Java applet on the requesting computer and then display the connected computer’s video in the browser’s VNC viewer window. In the upper right corner of the window is a “Configure” tab. Click on this tab to display the remote configuration option menu as shown below.

Remote Configuration

Connect **remotely** to the Vista Remote 2 unit from any network workstation. When connected, click on the “Configure” tab in the upper right corner of the display. The below configuration menu will display. Some of the remote configuration menus are similar to the local configuration menus.

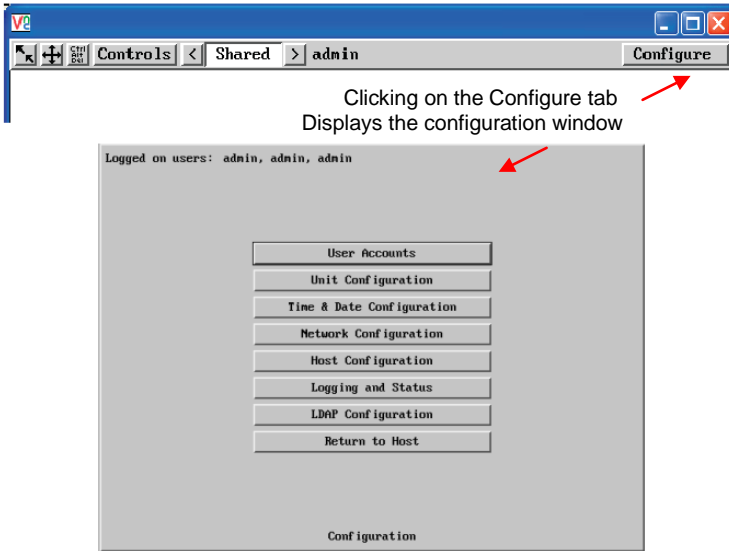


Figure 11. Remote Configuration Menu

(Following describes each of the Configuration Tabs.)

User Accounts	Allows you to create and manage up to sixteen separate user accounts, each with separate access permissions. Account #1 is the admin account. Enter User name, password. Tick/un-tick the Local and Remote options that are appropriate to the user.
Unit Configuration	Allows you to modify unit settings within the Vista Remote 2. You can define the keyboard, set-up the admin account, assign a name to the unit, screensaver time and encryption options
Time & Date	Set the time and date, this time stamps the log files
Network Configuration	Configures the network IP, network mask, gateway, VNC port, HTTP port. You can alter any of the existing network settings plus you can set-up the IP access control feature that lets you specifically include or exclude certain addresses or networks
Host Configuration	Allows configuration of various details for each host system connected to Vista Remote 2. 128 entries max, Add host names, Users and Hotkey.
Logging and Status	Provides various details about the Vista Remote 2 activity
LDAP Configuration	Configures unit for LDAP
Return to Host	Exit the configuration menu system and return to the host computer

User Accounts

Selecting user accounts will display the following menu.

Logged on users: admin

User Name	Password	Local	Remote	Auto Logon
admin	*****	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save User Configuration Cancel

Figure 12. User Accounts

The first of the sixteen accounts is the admin account and is the only account with access rights to the configuration menus. The user name and access rights are fixed for the admin account. The only change possible for this account is the password.

There are fifteen user account positions.

To create a new account

- 1 Enter the required User Name to activate that position (the Password, access tick boxes, and Auto Logon positions will become editable).
- 2 Optionally enter a password for the user account.
- 3 Tick/un-tick the Local, Remote, and the Auto Logon options that are appropriate to the user.
(A tick indicates the user has permission for that function)
- 4 Click the Save button to register your changes.

User Name - 1-16 characters max, **lower case characters or numbers only**. No symbols or upper case characters are permissible.

Password - 1-16 characters max, **case sensitive** and can include certain keyboard symbols. The password background remains amber while the Vista Remote 2 considers your entered password to be too easy to guess. A suitable password is best constructed using a mixture of more than 6 letters, numbers and punctuation characters.

Local - When ticked, the selected user can gain access using the local KVM station directly connected to the Vista Remote 2.

Remote - When ticked, the selected user can gain access via an IP network link, such as a local intranet or the wider Internet (depending on how the Vista Remote 2 is connected and the network access is configured.).

Auto Logon - When ticked, and the unit is powered on, logs in a single user that is set for auto logon only if the user is allowed local access.

Unit Configuration

The 'Unit Configuration' option tab will display the following menu.

Logged on users: admin

Hardware Version:

Firmware Version:

Host Keyboard Layout: < US >

Admin Password: *****

Unit Name: *192.168.0.50

Local Hot Key Sequence: < Ctrl+Alt >

Screensaver Timeout: < Off >

Menu Bar Toggle Hot Key: < None >

Display Menu Bar for New Connections:

Encryption: < Always On >

Console Configuration Advanced Unit Configuration

Save Unit Configuration Cancel

Hardware Version

Indicates the version of the electronic circuitry within the Vista Remote 2 unit.

Firmware Version

Indicates the version of the hardwired software within the Vista Remote 2 flash memory. This may be updated using the flash upgrade procedure.

Host Keyboard Layout

Use the arrow buttons to match the keyboard layout expected by the host system.

Admin Password

Enter the password that will be used to gain administrator access to the Vista Remote 2. There can only be one admin user and only that user is given access to the configuration menus.

Unit Name

The name entered here will be displayed on the local menus and the remote VNC viewer/browser windows.

Local Hot Key Sequence

Use the arrow buttons to select an appropriate hot key sequence for the locally connected keyboard. This sequence is used in combination with other key presses to access the on-screen menus and to change between hosts. The options are: Ctrl+Alt (default), Ctrl+Shift, Alt+Shift, Alt Gr, Left + Right Alt, Left Ctrl + Alt or Right Ctrl + Alt.

Screensaver Timeout

Use the arrow keys to select an appropriate period of inactivity before a screensaver is displayed and the user is logged out. This setting applies to local users only and once the screensaver is displayed, for security purposes the user is required to log in again. The timeout period can be selected between 5 minutes and 1 day (24 hours), it cannot be disabled.

Encryption

Three encryption options are available; Always on, Prefer off, Prefer on. The one to choose depends on the specific details of your installation. The use of encryption imposes a slight performance overhead of roughly 10% but is highly secure against third party intrusion.

Encryption settings

The Unit configuration page offers three encryption settings:

- Always on - This setting will force all viewers to use encryption. *Note: This setting will preclude any VNC viewer versions that do not support encryption.*
- Prefer off - This setting does not enforce encryption unless a viewer specifically requests it. If a viewer has its 'Let server choose' setting, then an un-encrypted link will be set up.
- Prefer on - This setting generally enforces encryption unless an earlier viewer version is unable to support it, in which case the link will be un-encrypted. If a viewer has its 'Let server choose' setting, then the link will be encrypted.

Unit Advanced Configuration

The "Advanced Configuration" tab will display advanced options that generally do not need modifying.

Logged on users: admin

Force VNC Protocol 3.3	<input type="checkbox"/>
Idle Timeout (minutes)	60
Protocol Timeout (seconds)	20
Background Refresh Rate	< Medium >
Mouse Latency Allowance (milliseconds)	0
Mouse Rate (milliseconds)	20
Single Mouse Mode Mouse Switch	< Disabled >
Use Quick Mouse Calibration	<input checked="" type="checkbox"/>
Behaviour for admin connections when limit reached	< Replace oldest connection >
Use VESA GTF	<input checked="" type="checkbox"/>
Enable Virtual Media	<input checked="" type="checkbox"/>

Upgrade Firmware Reset Unit

Save Advanced Unit Configuration Cancel

Figure 13. Unit Advanced Configuration

Force VNC protocol 3.3

IMPORTANT: The use of this option is not recommended. VNC protocol 3.3 is a legacy version that does not offer any encryption.

Idle timeout

Determines the period of inactivity on a remote connection before the user is logged out. The idle timeout period can be set to any time span, expressed in minutes. Note: The [Screensaver](#) option serves a similar purpose for local connections. A value of 0 will disable the timeout.

Protocol timeout

Sets the time period by which responses should have been received to outgoing data packets. If the stated period is exceeded, then a connection is considered lost and terminated.

Mouse Latency Allowance

This option is used during calibration to account for latency delays (caused as signals pass through a device) introduced by some KVM switches. During calibration, the Vista Remote 2 waits for 40ms after each mouse movement before sampling the next. If a KVM device adds a significant delay to the flow of data, the calibration process can be lengthened or may fail entirely. The value entered here is added to (or subtracted from) the default 40ms sampling time.

Note: You can enter negative values (down to -40) in order to speed up the calibration process. Use this option with caution as it can adversely affect the calibration process.

Mouse rate

Defines the rate at which mouse movement data are transmitted to the system. The default option is 20ms, which equates to 50 mouse events per second. This default rate can prove too fast when passed through certain connected KVM switches. In such cases, data are discarded causing the local and remote mouse pointers to drift apart. If this effect is encountered, increase the mouse rate to around 30ms (data are then sent at a slower rate of 33 times per second).

Background refresh rate

Use the arrow keys to alter the refresh rate for screen images via remote links. This allows you to tailor the screen refresh to suit the network connection speeds. The options are: Slow, Medium, Fast or Disabled. When the disabled option is selected, the remote users will need to manually refresh the screen.

Note: When a low connection speed is detected, the background refresh is automatically disabled, regardless of the settings of this option.

Single Mouse Mode Mouse Switch

This option allows you to select the mouse button combination that can be used to exit from single mouse mode (when active). Options are: Disabled, Middle+Right Button, Middle+Left Button.

Behavior for admin connections when limit reached

Use the arrow keys to modify the action taken when the number of admin connections is reached. The options are:

- Replace oldest connection
- Replace newest connection
- Don't replace

Use VESA GTF

When ticked, the VESA Generalized Timing Formula will be used to help determine the correct input video resolution and timing details. See Appendix G for a list of all supported video modes.

Upgrade Firmware

The Upgrade Firmware tab allows you to easily update the firmware when changes and enhancements have been made to the Vista Remote 2.

Reset Unit

The reset unit tab, when selected, will reset the Vista Remote 2 unit to factory defaults. All user settings that have been entered will be replaced with the factory default settings.

Time and Date Configuration

Logged on users: admin

Time And Date

Timezone specifier (e.g. EST5)

Use NTP

NTP Server IP address

Set Time from NTP Server

Save Time & Date Configuration Cancel

Figure 14. Time and Date Configuration

Use the left and right arrow keys to select the correct time and date. The time entry uses the 24 hour clock notation. The internal real time clock will continue to run for roughly one week without power to the Vista Remote 2, after that it will be lost and require resetting. Use the up and down arrow keys to move between each of the sections within the time and date entries.

If you wish to use an NTP server to obtain the date and time, check the Use NTP box, enter the NTP Server IP address, and click on "Set Time from NTP Server".

When all information has been entered, click on the "Save" tab to save the information.

Network Configuration

This menu allows you to **remotely** configure various aspects of the IP port and its relationship with the local network.

