

ROSE.COM

INSTALLATION AND OPERATIONS MANUAL



LIMITED WARRANTY

Rose Electronics® warrants the UltraLink 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 A digital device, pursuant to Subpart J of 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.

DECLARATION of CONFORMITY

Declaration of Conformity

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 A digital device in accordance with the specifications Subpart J 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.

European EMC directive 89/336/EEC

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standard EN55022. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions may cause harmful interference to radio or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference with one or more of the following measures:

- (a) Reorient or relocate the receiving antenna.
- (b) Increase the separation between the equipment and the receiver.
- (c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- (d) Consult the supplier or an experienced radio/TV technician for help.

Canadian Department of Communications RFI statement

This equipment does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

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 radioélectriques publié par le ministère des Communications du Canada.

Radio Frequency Energy

A Category 5 (or better) twisted pair cable must be used to connect the UltraLink 2 unit in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances. All other interface cables used with this equipment must be shielded in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

TABLE of CONTENTS

Contents	Page #
System Introduction	3
About this manual	3
Features	4
Compatibility	4
Cables	5
Package Contents	5
Rose Electronics web site	5
Single Access Model	6
Dual Access Model	6
Method #1 - Unit configuration via USB ports (all models).....	7
Method #2 - Unit configuration via network crossover cable (all models)	8
Method #3 - Unit configuration via Local KVM station (dual access model only)	10
Configure Unit	11
Configure Network	11
Secure Keys Menu	13
Connecting Remotely	14
VNC Viewer Toolbar	15
VNC Remote Configuration menu	16
User Account	17
Unit Configuration	18
Advanced Unit Configuration	19
Time and Date	21
Network Configuration.....	22
Host Configuration	24
Permissible key presses.....	25
Logging and Status	26
LDAP Configuration	27
Single Unit Installation	28
Dual Unit Installation	28
Dual Unit Installation to a KVM Switch	29
Operating procedure	30
Troubleshooting	35
Safety	36
Maintenance and Repair	37
Technical Support	37

Figures	Page #
Figure 1. UltraLink 2 Models	6
Figure 2. Configuration via USB.....	7
Figure 3. Configure via Network crossover cable	8
Figure 4. Initial connect screen	8
Figure 5. Configure Dual model	10
Figure 6. VNC Toolbar	15
Figure 7. Remote Configuration Menu	16
Figure 8. Remote User Account Menu	17
Figure 9. Remote Unit Configuration	18
Figure 10. Remote Advanced Unit Configuration	19
Figure 11. Remote Time / Date Configuration	21
Figure 12. Remote Network Configuration	22
Figure 13. Remote Hosts Configure Menu	24
Figure 14. Logging and Status Screen	26
Figure 15. LDAP Configuration	27
Figure 16. Single unit installation	28
Figure 17. Dual unit installation	28
Figure 18. Installation to a KVM switch	29
Figure 19. VNC Viewer Toolbar	31
Figure 20. Virtual Media set-up	41

Appendices	Page #
Appendix A- Specifications.....	38
Appendix B- Part Numbers	39
Appendix C- Video Modes.....	40
Appendix D- Virtual Media Feature	41
Appendix E- VNC Viewer Options.....	43

System Introduction

Thank you for choosing UltraLink™ 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 switching solutions for today's demanding workplace. The UltraLink 2, when installed and connected to your network, allows you full access and control of the connected computer from the built in viewer client or any web browser from almost anywhere. This small, flexible, and powerful product uses Real VNC client software that is designed for very secure, encrypted, and password protected exchange of information between the server and the remote viewer.

The UltraLink 2 sets a new standard for an easy and very secure way to remotely manage server room environments, remote standalone applications such as digital signage, and many other remote applications. Connect the UltraLink 2 to a KVM switch and you now have access and control to as many computers as your KVM switching system can support.

The UltraLink 2 is different in the way it manages remote access to your systems. All of the systems that will be remotely connected remain completely unchanged and can run their usual operating system normally. They only need to be connected to the UltraLink 2 unit. Being totally operating system independent, a user can remotely connect to a Windows, Linux, UNIX, Sun, and even a DOS system with no problem. The UltraLink 2 is ideal for remote computers running stand alone applications like ATMs and remote digital signage devices.