Logged on users: admin

MAC address: 00:0F:5B:01:1F:6E

Use DHCP

IP Address

IP Network Mask

IP Gateway

UNC Port 5900

HTTP Port (0=disabled) 80

IP Access Control

Add Remove Up Down Edit

+0.0.0.0/0.0.0.0

Save Network Configuration Cancel

Figure 15. Configure Network

MAC address

Media Access Control Address – this is the unique and unchangeable code that was hard coded within Vista Remote 2 unit when it was built. It consists of two 6-digit hexadecimal (base 16) numbers separated by colons. A section of the MAC address identifies the manufacturer, while the remainder is effectively the unique electronic serial number of your particular unit.

Use DHCP

DHCP is an acronym for 'Dynamic Host Configuration Protocol'. Its function is particularly useful when connecting to medium size or larger networks. When this option is selected, your Vista Remote 2 will attempt to locate a DHCP server on the network. If such a server is located, it will supply three things to the Vista Remote 2: an IP address, an IP network mask (also known as a Subnet mask) and a Gateway address. These are not usually granted permanently, but on a 'lease' basis for a fixed amount of time or for as long as the Vista Remote 2 remains connected and switched on. Remote users must be informed of this IP address in order for them to successfully connect to the Vista Remote 2 unit.

IP Address

This is the identity of the Vista Remote 2 within a network. The IP address can be altered to suit the network it is connected on. It can either be entered manually or configured automatically using the DHCP option. When the DHCP option is enabled, this entry is grayed out.

IP Network Mask

Also often called the subnet-mask, this value is used alongside the IP address to help define a smaller collection (or subnet) of devices on a network. In this way a distinction is made between locally connected devices and ones that are reachable elsewhere, such as on the wider Internet. This process helps to reduce overall traffic on the network and hence speed up connections in general.

IP Gateway

This is the address of the device that links the local network the Vista Remote 2 is connected to another network such as the wider Internet. Usually the actual gateway is a network switch or router and it will be used whenever a required address lies outside the current network.

VNC Port

This is the logical link through which communications with a remote VNC viewer will be channeled. The default setting is 5900 which is a widely recognized port number for use by VNC software. However, in certain circumstances it may be advantageous to alter this number.

HTTP Port

This is the logical link that communications with a remote web browser will be channeled. The default setting of 80 is an established standard for web (HTTP – HyperText Transfer Protocol) traffic though this can be changed to suit your local network requirements.

IP Access Control

This section allows you to optionally specify ranges of addresses which will or will not be granted access to the Vista Remote 2. If this option is left unchanged, then the default entry of '+0.0.0.0/0.0.0.0' ensures that access from all IP addresses will be permitted. If this feature is needed, please see Appendix D for a detailed explanation of IP access control.

Host Configuration

The Host Configuration menu allows you to configure various details for each of the host systems that may be connected to the Vista Remote 2. Each of the entries can be configured with a name, the permitted users, and the hot key combinations to switch to it. Depending on the model, enter names for 4 or 8 host computers.

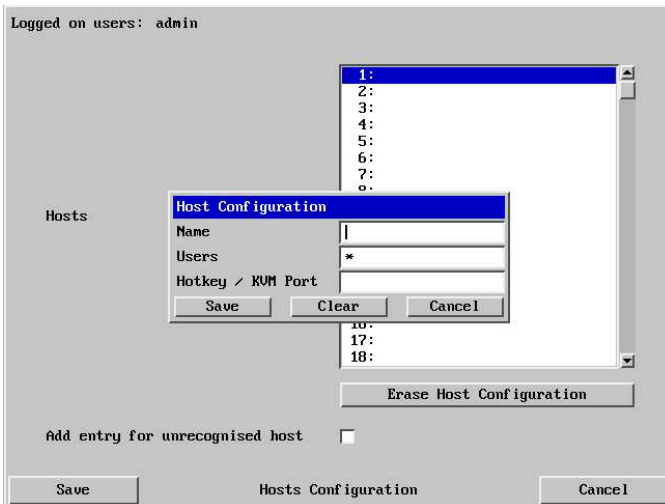


Figure 16. Configure Host

Click on the “Erase Host Configuration” tab to remove all host entries if needed.

Check the box “Add entry for unrecognized host” to add any system connected to that is not specified in the Host list. Verify these added hosts for the correct Hot key sequence and user permission.

It is recommended that the naming and hot key assignments for each Host Configuration entry match the CPU port configuration of the Vista Remote 2.

Entry #1 - Name and hot key defined to switch to CPU port #1, Entry #2 for CPU port #2, etc. Examples of Hot key sequences for switching to a given port are shown below.

Name

Enter the name that will be displayed in the viewer window when you click the Host button.

Users

Select the users that will be permitted to connect to this host. Either enter * to allow all users or a list of users separated by commas (e.g. sales, admin, eng, david). Names must be set-up on the user accounts menu and match these names.

Hotkey / KVM Port

Declare the hot key sequence, or Remote Port Direct address that will cause the KVM switch module to link with the required host system. Remote Port Direct addresses must be entered within square brackets. To set-up the hotkey values used to switch to a given CPU port, the following information is used to create the hot key sequence:

- + means press down the key that follows
- means release the key that follows
- +-- means press down and release the key that follows

To switch to CPU port #1, the Hotkey / KVM port sequence would be ++Ctrl+1+-Enter, to switch to CPU port #8, the sequence would be ++Ctrl+-8+-Enter. A list of the valid hotkey codes are given in Appendix I.

Logging and Status

This screen provides various details about the user activity on the Vista Remote 2.

Note: The log has a maximum capacity of 1000 event lines. After 1000 entries, the oldest entries are overwritten. If log data are important to your installation, ensure a regular backup procedure or use the Syslog Server IP Address option to send log information automatically to another system.

Logged on users: admin

```
Dec 31 18:02:12 arkapp: disconnected: 192.168.0.136::1338 (Visit http
://192.168.0.50 to perform the firmware upgrade)
Jan  1 00:00:03 syslogd started: BusyBox v1.4.2
Jan  1 00:00:04 init: Starting pid ?1, console /dev/ttyS0: '/bin/sh'
Dec 31 18:00:08 arkapp: power on
Dec 31 18:00:08 arkapp: Using NTP server 192.168.0.136
Dec 31 18:00:08 arkapp: Sending NTP request to 192.168.0.136
Dec 31 18:00:13 arkapp: Timed out waiting for NTP reply
Dec 31 18:08:44 arkapp: connected: 192.168.0.138::1146
Dec 31 18:08:49 arkapp: logon admin, 192.168.0.138, password
Dec 31 18:08:49 arkapp: Authenticated: 192.168.0.138::1146, as (anony
mous)
Dec 31 18:22:00 arkapp: Using NTP server 192.168.0.136
Dec 31 18:22:06 arkapp: Timed out waiting for NTP reply
Dec 31 18:28:14 arkapp: Using NTP server 192.168.0.136
Dec 31 18:28:20 arkapp: Timed out waiting for NTP reply
```

Clear Log Refresh

Syslog Server IP Address 192.168.0.136

Save Logging and Status Cancel

The first three (3) columns show the date the event occurred.

The next column is the time the event occurred.

The last column describes the type of event with the users name and the access method.

The "Clear log" tab will clear all entries in the log

The "Refresh" tab will refresh the log list

The "Syslog Server IP Address field is an optional field where you can enter an IP address to send the status log.

The "Save" tab will save the log file

The "Cancel" tab will exit the log menu and return to the main menu

Note: The log has a maximum capacity of 1000 event lines. After 1000 entries, the oldest entries are overwritten. If log data are important to your installation, ensure a regular backup procedure or use the Syslog Server IP Address option to send log information automatically to another system.

To copy and paste the log

You can copy the information listed within the log and paste it into another application. While viewing the log screen, press Ctrl and C, to copy the data into the clipboard. Start a text application (i.e. Word, WordPad, Notepad) press Ctrl and V, or right mouse click and 'Paste'.

This basically covers the configuration of the input module and allows user access to the unit. Following is the additional KVM switch module configuration. Some configurations are needed to assure proper functionality and other configurations are optional.

KVM Switch Module Configuration

Connect to the unit directly from the local KVM station and logon. A computer must be connected to CPU port #1 and powered on. Using the local keyboard, press and release the left Ctrl key, then within 2 seconds press the F12 key. The press and release of the left Ctrl key notifies the KVM Switch module that the next command issued within 2 seconds is a command for the KVM Switch, not a connected computer. The F12 key will invoke the KVM switch modules OSD main menu shown below.

The on-screen display (OSD) option is available for the all Vista Remote 2 models. You can use the OSD to configure the switch module, select a computer from a list, display what computer you are switched to and set up additional security options for the switches' configuration and for computer access.

When entering information into the menu system, use only the numeric keys above the keyboard, the numeric keys and <Enter> key on the keypad will not work.



Figure 17. KVM Switch Module OSD

Use the up / down arrow keys to select the item needed and press enter. That selection menu will display for inputs

Change the computer names

Selecting “Names” and pressing enter will display the below display.



Figure 18. Change computer names

Each computer is initially assigned a computer name, “computer x”, where “x” = 1-8. To change the computer name to one of your choosing, use the up/down arrow keys to select (highlight) the computers name to change. Once selected (highlighted), press enter to clear the present name. Enter the new computer name (up to 16 valid ASCII characters) and press <Enter>. The new name will be changed and saved immediately in non-volatile memory.

The computer name is case sensitive. Use upper/lower case letters as needed. (16 ASCII characters Maximum).
The “Reset to Initial Factory Settings” function will not change the assigned computer names from their present values.

Configure appearance

The “Configure appearance” menu allows you to change the foreground and background colors, position the computer name on the screen, change the name fadeout time, font, and set up a screen saver type.

Use the up/down arrow keys to select (highlight) the selection to change. Once selected, press the space bar to cycle through the list of available options or press enter for that selection.

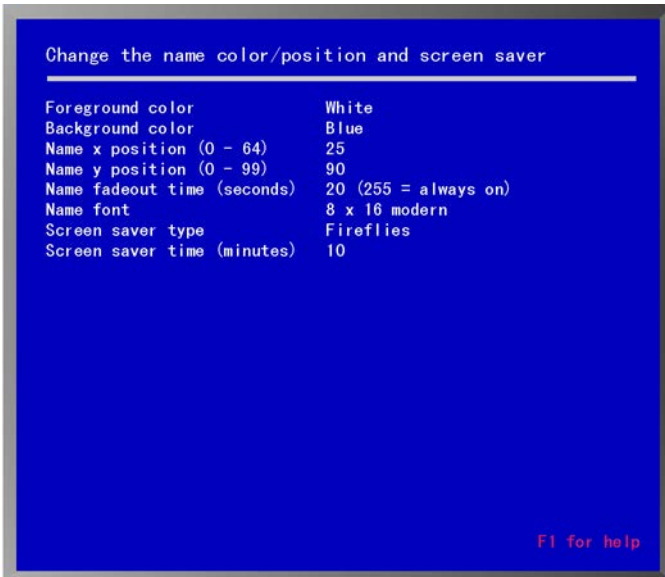


Figure 19. Change appearance

Appearance options:

Foreground/Background color:

Change the foreground and background colors of the computer label showing the selected computer. Solid colors are black, red, green, yellow, blue, magenta, cyan, and white. The transparent colors are: clear, red, green, yellow, blue, magenta, cyan, and white.

To change the foreground or background color, first select (highlight) the option and press the space bar to cycle through the list of all the available colors. Stop when the desired color displays and hit <Enter>.

Name x or y position:

This option allows you to position the computer name that is displayed on the KVM monitor when you switch to that computer. The label can be positioned anywhere on the screen and that position will be maintained even with different screen resolutions. To change the position, highlight the x or y position and press enter to clear the field. Enter the new x or y position and press <Enter>. Valid x position values are 0 – 64, valid y position values are 0 – 99.

Name fadeout time:

This option sets the time when the computer label disappears after switching to a computer. To change this value, highlight Name fadeout time and press <Enter> to clear the present value. Enter the new value

(0-255) and press <Enter>.

A value of 0 (zero) inhibits the label from displaying.

A value of 255 keeps the label displayed at all times.

Name font:

To change the name font, first select (highlight) the option and press the space bar to cycle through the list of available fonts. Stop when the desired font displays.

The choices are:

- 8X16 modern
- 8X16 classic
- 16X24 modern
- 16X24 classic
- 16X32 modern
- 16X32 class

Screen saver type:

To change the "Screen saver type", first select (highlight) the option and press the space bar to cycle through the list of all the available screen savers. Stop when the desired screen saver displays.

The choices are:

▪ Blank screen	▪ Fireflies	▪ Weaving	▪ Bounce
----------------	-------------	-----------	----------

Screen saver time:

This sets the time in seconds when the screen saver activates when no keyboard or mouse activity has occurred.

To change the "Screen saver time", highlight screen saver time and press <Enter> to clear the present value. Input the new value (0 – 999 minutes) and press <Enter>.

A value of 0 (zero) disables the screen saver function.

Configure security



Figure 20. Switch module security settings

Configuration password:

Assigning a "Configuration password" prevents unauthorized changes to the Vista Remote 2 switches' configuration. To change the password, highlight the configuration password field and press <Enter> to clear the existing password. Type in a new password (8 characters max / case sensitive) and press <Enter>. An input box will then appear requesting confirmation of the password. Re-type the password and press <Enter>. You will be prompted for a password whenever you access the configuration menu (<Ctrl> F12).

DO NOT forget your configuration or access passwords.

Access password:

Assigning an "Access password" prevents unauthorized access to the connected computers. To change the password, highlight the access password field and press <Enter> to clear the existing password. Type in a new password (8 characters maximum / case sensitive) and press <Enter>. An input box will appear for you to confirm the access password. Re-type the same password and press <Enter>. You will be prompted for an access password whenever the Vista Remote 2 switch is powered on or you have disconnected from a computer.

To remove a password, highlight the configure password or access password field and press enter to clear the password field. Press enter again with no password input and the password will be removed. The configuration password must be entered before passwords can be changed or removed.

If you forget your “Access password”, the person who knows the configure password can enter a new “Access password” for you. If you forget your “Configure password”, contact Rose Electronics Technical Support for instructions.

Access time:

Automatically log out (disconnects) of the Vista Remote 2 switch after a period of non-activity time. The access time is changeable from 1 to 999 minutes. Time starts when there is no keyboard or mouse activity. To change the access time value, highlight the access time field and press <Enter> to clear the field. Input a new value and press <Enter>. Entering an access time of 0 (zero) disables the logout function.

Configure mouse type

The “Configure mouse type” menu allows you to change the mouse type for each connected computer.

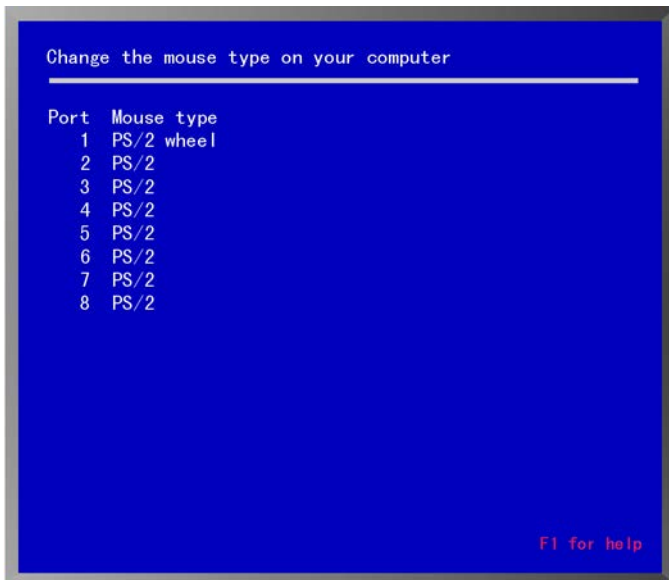


Figure 21. Configure mouse type

You should only have to change the mouse type if you un-plug the mouse or change the mouse from the auto-detected type.

To change the mouse type, first select (highlight) the port (Computer #) to change the mouse type and press the space bar to cycle through the list of all the available mouse types. Stop when the desired mouse type is displayed.

The choices are:

- PS/2 (2 or 3 button mouse)
- Serial 2 button
- PS/2 Wheel mouse (2 button + wheel)

Configure keyboard type

The “Configure keyboard type” menu allows you to change the keyboard type.

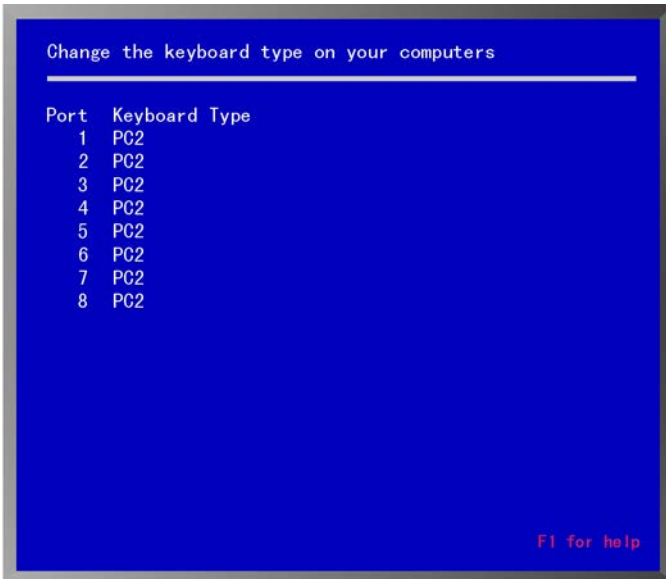


Figure 22. Configure Keyboard

You should only have to change the keyboard type if you un-plug the keyboard or change the keyboard from the auto-detected type.

To change the keyboard type, select (highlight) the port (Computer #) to change the keyboard type and press the space bar to cycle through the list of all the available keyboard types. Stop when the desired keyboard type is displayed.

The choices are:

- PC1
- PC2
- PC3

Configure miscellaneous

This menu allows you to change the maximum computer ports and scan time.

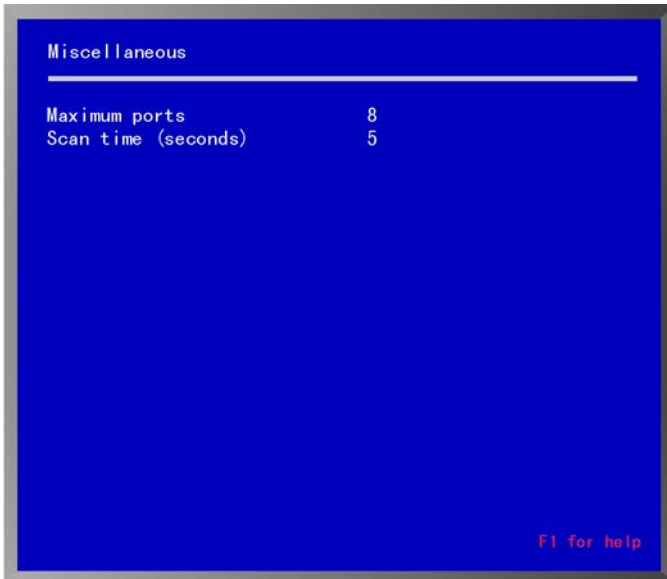


Figure 23. Configure Misc

Maximum ports:

The "Maximum ports" configuration allows you to change the total number of computer ports that are in use. If you're using an 8-port switch and only connecting 6 CPUs, changing the maximum ports from 8 to 6 will skip computer ports 7 and 8 during the scan function. To change the "Maximum Ports", highlight the maximum ports and press <Enter> to clear the field. Type in the new value (1-8) and press <Enter>.

Scan time:

This item sets the pause time during the scan function.

To change the "Scan time", highlight the scan time and press <Enter> to clear the field. Type in the new value (1-16 seconds) and press <Enter>.

Save

The “Save” function, saves all configuration changes that have been made to flash memory.



Figure 24. Save Switch settings

To save the configuration changes that have been made, select (highlight) save from the main menu and press <Enter>. When you press <Enter>, a message box will display. Press <Enter> again to save your changes or press the escape key to return to the main menu.

Exit

Select Exit and press enter to return to normal operation.

Remote System Operation

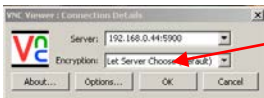
Connecting using a web browser

Connecting to the Vista Remote 2 from a network location or over the internet can be done two ways; using the Built-in Java VNC Viewer or Downloading Windows VNC Viewer from the unit and installing it on the remote computer. It is recommended that the Windows VNC viewer be downloaded from the unit and installed on the remote computer. The VNC viewer is more robust than the Java applet and has more functionality and features than the Java applet. If you experience problems using the Java applet, switch to the VNC viewer application. To connect to the Vista Remote 2 from any workstation, start a web browser and enter the assigned IP address for the unit in the URL field of the browser (Example <http://192.168.0.44>). The Vista Remote 2 will respond with the below three options displayed in the browser's window.



The first time a connection to the Vista Remote 2 is made, it is recommended that you download the Windows VNC viewer from the unit, save it and run the VNC viewer to connect to the unit directly. Some operating systems may request permission to run or save the program. Save the program to the location wanted and create a desktop ICON for the program. The next time the RealVNC viewer is needed, just click on the desktop ICON to connect.

After the installation is complete, run the VNC viewer program and the VNC Viewer Connection Details window will display. Make sure that the Server IP address is correct and the port number is 5900. If the port number was changed during the unit configuration procedure, this number will match that VNC port configuration number.



Click on "OK" to enter your Username and Password



Click on the OK tab and VNC Authentication box will display. Enter the Username and password and click OK. Upon validation, the remote connected computer's video will display. NOTE: If the username or password is entered incorrectly five consecutive times, the remote user station's IP address is locked out and remote access is denied. The lockout of an IP address will show up in the log as IP address "Blacklisted". (See the troubleshooting section for the procedure to unlock the IP address)

Click on the OK tab and the remote connected computer's video will display.



Viewer encryption settings

The web browser viewers and VNC viewers offer four encryption settings:

- Always on - This setting will ensure that the link is encrypted, regardless of Vista Remote 2 encryption setting.
- Let server choose - This setting will follow the configuration of the Vista Remote 2. If the Vista Remote 2 has 'Always on' or 'Prefer on' set, then the link will be encrypted. If the 'Prefer off' setting is selected at the Vista Remote 2, then the link will not be encrypted.
- Prefer off - This setting will configure an un-encrypted link if the Vista Remote 2 will allow it, otherwise it will be encrypted.
- Prefer on - If the Vista Remote 2 allows it, this setting will configure an encrypted link, otherwise it will be un-encrypted.