Whatever your remote accessing needs are, the versatility of the UltraLink 2 from Rose Electronics can fulfill those needs. It can be installed at any network level, connected to a single server, a computer running any operating system, or connected to a KVM switch. PS/2 or USB, analogue or digital video, UltraLink 2 can handle it.

For the majority of applications, the UltraLink 2 requires no external power. It obtains its power from the PS/2 keyboard and mouse or USB ports on the connected PC. A power adapter is needed if you connect to a KVM switch that does not provide +5V on **both** the keyboard and mouse lines.

About this manual

This manual covers the installation, configuration, operation, and applications for the UltraLink 2 single and dual models.

Features

- Connect to a remote computer, server, or KVM switch directly or remotely over IP using any supported internet browser and the built-in Real VNC viewer.
- Remote application (Real VNC or Java applet) can be installed directly from the unit
- BIOS level control
- USB or PS/2 keyboard and mouse
- Supports resolutions up to 1600 x 1200
- Power supplied from the computer's keyboard, mouse, or USB ports.
- Virtual Media (via USB) support feature allows authorized remote users to transfer files and folders (2Gig max) to a host computer. This feature makes maintenance and upgrades possible from remote locations
- Easy installation and configuration locally using the local keyboard and mouse with the dual access model, using a crossover network cable, or directly from a computer or laptop's USB ports.
- Dual model features local access for unit configuration and direct access to the connected computer
- Solid-state embedded unit for maximum reliability
- Flash upgradeable so your unit is always up to date with new features and enhancements
- Private single user or shared access
(Shared access allows up to four simultaneous users to access the UltraLink 2 at any one time)
- Up to 16 user profiles can be set-up with event logging
- Compatible with Rose Electronics KVM switches, extenders, and most other KVM devices. The optional power adapter may be needed when connected to some KVM switches
- Front panel indicators show Link, Local or Remote connection, VNC access, Network speed, and Power
- State of the art security using AES 128 bit encryption and RSA 2048 bit public key authentication (Connection using Real VNC enhances the security by allowing the creation of ciphered user communication)
- IP lockout feature for incorrect login (IP address shown as "Blacklisted" in log file)
- Intelligent auto sensing Ethernet port. Automatically senses a 10Mb or 100Mb network connection
- Configurable to use your LDAP server for authorization and validation
- Optional Rack mount kits available for rack mounting up to 16 units in 2U of rack space

Compatibility

Hardware – Computer Keyboard Mouse Monitor	PC, RS/6000, Alpha, SGI, Sun, Mac, and others PS/2, USB PS/2, USB Analogue or Digital
Operating systems	Windows (all), Sun, Solaris, Mac, NetWare, Unix, Linux, BSD and others

Cables

UltraLink 2 to computer	(HD15M, MD6M, MD6M to HD15M, MD6M, MD6M Supplied)
UltraLink 2 to network	CAT 5 or CAT 6 cable terminated with RJ45M connectors
UltraLink 2 to Local KVM	Local access unit only - No cables required, keyboard, monitor, and mouse cables connect directly to the unit's ports. PS/2 to USB adapter is needed for using a USB keyboard and USB mouse (Included)
UltraLink 2 to Rose Electronics KVM switch	CAB-CX0606Cnmm / ZX0606Cnmm (DB25M to HD15M, MD6M, MD6M) or CAB-CXV66Mmnn (HD15M, MD6M, MD6M to HD15M, MD6M, MD6M) Note: Optional PSU maybe required

Package Contents

The package contents consist of the following:

The UltraLink 2 Unit as ordered

1-UltraLink 2 to Computer cable

2-PS/2 to USB adapters

4-Self-adhesive rubber feet

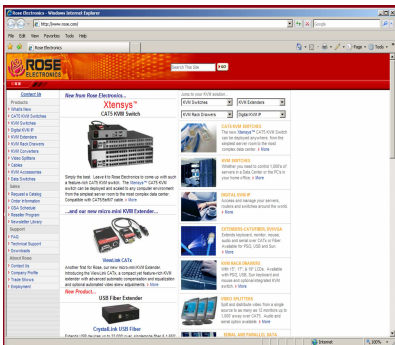
CD-Rom (Includes Product Datasheet, Manual, and Quick Start Guide)

Power Adapter (Optional)

Additional 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 the UltraLink 2 and other products designed for data center applications, classroom environments, and many other applications.