VNC Viewer Toolbar

Figure 25 **Error! Reference source not found.** shows the VNC Viewer toolbar and an explanation of each toolbar tab. The VNC viewer uses a two mouse cursor technique to identify if you are working on the VNC Viewer or the remote PC's desktop. The local cursor is the dot and the arrow cursor is the host computers desktop. When you move the cursor, the arrow cursor will follow the dot cursor. When you move the cursors off of the host computer's desktop onto the remote computer's desktop, a single arrow cursor will be present for local cursor activity.

The first time you connect to the Vista Remote 2 or switch CPU ports the cursors may be out of sync. Click on the Calibration tab on the toolbar  and calibrate the Video + Mouse. After the calibration is complete, the mouse cursors  will follow each other over the viewer window.

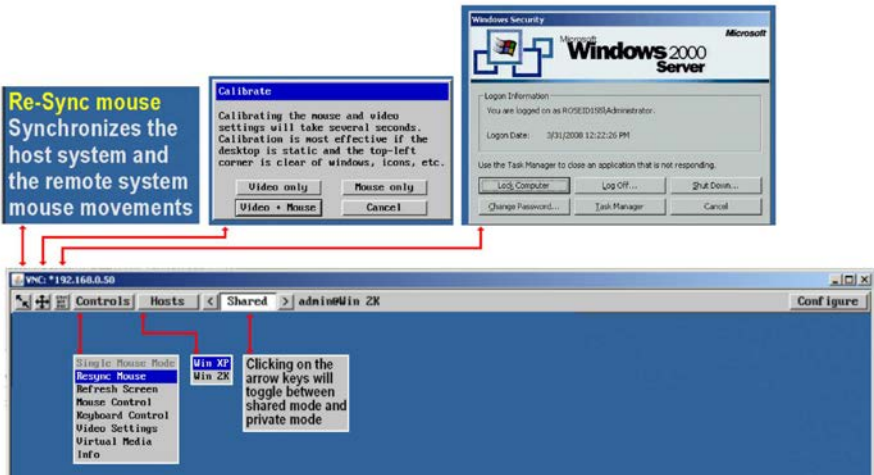


Figure 25. VNC Viewer Toolbar

Controls Tab

When you click on the “Controls” tab, the below dropdown menu will display.



Single Mouse Mode

This mode is for fast network connections where the cursor response is sufficient to provide instant visual feedback on the remote screen. When enabled, the cursor is ‘captured’ within the viewer window until you use the ‘escape’ hot keys. To escape from the single mouse mode, press F8 and then P. The single mouse mode does not require calibration and available only when using the VNC viewer.

Resync Mouse

This option has the same effect as the button on the menu bar and resynchronizes the local and remote mouse pointers.

Refresh Screen

This option refreshes the whole screen image to remove any artefacts from moved screen items. This is useful when using very low refresh rates on slow speed communication links.

Mouse Control

This option displays a mouse control dialog box and is useful when the remote cursor is failing to respond correctly to your mouse movements, even after using the Re-sync and calibration mouse option.

The mouse control dialog allows you to control the remote mouse cursor manually using a selection of buttons that you click with your local mouse. Additional options also allow you to restore the settings of a mouse that has failed to operate correctly.

Keyboard Control

This option displays a keyboard control dialog and is useful for sending keyboard combinations (to the host) that are needed regularly.

When entering codes:

- + means press down the key that follows
- means release the key that follows
- +– means press down and release the key that follows
- * means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds - *300 = 300 ms wait)

It is automatically assumed that all keys specified will be released at the end, so there is no need to specify -Ctrl or -Alt if these keys are to be released together.

See Appendix J for a list of key sequence codes that can be used.

Examples:

‘Ctrl + F12’ to invoke the KVM switch module’s OSD would be expressed as: +-Ctrl+-F12

‘Ctrl + Esc’ to invoke the KVM switch module’s CPU port selection window would be expressed as: +-Ctrl+-Esc

Video Settings

This dialog provides access to all of the key video settings that determine image quality and link performance.

Using automatic configurations

- Every setting can be individually subjected to an automatic configuration (click the appropriate 'Auto' button) and most can also be manually adjusted.
- Use the Calibrate All button to automatically determine the optimum settings for all items.

Note: Before using the 'Calibrate All' option, if possible, remove on-screen display (OSD) elements generated by any connected KVM switches (such as a host name label or menu). These OSD elements use different video rates to those of the host system(s) and can affect the setting of the automatic threshold value. Vista remote-2 uses an improved calculation procedure to filter out the effect of these elements. However, best results are obtained when the screen contains only host system information.

Note: To maximize performance, the threshold level is automatically increased by 50% when a slow link is detected.

Note: If the Vista Remote-2 is used with one or more KVM switches, the threshold needs to be higher than 32 due to the significant amounts of 'noise' that these switches introduce. The Vista Remote-2 configuration should detect such noise and adjust the threshold accordingly.

Setting the Threshold manually

Occasionally it can be useful to manually adjust the Threshold setting, in order to achieve a setting that best suits your particular requirements.

- 1 Use the 'Calibrate All' function to ensure that all other settings are optimized.
- 2 Click the Threshold left arrow button to decrement the setting by one and observe the 'Display Activity' indicator.
- 3 Repeat step 2 until the Display Activity indicator suddenly rises to a much higher level (i.e. 50%). This will mean that you have reached the noise boundary. At this point, increment the Threshold value by 2 or 3 points to achieve an optimum setting.

Virtual Media

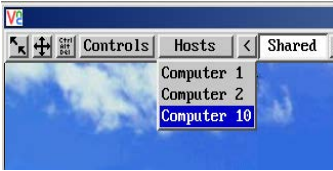
The Remote Virtual Media feature is not implemented on this model

Info

When selected, this option displays an information dialog showing the current logged on users, the current host, its video mode and its mouse motion details.

Host Tab

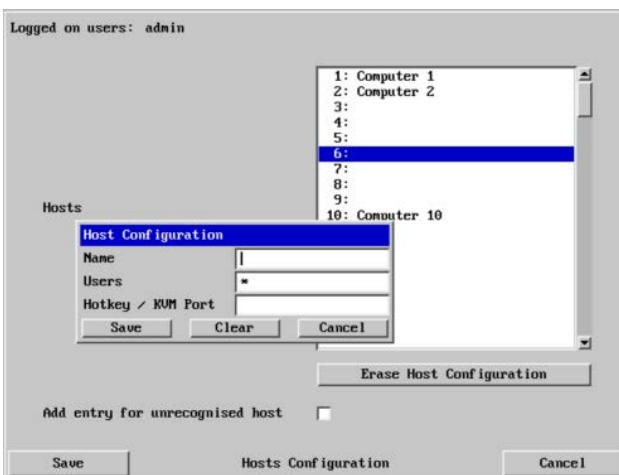
The “Host” tab on the toolbar allows you to easily switch to any CPU port on the unit or system. Each of the Host locations can be set-up with the appropriate keyboard command to switch to that port. These keyboard commands are set-up from the “Configure, Host” tab. Using the Hosts tab method to switch between host computers assures that the screen calibration details for each host are reused. The alternative is to use KVM switch hotkey combinations (Ctrl + n enter) or the KVM switch on screen display (Ctrl + Esc). You must be logged on as administrator to configure the host parameters.



To configure the Hosts feature, click on the “Configure” tab in the upper right corner of the viewer window. This will display the configuration options. Select “Host” from the option tabs and the Host configuration window will display as shown below.

1. Select (highlight) the Host slot to configure and the Host Configuration box will display.
2. Enter the name for this position (Example: Computer 6). Enter the user names that will be given access to this host location. An * allows all users access or a list of users separated by commas (e.g. admin,nigel,andy,steve).
3. Enter the Hotkey / KVM port keyboard command sequence to switch to the CPU port (+ctrl+6+enter) for locations 10 or greater like port 15, the command sequence would be +ctrl+1+5+enter).

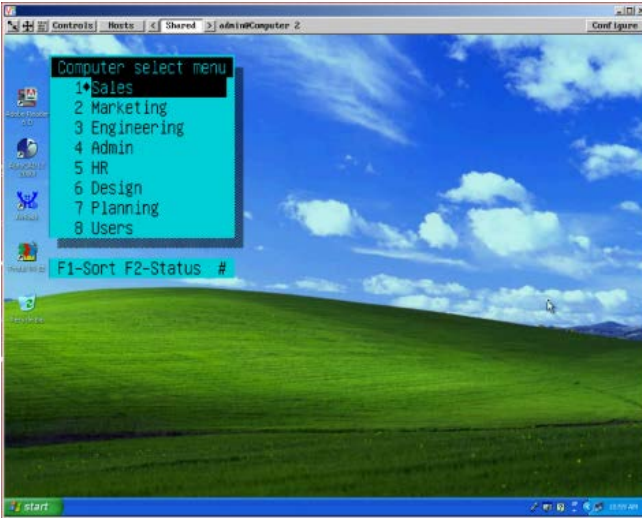
When all needed host switching commands have been entered. Save the Host Configuration and also save the Host menu information. Once saved, you will return to the configuration menu. From the Configuration menu, return to the Host and click on the Hosts button on the viewer toolbar. The defined hosts will display in the dropdown menu. Click on any Host name and you will be immediately switched to that CPU port. The Host configuration feature can also be used to send any keyboard command sequence to the KVM switch module. It is recommended that only commands to switch to a CPU port are used. You can set-up a host location to display the KVM switch module’s OSD menu (+Ctrl+F12+Enter) but it is best to use the “Command, Keyboard” function for these types of commands.



Using the VNC Viewer and not the Java applet, you can also directly access the KVM switch module using keyboard commands or the Hosts feature. Using the Java applet, each keyboard

commands to instruct the KVM Switch module to exercise an option must be configured to either the “Command, Keyboard Control” tab or the Hosts tab.

The easiest way to switch to a CPU port is invoke the Computer select window. To do this connect using the VNC viewer, press and release the Ctrl key, then within 2 seconds, press the Esc key. The computer select window will display as shown below, listing the computers connected to the Vista Remote 2.



Using the up or down arrow keys, select the computer port to switch to and press enter. You will be immediately switched to that CPU port and the connected computer's video will display. You will have complete control (if your security profile permits it) of that computer. All functions can be performed as if you were directly connected to that computer. Files can be opened, edited, and saved, and applications installed on that computer can be executed.