Register your product for future updates at:
www.rose.com/html/online-registrationform.htm

MODELS

Single Access Model



Front Panel

- Connectors - Network – RJ45F
- Power – Male barrel jack (Power adapter optional)
- Indicators - 6 LEDs indicating:
 - Link / Remote connection
 - VNC connection
 - Network speed
 - Local connection
 - Power
- Reset - Recessed push button

Rear Panel

- Connectors - Keyboard – PS/2 (MiniDIN6F)
- Mouse – PS/2 (MiniDIN6F)
- Monitor – HD15

Dual Access Model



Front Panel

- Connectors - Network – RJ45F
- Power – Male barrel jack (Power adapter optional)
- Indicators - 6 - LEDs indicating:
 - Link / Remote connection
 - VNC connection
 - Network speed
 - Local connection
 - Power
- Reset - Recessed push button

Panel

- Connectors
 - To KVM (TOP) Keyboard – PS/2 (MiniDIM6F)
 - Mouse – PS/2 (MiniDIN6F)
 - Monitor – HD15F
 - To Computer (Bottom) Keyboard – PS/2 MiniDIM6F
 - Mouse – PS/2 (MiniDIN6F)
 - Monitor – HD15F

Figure 1. UltraLink 2 Models

CONFIGURATION

Configuration – All Models

There are three ways to configure the UltraLink 2. All models can be configured using a connection to the unit and to a standalone computer or laptop's USB ports. All models can also be configured using a network crossover cable. The dual access model can be configured directly using a local keyboard and mouse. Each method is described below.

Method #1 - Unit configuration via USB ports (all models)

The configuration procedure using the USB connections are shown below.

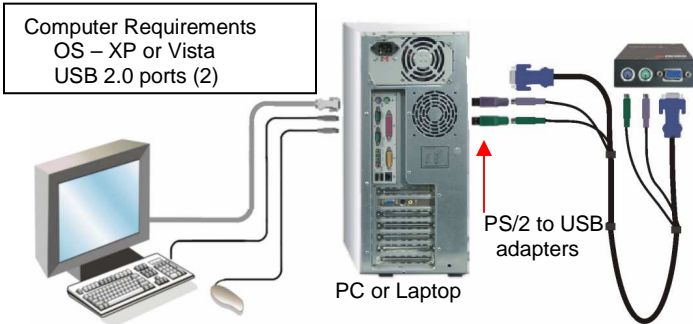
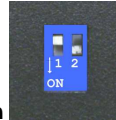


Figure 2. Configuration via USB



Position Switch 2 on the UltraLink 2 to the ON position located on the side of the unit.

1. Disconnect unit from the network (computer and monitor should be ON)
2. Connect the PS/2 to USB adapters to the CPU adapter cable and to the computer or laptop's USB ports.
3. Connect the other end of the cable to the UltraLink 2's PS/2 connectors. (Bottom connectors on Dual model)
4. When the keyboard and mouse connectors are connected to the UltraLink 2, the computer operating system will detect the UltraLink 2 unit as a removable drive.
5. Using Windows explorer, select the UL-2 removable drive and you should see a text file name "Config.txt". Edit this text file using a text editor like Notepad and change the IpAddress, IpNetMask and ipGateway to the IP address information assigned to the UltraLink 2 unit. Also the Unit name, Use DHCP, and Reset Admin Password options can be selected here. Complete instructions are included in the "Config.txt" file.
6. When changes are complete, save the file and close the text editor. From Windows explorer, right click on the removable drive and "Eject" the disk.
7. Wait 2-5 seconds, and then choose "Safely Remove USB Mass Storage Device" by clicking on the "Safely Remove Hardware" ICON in the bottom right Windows toolbar.
8. Disconnect the CPU adapter cable from the computer, wait 15 second, position S2 to the "OFF" position.
9. The UltraLink 2 is now configured and ready to install to your network.

Method #2 - Unit configuration via network crossover cable (all models)

To modify the IP address using method #2, connect the UltraLink 2's RJ45 port to a computer configured with an Ethernet card and Window's operating system (XP or Vista). Use a network cross over cable to connect the computer to UltraLink 2. Connect the computer to be accessed as shown below using the supplied CPU adapter cable.