Keyboard Commands

Keyboard commands can be used to further customize the KVM switch module. These commands can be invoked directly from a local or remote keyboard or from the “Command, Keyboard commands” tab on the VNC view toolbar. (To use the keyboard commands, you must be connected via the VNC viewer, not the java applet)

The commands listed in the “Key sequence / Hotkey Command” column are:

TOP - direct keyboard command /

BOTTOM - key sequence string to add to the “Command, Keyboard Command OSD menu”

Command	Key Sequence / HotKey Command*	Description
Invoke the On Screen Display	<Ctrl> F12 +ctrl+f12	Displays the KVM switch module’s on-screen display
List computers	<Ctrl> Esc +ctrl+esc	Provides a list of connected computers to connect to
Reset command	<Ctrl> R +ctrl+r	Resets and enables mouse and keyboard, enables PS/2 mouse on currently selected port.
Reset mouse command	<Ctrl> O +ctrl+o	Sends reset mouse command to currently selected CPU. Will recover stuck NT mouse.
Send null byte	<Ctrl> N +ctrl+n	Used to re-synchronize PS/2 mouse.
Identify ROM version	<Ctrl> I +ctrl+i	Identifies ROM version, CPU must be at a command prompt, word processor, or text editor to receive value.
Keep	<Ctrl> K +ctrl+k	Saves current scan state and custom settings.
Scan time interval	<Ctrl> Txx <Enter> +ctrl+txx (xx = 1 – 16 sec.)	Sets the pause time for each port when scanning.
Mode command	<Ctrl> M x <Enter> +ctrl+mx Where: x = 1,2,3,7,8,9 for modes 1-9	First select the CPU port to configure, and then enter the mode command. Mode 1, 2, 3 for keyboard. Mode 7, 8, 9 for mouse
Maximum computers	<Ctrl> P x <Enter> +ctrl+px (x = 1 – 4 or 1 – 8)	Limits scanning to maximum port number
Typematic value	Factory setting = 43 Rate = 10.9 chars/sec Delay = 500 millisecond.	See Attachment H.
Mouse type	<Ctrl> Q x <Enter> +ctrl+qx Where: x = 0 for PS/2 mouse x = 1 for Serial mouse x = 2 for Wheel mouse	First select the CPU port, and then enter the type command

* See the “Controls” tab section for entering the hotkey commands

Keyboard commands (continued)

Command	Key	Description
Computer Select	<Ctrl> x +ctrl+x (x = 1, 2, 3, 4, 5, 6, 7, 8)	Connects your keyboard, video monitor, and mouse to the selected computer.
Connect to next computer	<Ctrl> + (Plus) +ctrl++	Selects the next sequential computer.
Connect to previous computer	<Ctrl> - (Minus) +ctrl+-	Selects the previous sequential computer.
Computer disconnect.	<Ctrl> L +ctrl+l	Disconnects from computer.
Scan (On)	<Ctrl> S +ctrl+s	Turns scan mode on, causing the Vista Remote 2 to start scanning sequentially from the current port through the remaining ports and start again at Port 1.
Scan (Off)	<Ctrl> X +ctrl+x	Turns scan mode off.
Reset mouse command	<Ctrl> O +ctrl+o	Sends reset mouse command to the currently selected computer. Will recover stuck NT mouse

Table 1. Keyboard Commands

Follow each set-up command with the “Keep” command to save the changes. “Keep” command = press and release the left <Ctrl> key, then the “K” key.

Keyboard command description

Computer select

To select a computer from your keyboard, press and release the left <Ctrl> key and then type in the computer number (1-4 or 1-8).

Next computer

To switch to the “Next computer”, press and release the left <Ctrl> key, then press the plus/equal key.

Previous computer

To switch to the “Previous computer”, press and release the left <Ctrl> key then press the minus/underscore key.

Scan mode (On)

To enable the “Scan mode”, press and release the left <Ctrl> key, then type S. The Vista Remote 2 switch will begin scanning sequentially from its current computer through the remaining computers (as set by the maximum computers command), and then begin again at computer 1.

Scan mode (Off)

To stop the “Scan mode”, press and release the left <Ctrl> key and then type “X”. Issuing a computer select command also turns off scanning.

Scan time interval

The “Scan Time interval” command sets the time, in seconds that the Vista Remote 2 switch will pause at each of the computers when scanning. The default setting is 5 seconds. To

change the Scan Time to another interval press and release the left <Ctrl> key, type "T" then enter the new scan time interval (1-16 seconds), and press <Enter>.

Reset

To "Reset" the mouse and keyboard, press and release the left <Ctrl> key, then type "R". This command is used to reset the mouse and keyboard on the currently selected Vista Remote 2 port without removing power from the Vista Remote 2 switch. This is most useful to reset a PS/2 mouse that has been unplugged and plugged back in. Upon issuing this command, all keyboard LEDs will go on and then return to their previous state.

Reset computer mouse type (NT and WIN 2K systems only)

DO NOT issue this command on non-NT or Win 2K based computers.

Press and release the left <Ctrl> key, then type "O". This command sends a reset mouse command to the currently selected NT or Win 2K computer. The command is used to recover a stuck mouse on an NT or Win 2K system.

Send null byte

Press and release the left <Ctrl> key, then type "N". This command is used to re-synchronize an out-of-sync PS/2 mouse. The command may need to be entered once or twice, depending if the mouse is out-of-sync by one or two bytes.

Identify ROM version

Press and release the left <Ctrl> key, then type "I". This command is used to identify the revision level of the Vista Remote 2 firmware currently installed. Before entering this command, the selected CPU must be at a command prompt, word processor, or text editor, so when the Vista Remote 2 switch sends the ROM revision level the result can be displayed.

Keep command

Press and release the left <Ctrl> key, then type "K". The Keep command saves all settings.

Mode command

The Vista Remote 2 switch supports keyboard modes 1, 2 and 3 and mouse modes 7,8, and 9. To issue the "Mode" command, press and release the left <Ctrl> key, type "M", then enter the mode number (1,2,3,7,8,9) followed by <Enter>.

Mode 1 - CPU Keyboard = PC Mode 1 (Some IBM's & PS/1's)

Mode 2 - CPU Keyboard = PC Mode 2 (Most PCs)

Mode 3 - CPU Keyboard = Most (RISC) Unix Workstations & Rose Translator

Mode 7 - CPU Mouse = 2 Button Serial (Microsoft) (7 Bt)

Mode 8 - CPU Mouse = 2 Button Serial (Not Used) (8 Bt)

Mode 9 - CPU Mouse = 3 Button Serial (Mouse Systems)

Maximum computers

Press and release the left <Ctrl> key, type "P", enter the total number of computers, and press <Enter>. This command limits the number of computers to scan. For example on an eight-port unit, if no computers were connected to ports 7 and 8, setting maximum computers to 6 would bypass scanning computers 7 and 8.

Typematic command

Initial factory setting = 43. Rate = 10.9 chars/sec, Delay = 500 millisec. See Attachment H for typematic value calculations.

Mouse type

To issue the "Mouse type" command press and release the left <Ctrl> key, type "Q", enter mouse type (0,1,2), and press <Enter>.

Mouse type 0 = PS/2 mouse

Mouse type 1 = Serial mouse

Mouse type 2 = Wheel mouse

Troubleshooting

Remote network users are unable to contact the unit

- Check that the correct address is being used by the remote users.
- Check the network settings. Check that the user's network address has not been excluded in the IP access control section.
- If Vista Remote-2 is situated behind a firewall, check that the relevant ports are being allowed through the firewall and are being correctly routed.
- Check the front panel indicators, the LNK indicator should be on. If the network link is a 100Mbps connection, the 100 indicator should also be on.
- If connecting using the VNC Java applet, close the applet and connect using the VNC Viewer program. First time connections must connect using the VNC Viewer, not the Java applet.

Remote IP address is locked out (Blacklisted)

- If the remote user logged on incorrectly five times using the VNC Viewer, try logging on using the Applet. If logging on using the Applet is successful, the IP address will be unlocked.
- If the remote user logged on incorrectly five times using the Applet, try logging on using the VNC Viewer. If logging on using the VNC Viewer is successful, the IP address will be unlocked.
- If both the VNC viewer and Applet login is denied access, remove power from the Vista Remote-2 for two to three seconds. This will reset the unit and unlock the IP address. If the Vista Remote-2 unit is using DHCP, the previously assigned IP address may be changed to a different IP address when power is restored. Remote users will need to be informed of the new IP address. If you still have problems with a Blacklisted IP address, please contact Rose Electronics technical support.

The remote cursor is not correctly responding to my mouse movements

- Recalibrate the mouse. When doing so, ensure that the host system does not have mouse cursor trails enabled and that the top left corner of the screen is clear of application windows.

When logging on using VNC viewer, I cannot enter a username

- Either, the VNC viewer is an old version or only the admin user has been configured on the unit.

When connecting to the Vista Remote-2 unit, the video is out of sync.

- Make sure a computer is connected to CPU port #1 and operating. With no CPU on port #1, the viewer video may not sync properly

Computer does not boot, keyboard or mouse error received.

- Cable is loose, reseal cable and on PC hit F1 to continue or reboot computer.
- Wrong cable or keyboard and mouse cables reversed.
- Cable is defective; try using cable from another computer.
- Port on the Vista Remote-2 is defective; try using another port on Vista Remote-2. If the problem goes away port is defective.
- Port on computer is defective, try plugging in keyboard or mouse directly if problem remains computer port is defective. If power status LED not lit, fuse on motherboard may be blown.
- Computer keyboard and mouse not configured.

Mouse driver does not load.

- If PS/2 type mouse, computer must be connected to Vista Remote-2 at boot-up time in order for mouse to be recognized by the computer. Reboot computer with Vista Remote-2 powered on and cable attached.
- If RS232 type mouse, make sure right COM port is being used and syntax of mouse driver is correct to search for the correct port.
- Computer keyboard and mouse not configured.

Can't switch computers from keyboard

- Power to the Vista Remote-2 was removed for less than three seconds possibly causing keyboard to lock up. Disconnect and re-connect the keyboard.
- If PS/2 type keyboard and mouse cables may be reversed.
- Not using left control key. Using numeric keypad instead of keys on top row. Not releasing control key before typing in number. Waiting more than 2 seconds to enter computer number. Using caps lock or shift key.
- Remotely connected using the Java applet. Close the applet and connect using the VNC viewer application.

Wrong or missing characters from those typed

- For PCs, the mode of the keyboard does not match that of the computer. Issue the mode command, usually 1 for IBM PS/2s, 3 for Unix computers, and 2 for all others. The default setting is mode 2. Sometimes an incorrect mode will confuse the computer or keyboard and require re-booting the computer or resetting the keyboard by unplugging and plugging it back in.

Mouse does not move

- Mouse not configured.
- Vista Remote-2 turned off after or not connected when computer booted or application using mouse run. Exit and re-enter application using mouse or issue reset command.
- PS/2 mouse was not connected when Vista Remote-2 powered up or disconnected and reconnected. Issue the reset command or reconfigure the mouse.

PS/2 mouse gets out of sync

- Cabling was disturbed during mouse movement. Issue the null command once or twice to re-sync the mouse. Update mouse driver. Try using ctrl O command to recover if O/S is NT.
- Sun keyboard needs to be reset, with unit power on, disconnect and re-connect the sun keyboard.

Video fuzzy

- Cable too long or wrong type. Verify that resolution and distance match. See Appendix G. Upgrade cable if necessary.

Video not synchronized or wrong color

- Cable is loose, reseal cable.
- Monitor not capable of syncing to video selected, upgrade monitor.
- Cable is defective; try using cable from another computer if problem goes away cable is defective.
- Port on Vista Remote-2 is defective; try using another port on Vista Remote-2. If problem goes away port is defective.

Lower resolution OK, but can't enter high resolution mode

- Video driver has not been setup for this resolution. Configure the driver.

On-screen display not synchronized

- No video from computer or resolution setting not configured correctly.

Maintenance and Repair

This Unit does not contain any internal user-serviceable parts. In the event a Unit needs repair or maintenance, you must first obtain a Return Authorization (RA) number from Rose Electronics or an authorized repair center. This Return Authorization number must appear on the outside of the shipping container. See Limited Warranty for more information.

When returning a Unit, it should be double-packed in the original container or equivalent, insured and shipped to:

Rose Electronics
Attn: RA _____
10707 Stancliff Road
Houston, Texas 77099 USA

Technical Support

If you are experiencing problems, or need assistance in setting up, configuring or operating your switch, consult the appropriate sections of this manual. If, however, you require additional information or assistance, please contact the Rose Electronics Technical Support Department at:

Phone: (281) 933-7673
E-Mail: TechSupport@rose.com
Web: www.rose.com

Technical Support hours are from: 8:00 am to 6:00 pm CST (USA), Monday through Friday.

Please report any malfunctions in the operation of this Unit or any discrepancies in this manual to the Rose Electronics Technical Support Department.

Safety

This Unit has been tested for conformance to safety regulations and requirements, and has been certified for international use. Like all electronic equipment, the Unit should be used with care. To protect yourself from possible injury and to minimize the risk of damage to this Unit, read and follow these safety instructions.



Caution!

Risk of explosion can occur if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

- Follow all instructions and warnings marked on this Unit.
- Except where explained in this manual, do not attempt to service this Unit yourself.
- Do not use this Unit near water.
- Assure that the placement of this Unit is on a stable surface or rack mounted.
- Provide proper ventilation and air circulation.
- Keep power cord and connection cables clear of obstructions that might cause damage to them.
- Use only power cords, power transformer and connection cables designed for this Unit.
- Use only a grounded (three-wire) electrical outlet.
- Keep objects that might damage this Unit and liquids that may spill, clear from this Unit. Liquids and foreign objects might come in contact with voltage points that could create a risk of fire or electrical shock.
- Operate this Unit only when the cover is in place.
- Do not use liquid or aerosol cleaners to clean this Unit. Always unplug this Unit from its electrical outlet before cleaning.
- Unplug this Unit from the electrical outlet and refer servicing to a qualified service center if any of the following conditions occur:
 - The power cord or connection cables is damaged or frayed.
 - The Unit has been exposed to any liquids.
 - The Unit does not operate normally when all operating instructions have been followed.
 - The Unit has been dropped or the case has been damaged.
 - The Unit exhibits a distinct change in performance, indicating a need for service.

Safety and EMC Regulatory Statements

Safety Information



Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

WARNING A WARNING in the manual denotes a hazard that can cause injury or death.
CAUTION A CAUTION in the manual denotes a hazard that can damage equipment.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding

These are Safety Class I products and have protective earthing terminals. There must be an un-interruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

Servicing

There are no user-serviceable parts inside these products. Only service-trained personnel must perform any servicing, maintenance, or repair.

The user may adjust only items mentioned in this manual

Appendix A – General specifications

Dimensions	Width	Depth	Height
4 / 8 port	16.7" / 42.4cm	15.2" / 38.6cm	1.75" / 4.5cm
Weight	4-port units	8-port units	
	6.9 lbs / 3.1 kg	9.3 lbs / 4.2 kg	
Connectors	Power CPU ports KVM port RS232 Network	IEC320 DB25F DB25F RJ45F RJ11F	
Video Bandwidth	150 MHz		
Resolution	1280 x 1024		
Ethernet Link	10/100 Mbs Ethernet speed		
Controls	All controls are performed using an on-screen menu system		
Indicators	LED's: Power,		
Chassis	Electro-galvanized steel, black powder coated		
Environmental	0° - 45° C, 32° - 113° F		
Humidity	5% - 80% non-condensing		

Appendix B – Part Numbers

KVR-1R4UA/OV/2	4-port / local-remote access
KVR-1R8UA/OV/2	8-port / local-remote access
CAB-CX0606Cnnn	DB25 to HD15/PS2/PS2 (Unit to Computers)
CAB-ZX0606Mnnn	DB25 to HD15/PS2/PS2 (Unit to KVM Station)
RM-UBnn	Rack mount kit for 4 / 8 port units

Appendix C – RackMount

The rack mount kit includes the following items:

- Two black anodized mounting brackets
- Four 6 - 32 x 3/8" flat head mounting screws

To rack mount Vista Remote 2 unit, attach the two rack mounting brackets to your Unit with the short flange against the Unit using the four screws provided. Secure the mounting brackets to the rack using the appropriate size bolts, nuts and lock washers. Using hardware other than that provided could cause damage to the electronics and/or result in loss of mounting integrity. Do not over tighten the screws used to mount the Unit to the mounting brackets.

The following general guidelines should be observed when installing your Unit into a rack.

- a). The Vista Remote 2 is designed to work in an ambient temperature of 0° C to 45° C (32° F – 113° F).
- b). Do not block power supply vents or otherwise restrict airflow when rack-mounting this Unit.
- c). Mechanical loading of the rack should be considered to prevent instability and possible tipping over.
- d). Tighten all connectors securely and provide adequate strain relief for all cables.
- e). Provide a grounded power source to all Units. Pay special attention to overall branch circuit load ratings before connecting equipment to this source. Overloaded circuits are potential fire hazards and can cause equipment failures or poor performance.

Rack mount illustration



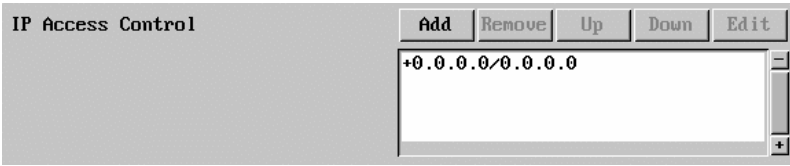
Appendix D – IP Access Control

Setting IP access control

The golden rule with this feature is 'Include before you exclude' or to put it another way 'Arrange *allowed* addresses in the list *before* the *denied* addresses'.

This is because the positions of entries in the list are vitally important. Once a range of addresses is denied access, it is not possible to make exceptions for particular addresses within that range. For instance, if the range of addresses from A to F are denied access first, then the address C could not be granted access lower down the list. Address C needs to be placed in the list before the denied range.

IMPORTANT: This feature should be configured with extreme caution as it is possible to deny access to everyone. If such an error occurs, see Clear IP access control for details about how to regain access.



In the list, access control addresses prefixed by '+' are allow entries while those prefixed by '-' are deny entries.

To define a new IP access control entry, click the Add button to display a popup dialog:



Network/Address

Enter the network address that is allowed or denied access. If a range of addresses is being specified then specify any one of the addresses within the range and use the Mask entry to indicate the size of the range. (See address range and mask sections)

The IP access control function uses a standard IP address and a net mask notation to specify both single locations and ranges of addresses. In order to use this function correctly, you need to calculate the mask so that it accurately encompasses the required addresses.

Single locations

Some of the simplest addresses to allow or deny are single locations. In this case you enter the required IP address into the 'Network/Address' field and simply enter the 'Mask' as 255.255.255.255 (255 used throughout the mask means that every bit of the address will be compared and so there can only be one unique address to match the one stated in the 'Network/Address' field).

All locations

The other easy setting to make is ALL addresses are allowed or denied. Using the mask 0.0.0.0 as standard, the IP access control section includes the entry: +0.0.0.0/0.0.0.0. The purpose of this entry is to include all IP addresses. It is possible to similarly *exclude* all addresses, however, take great care not to do this as you instantly render all network access void. There is a recovery procedure should this occur.

Address ranges

Although you can define ranges of addresses, due to the way the mask operates, there are certain restrictions on the particular ranges that can be set. For any given address you can encompass neighboring addresses in blocks of either 2, 4, 8, 16, 32, 64, 128, etc. and these must fall on particular boundaries. For instance, if you wanted to define the local address range:

192.168.142.67 to 192.168.142.93

The closest single block to cover the range would be the 32 addresses from:

192.168.142.64 to 192.168.142.95.

The mask needed to accomplish this would be: 255.255.255.224

When you look at the mask in binary, the picture becomes a little clearer. The above mask has the form: 11111111.11111111.11111111.11100000

Ignoring the initial three octets, the final six zeroes of the mask would ensure that the 32 addresses from .64 (01000000) to .95 (01011111) would all be treated in the same manner.

See Net masks - the binary explanation for details.

When defining a mask, the important rule to remember is:

There must be no 'ones' to the right of a 'zero'.

For instance, (ignoring the first three octets) you could not use a mask that had 11100110 because this would affect intermittent addresses within a range in an impractical manner. The same rule applies across the octets. For example, if you have zeroes in the third octet, then all of the fourth octet must be zeroes.

The permissible mask values (for all octets) are as follows:

Mask octet	Binary	Number of addresses encompassed
255	11111111	1 address
254	11111110	2 addresses
252	11111100	4 addresses
248	11111000	8 addresses
240	11110000	16 addresses
224	11100000	32 addresses
192	11000000	64 addresses
128	10000000	128 addresses
0	00000000	256 addresses

If the access control range that you need to define is not possible using one address and one mask, then you could break it down into two or more entries. Each of these entries could then use smaller ranges (of differing sizes) that, when combined with the other entries, cover the range that you require.

For instance, to accurately encompass the range in the earlier example:

192.168.142.67 to 192.168.142.93

You would need to define the following six address / mask combinations in the IP access control section:

Network/address entry	Mask entry	
192.168.142.67	255.255.255.255	defines 1 address (.67)
192.168.142.68	255.255.255.252	defines 4 addresses (.68 to .71)
192.168.142.72	255.255.255.248	defines 8 addresses (.72 to .79)
192.168.142.80	255.255.255.248	defines 8 addresses (.80 to .87)
192.168.142.88	255.255.255.252	defines 4 addresses (.88 to .92)
192.168.142.93	255.255.255.255	defines 1 address (.93)

Mask

Enter an IP network mask that indicates the range of addresses that will be allowed or denied access. For instance, if only a single specified IP address were required, the mask entry would be 255.255.255.255 in order to specify a single location.

Access

Use the arrow buttons to select either 'Allow' or 'Deny' as appropriate.

- 1 Enter the base network address, the mask and select the appropriate access setting.
- 2 Click the OK button.

To reorder access control entries

IMPORTANT: When reordering, ensure that any specific allowed addresses are listed higher in the list than any denied addresses. Take care not to invoke any deny access settings that would exclude valid users.

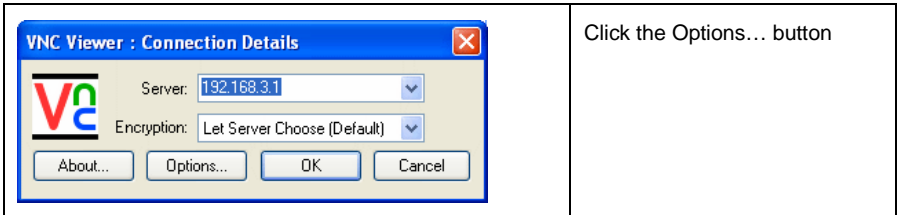
- 1 In the access control list, click on the entry to be moved.
- 2 Click the Up or Down buttons as appropriate.