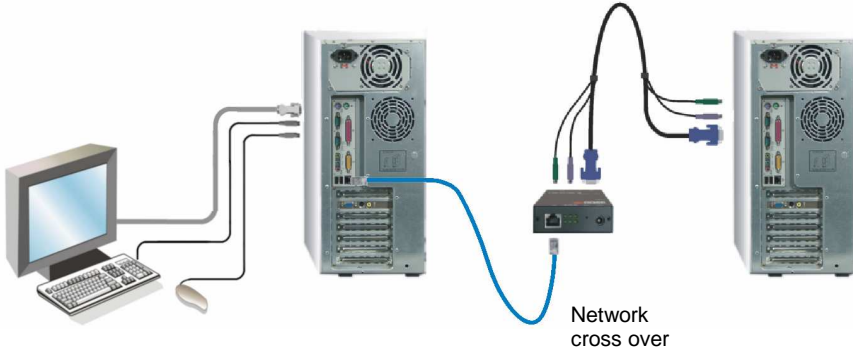


Figure 3. Configure via Network crossover cable

1. Access the control panel, network tab on the computer being used to configure the UltraLink 2 and change the existing IP address to 192.168.1.40 and the IP network mask to 255.255.255.0. This change creates a compatible standalone network between the UltraLink 2 and the computer.
2. From the computer used to configure the unit, start a web browser and enter the IP address 192.168.1.42 (Initial UltraLink 2 default IP address) as the URL.
3. The UltraLink 2 will answer with the following display in the browser.



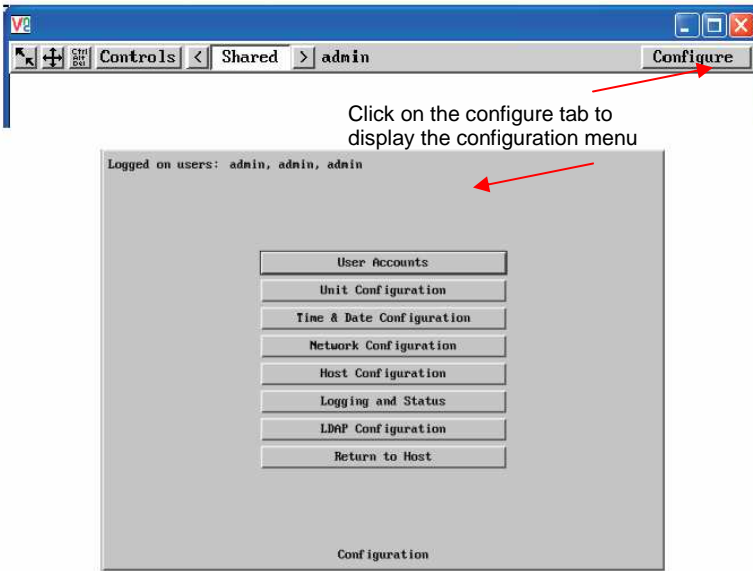
Figure 4. Initial connect screen

There are three options available to select from:

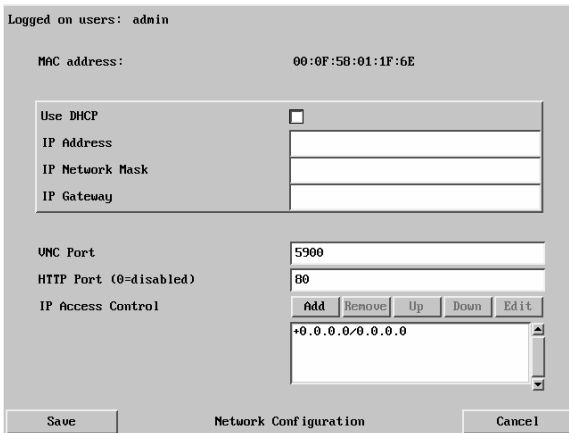
1. Connect using built-in Java VNC Viewer (This option places a temporary Java VNC applet on the computer being used to connect to UltraLink 2, then displays the initial connect screen)
2. Download Windows VNC Viewer from unit (This option downloads the executable file "VNC_VIEWER.EXE" from the UltraLink 2 to the connecting computer. You can run this file to connect to the UltraLink 2 directly)
3. Download latest VNC Viewers from Realvnc.com (Selecting this option will connect to RealVNC's web site and download the latest VNC Viewer)

Initially select option 1 (Connect using built-in Java VNC Viewer) or option 2 (Download Windows VNC Viewer from unit) to connect to the computer. An access logon screen will display. Enter the user ID **“admin”** and no password. The connected computer’s video will display in the browser’s VNC window.