To edit/remove access control entries

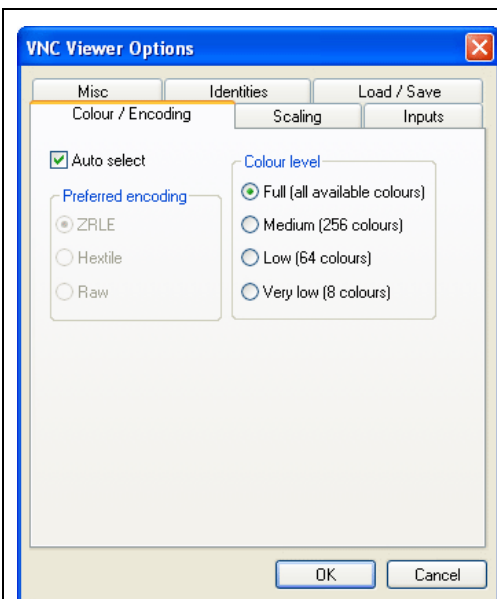
- 1 In the access control list, click on the appropriate entry.
- 2 Click either the Edit or Remove button as appropriate.

Appendix E – VNC Viewer connection options

When you are connecting to the Vista Remote 2 unit using the VNC viewer, a number of options are available.



There are six tabbed pages of options:



Color/Encoding

Auto select

When ticked, this option will examine the speed of your connection to the Vista Remote 2 unit and apply the most suitable encoding method. This option is suggested for the majority of installations.

Preferred encoding

There are three manually selectable encoding methods which are accessible when the Auto select option is un-ticked.

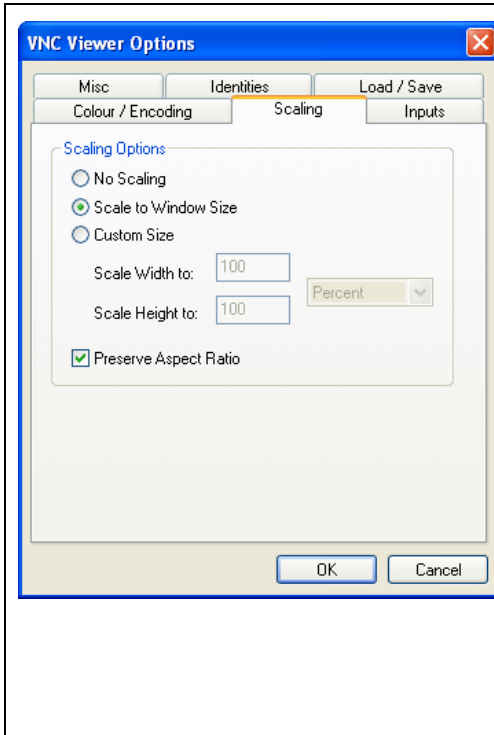
- **ZRLE** – This is a highly compressed method that is best suited to slow modem connections.
- **Hextile** – This method offers better performance than the ZRLE when used over a high speed network because there is no need for the Vista Remote 2 to spend time highly compressing the data.

- **Raw** – This is a primitive, uncompressed method that is mainly used for technical support issues. You are recommended not to use this method.

Color level

This section allows you to select the most appropriate color level for the speed of the connection to the Vista Remote 2 unit. Where the connection speed is slow or inconsistent there will be a necessary compromise between screen response and color depth.

- **Full** – This mode is suitable only for fast network connections and will pass on the maximum color depth being used by the host system.
- **Medium (256 colors)** – This mode reduces the host system output to a 256 color mode and is more suitable for ISDN and fast modem connections.
- **Low (64 colors)** – This mode is suitable for slower modem connections and reduces the host system output to 64 colors.
- **Very low (8 colors)** – This mode provides very rudimentary picture quality and hardly any speed advantage over the 64 color setting. You are recommended not to use this mode.



Scaling

No Scaling

No attempt is made to make the screen image fit the viewer window. You may need to scroll horizontally and/or vertically to view all parts of the screen image.

Scale to Window Size

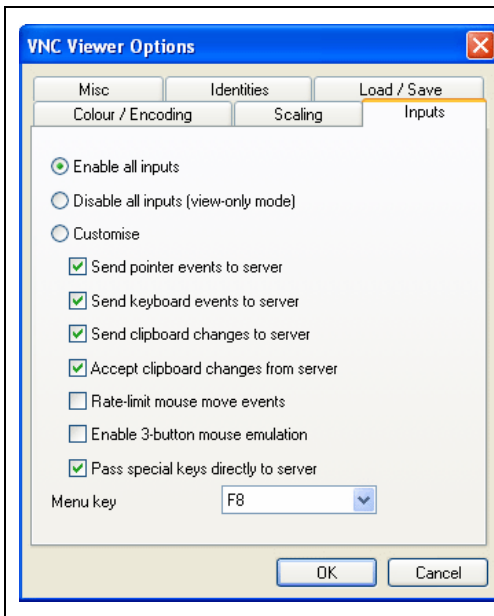
Adjusts the server screen image to suit the size of the viewer window.

Custom Size

Adjusts the server screen image according to the Width and Height settings in the adjacent fields. A drop box to the right of the fields allows you to define the image size by percentage or by pixels, as required.

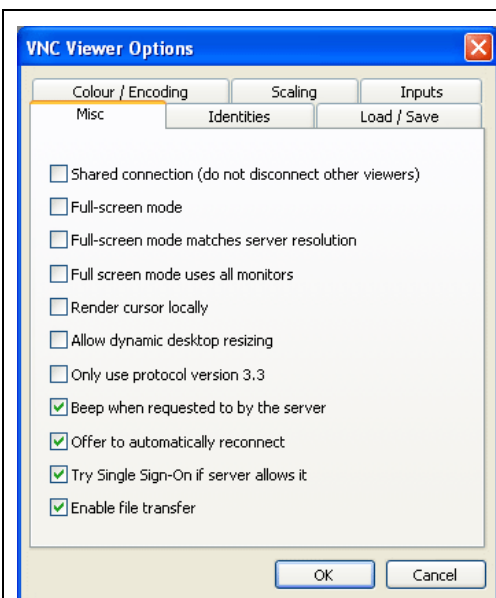
Preserve Aspect Ratio

When ticked, maintains a consistent ratio between the horizontal and vertical dimensions of the screen image.



Inputs

These feature do not apply to the Vista Remote 2 unit installations.



Misc

Shared connection (do not disconnect other viewers)

This option does not apply to Vista Remote 2 unit.

Full screen mode

When ticked, the VNC viewer will launch in full screen mode. Use the menu key (usually F8) to exit from full screen mode.

Full-screen mode matches server resolution

This option does not apply to Vista Remote 2 unit.

Full-screen mode uses all monitors

This option does not apply to Vista Remote 2 unit

Render cursor locally

This option does not currently apply to Vista Remote 2 unit.

Allow dynamic desktop resizing

When ticked, the viewer window will be automatically resized whenever the host system's screen resolution is altered.

Only use protocol version 3.3

This option does not apply to Vista Remote 2 unit.

Beep when requested to by the server

When ticked, your local system will beep in response to any error beeps emitted by the Vista Remote 2.

Offer to automatically reconnect

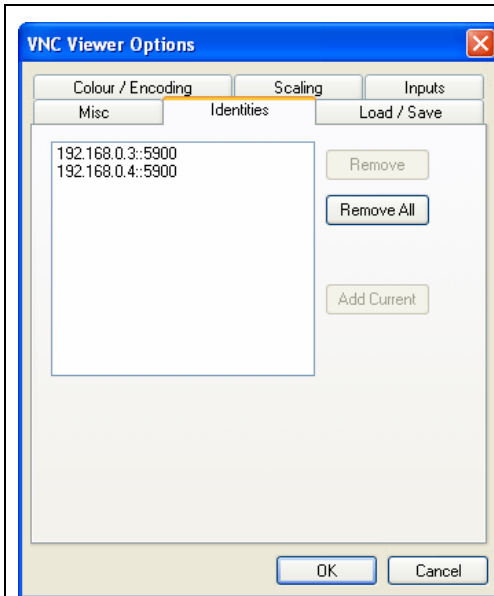
When ticked, the viewer will offer to restore a lost connection with the server.

Try Single Sign-On if server allows it

This option does not apply to Vista Remote 2 unit.

Enable file transfer

This feature does not apply to the Vista Remote 2 unit installations.

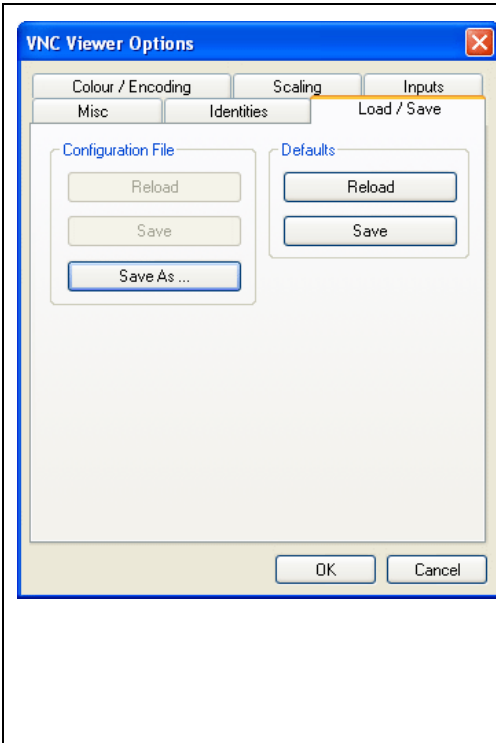


Identities

This feature helps your VNC viewer to confirm that a revisited Vista Remote 2 unit is genuine and not another device masquerading as an Vista Remote 2. The list given will retain the identities of all visited units (that have full security enabled).

When you first make a secure connection to the Vista Remote 2, the security information for that Vista Remote unit is cached within this Identities tab (i.e. the "identity" is known). The next time that you connect to the Vista Remote 2 unit, its identity is checked against the stored version. If a mismatch is found between the current and the stored identities then a warning will be issued to you.

If an existing Vista Remote 2 unit is fully reconfigured then it will need to be issued with a new identity. In this case the previous identity, listed in this tab, should be removed so that a new identity can be created on the next connection.



Load / Save

Configuration File - Reload

Allows you to load a configuration file saved from this, or another viewer.

Configuration File - Save

Allows you to save the current settings so that they can be copied from one viewer to another.

Configuration File - Save As...

Allows you to save the current settings under a new name so that they can be copied from one viewer to another.

Defaults - Reload

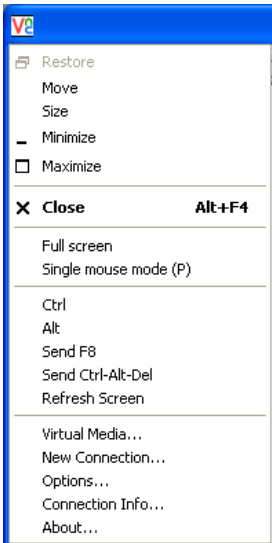
When clicked, all connection options are returned to the default settings that are currently saved.

Defaults - Save

When clicked, saves the current connection options as the default set that will be used in all subsequent VNC connections.

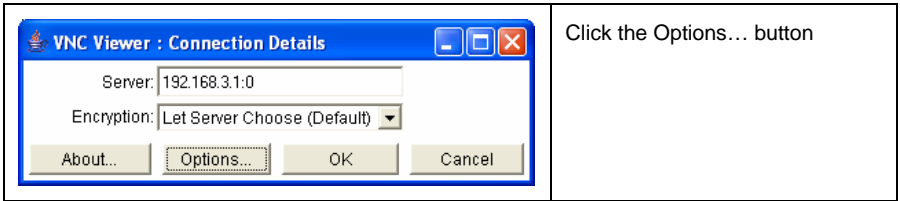
Appendix E – VNC viewer window options

Click the VNC icon in the top left corner of the viewer window (or press F8) to display the window options:

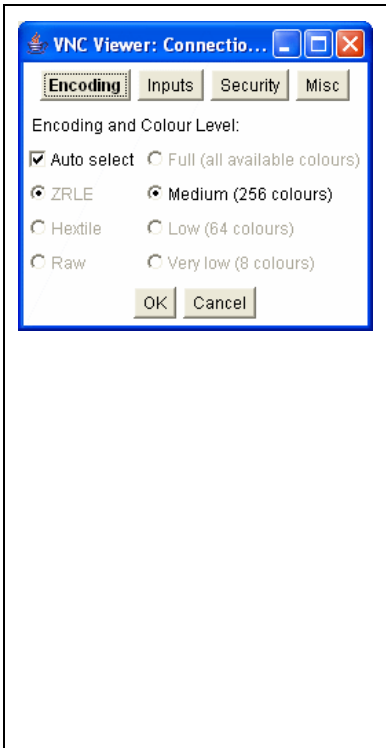
	<p>Standard window control items Restore, Move, Size, Minimize, Maximize, and Close control the VNC window as per any other application.</p> <p>Full screen Expands the VNC viewer window to fill the whole screen with no visible window edges or toolbar. Press F8 to redisplay this menu.</p> <p>Single mouse mode (P) Used for fast network connections where a second, “predictor” cursor is not required.</p> <p>Ctrl, Alt, Send F8, Send Ctrl-Alt-Del Sends the selected key press(es) to the Vista Remote 2 and the host system. This is necessary because certain keys and key combinations are trapped by the VNC viewer.</p> <p>Refresh Screen Requests data from the server for a complete redraw of the screen image, not just the items that change.</p> <p>Virtual Media... This feature is not available for the Vista Remote 2 unit</p> <p>New Connection... Displays the connection dialog so that you can log on to a different Vista Remote 2 unit or VNC server location.</p> <p>Options... Displays the full range of connection option</p> <p>Connection Info... Displays various connection and display details.</p> <p>About... Displays information about your VNC viewer.</p>
--	--

Appendix F – Browser viewer options

When you are connecting to the Vista Remote 2 unit using a Web browser and the VNC applet, a number of options are available.



There are four options pages:



Encoding and color level

Auto select

When ticked, this option will examine the speed of your connection to the Vista Remote 2 and apply the most suitable encoding method. This option is suggested for the majority of installations.

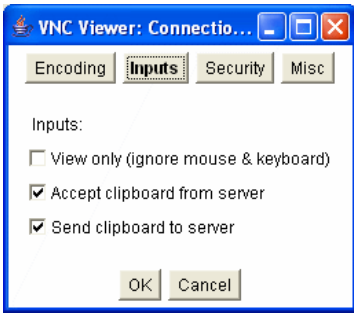
Preferred encoding

There are three manually selectable encoding methods which are accessible when the Auto select option is un-ticked.

- **ZRLE** – This is a highly compressed method that is best suited to slow modem connections.
- **Hextile** – This method offers better performance than the ZRLE when used over a high speed network because there is no need for the Vista Remote 2 unit to spend time highly compressing the data.
- **Raw** – This is a primitive, uncompressed method that is mainly used for technical support issues. You are recommended not to use this method.

Color level

The color level is fixed at Medium (256 colors) for almost all browsers.



Inputs

View only (ignore mouse & keyboard)

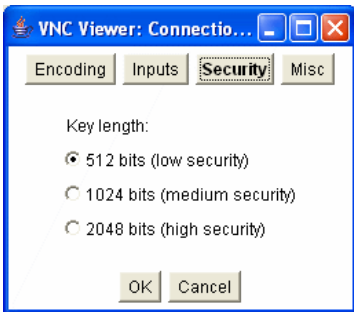
When ticked, the viewer will not send keyboard or mouse information to the Vista Remote 2 unit or host system.

Accept clipboard from server

This feature is restricted to software server versions of VNC and has no effect on Vista Remote 2 unit installations.

Send clipboard to server

This feature is restricted to software server versions of VNC and has no effect on Vista Remote 2 unit installations.



Security

512 bits (low security)

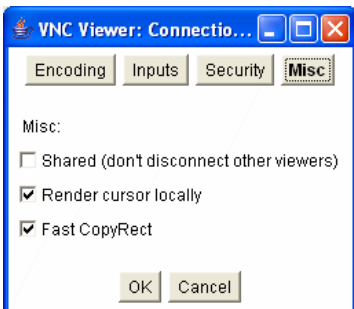
Selects the lowest level of encoding for communications between the browser and the Vista Remote 2 unit.

1024 bits (medium security)

Selects the middle level of encoding for communications between the browser and the Vista Remote 2 unit.

2048 bits (high security)

Selects the highest level of encoding for communications between the browser and the Vista Remote 2 unit.



Misc

Shared (don't disconnect other viewers)

This feature is restricted to software server versions of VNC and has no effect on Vista Remote 2 unit installations.

Render cursor locally

This feature is restricted to software server versions of VNC and has no effect on Vista Remote 2 unit installations.

Fast CopyRect

This feature is restricted to software server versions of VNC and has no effect on Vista Remote 2 unit installations.

Appendix G – Supported video modes

The following video modes are supported and can be automatically configured by the Vista Remote 2. If a recognized video mode cannot be found, the Vista Remote 2 will gradually change some of the key parameters to discover whether a video lock can be achieved. Support for VESA GTF (Generalized Timing Formula) is available and can be enabled via the Advanced Unit Configuration screen.

The half width video modes capture every other pixel. These are not generally recommended for normal use but may be used for emergency access to high resolution, high frequency system screens. Half width screens can be expanded to normal width using the scaling features of the viewer.

vesa 720 x 400 @ 85Hz	vesa 1152 x 864 @ 75Hz
vesa 640 x 480 @ 60Hz	vesa 1280 x 960 @ 60Hz
vesa 640 x 480 @ 72Hz	vesa 1280 x 1024 @ 60Hz
vesa 640 x 480 @ 75Hz	vesa 1280 x 1024 @ 75Hz
vesa 640 x 480 @ 85Hz	vesa 1600 x 1200 @ 60Hz
vesa 800 x 600 @ 56Hz	vesa 720 x 400 @ 70Hz*
vesa 800 x 600 @ 60Hz	sun 1152 x 900 @ 66Hz
vesa 800 x 600 @ 72Hz	sun 1152 x 900 @ 76Hz
vesa 800 x 600 @ 75Hz	sun 1280 x 1024 @ 67Hz
vesa 800 x 600 @ 85Hz	apple 640 x 480 @ 67Hz
vesa 1024 x 768 @ 60Hz	apple 832 x 624 @ 75Hz
vesa 1024 x 768 @ 70Hz	apple 1152 x 870 @ 75Hz
vesa 1024 x 768 @ 75Hz	
vesa 1024 x 768 @ 85Hz	

* Not actually a VESA mode but a common DOS/BIOS mode

Appendix H – Typematic Rate

Typematic Command

Press the left <Ctrl> key, type "A", enter the typematic value (1-3 digit) followed by <Enter>.

The typematic value is determined from the following tables using the equation: Typematic Value = Rate value + Delay Value. Pick the desired rate in keys/sec. and the delay in milliseconds from tables below. Add the Rate Value and the Delay Value. The sum of these values is the typematic value to enter.

For example to use a Rate of 16.0 keys/sec. and a 500 millisecond delay, the Rate value = 7 and the Delay value = 32. Add 7 + 32 = 39. To set a typematic value of 16, press the left <Ctrl> key, type "A", enter 39, and then press Enter.

Typematic Rate							
Rate Keys/sec	Rate Value	Rate keys/sec	Rate Value	Rate Keys/sec	Rate Value		
30.0	0	15.0	8	7.5	16	3.7	24
26.7	1	13.3	9	6.7	17	3.3	25
24.0	2	12.0	10	6.0	18	3.0	26
21.8	3	10.9	11	5.5	19	2.7	27
20.0	4	10.0	12	5.0	20	2.5	29
18.5	5	9.2	13	4.6	21	2.3	28
17.1	6	8.6	14	4.3	22	2.1	30
16.0	7	8.0	15	4.0	23	2.0	31

Typematic Delay							
Delay*	Delay Value	Delay*	Delay Value	Delay*	Delay Value	Delay*	Delay Value
250	0	500	32	750	64	1000	96

* Delay in milliseconds

Appendix I – Hot Key Codes

These codes are used when defining hotkey switching sequences (macros) for host computers and allow you to include almost any of the special keys on the keyboard.

Permissible key presses

Main control keys (see *'Using abbreviations'*)

Backspace | Tab | Return | Enter | Ctrl | Alt | Win | Shift | LShift | RShift
LCtrl | RCtrl | LAlt | AltGr | RAlt | LWin | RWin | Menu | Escape | Space
CapsLock | NumLock | PrintScreen | Scrolllock

Math operand keys (see *'Using abbreviations'*)

Add (Plus) | Subtract (Minus) | Multiply

Central control keys (see *'Using abbreviations'*)

Insert | Delete | Home | End | PageUp | PageDown
Up | Down | Left | Right | Print | Pause

Keypad keys (see *'Using abbreviations'*)

KP_Insert | KP_Delete | KP_Home | KP_End | KP_PageUp
KP_PageDown | KP_Up | KP_Down | KP_Left | KP_Right | KP_Enter
KP_Add | KP_Subtract | KP_Divide | KP_Multiply
KP_0 to KP_9

Function keys

F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12

ASCII characters

All characters can be entered using their ASCII codes, from 32 to 126 (i.e. A,B,C, ... 1,2,3 etc.) with the exception of the special characters '+', '-', '+-' and '*' which have special meanings, as explained below.

Codes with special meanings

- + means press down the key that follows
- means release the key that follows
- +– means press down and release the key that follows
- * means wait 250ms (note: if a number immediately follows the asterisk, then the delay will equal the number, in milliseconds)

Note: Hotkey sequences are not case sensitive.

Creating macro sequences

Hot key macro sequences can be up to 256 characters long. All keys are assumed to be released at the end of a line, however, you can also determine that a key is pressed and released within a sequence. Any of the following three examples will send a command that emulates a press and release of the Scroll Lock key:

```
+SCROLL-SCROLL  
+-SCROLL  
+SCROLL-
```

Example:

```
+SCROLL+-SCROLL+1+ENTER
```

Press and release scroll twice, press 1 then enter then release all keys (equivalent definition is +SCROLL-SCROLL+SCROLL-SCROLL+1+ENTER-1-ENTER)

Using abbreviations

To reduce the length of the key definitions, any unique abbreviation for a key can be used. For example: "scroll", "scr" and even "sc" all provide an identifiable match for "ScrollLock" whereas "en" could not be used because it might mean "Enter" or "End" ("ent" would be suitable for "Enter").

Note: Hotkey sequences and abbreviations are not case sensitive.



Server Management



Solutions