When the connected computer’s video displays, click on the **“Configure”** tab in the upper right corner. This displays the configuration menu.



From the configuration menu, click on **“Network Configuration”**, the below menu will display.



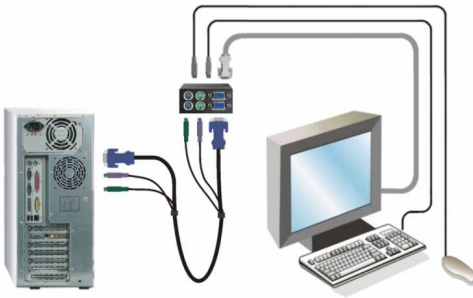
Change the IP address, network mask, and other network information that has been assigned to the UltraLink 2. The VNC port (5900) and HTTP Port (80) should only be changed if they conflict with existing network settings. If you choose to use DHCP, check the box adjacent to "Use DHCP". When complete "Save" the new IP information.

NOTE: When the unit is configured properly and connected to the network, if you have chosen the option "Use DHCP" the IP address will change to whatever IP address your DHCP server assigns it.

When complete, change the IP information on the computer used to connect to the UltraLink 2 back to the original values.

Method #3 - Unit configuration via Local KVM station (dual access model only)

To configure the network information using method #3, connect the UltraLink 2 unit as shown below. This procedure only applies to the dual access model.



1. Connect a local keyboard, monitor, and mouse to the top ports on the UltraLink 2.
2. Connect the supplied CPU adapter cable from the bottom ports on the UltraLink 2 to a standalone computer.
3. Boot the computer.
4. When the boot-up sequence is complete, you should see a logon screen on the KVM monitor.
5. Enter the user ID "admin" and no password.
6. The connected computer's video should display

Figure 5. Configure Dual model

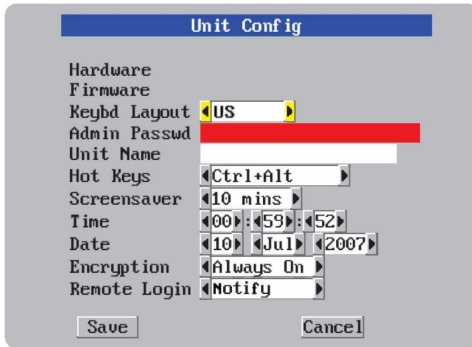
From the local keyboard, press the Ctrl, Alt, and "C" keys simultaneously. This will display the configuration menu as shown below.



Configuration Menu

1. Using the up / down arrow keys, select "Unit Configuration" and press enter.
2. The Unit configuration window will display.
3. Enter the Unit information as described below.

Configure Unit



Unit Configuration Menu

The **Hardware** and **Firmware** versions will display in the first two fields.

Keybd Layout

Use the left and right arrow keys to select the keyboard type of the host computer

Admin password

Enter a password of at least six characters that has a mix of letters and numerals. The background color provides an indication of password suitability and 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

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

Hot Keys

Use the left and right 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. If the UltraLink 2 is connected to a KVM switch, make sure that the hot key combination selected does not conflict with the KVM switch hot key assignments.

Screensaver

Use the left and right arrow keys to select the period of inactivity before a screensaver starts 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.

Time and Date

Set these correctly as all entries in the activity log are time stamped using them.

Encryption

Arrange this setting according to your security requirements. See Encryption settings for a description of the settings.

When the needed information has been entered, click on "Next" to configure the network.

Remote Login

Use the left or right arrow key to select "Notify" or "Ignore". Selecting "Notify" will display on the local KVM monitor all remote users when they connect to UltraLink 2.

Configure Network

The network configuration menu allows you to customize the network settings to be compatible with the network UltraLink 2 will be installed on.

Network Config

MAC Address

Use DHCP

IP Address 192.168.1.42

Net Mask 255.255.255.0

Gateway

VNC Port 5900

HTTP Port 80

Clear IP Access Control

Save Cancel

MAC Address

The MAC address is a unique machine address that identifies the serial number and manufacturer. This is fixed and can not be changed.

Use DHCP

If you have a DHCP server on the network, you can elect to have the server assign the network information. When you change the Use DHCP option to "YES", UltraLink 2 will attempt to locate the DHCP server. If the server is located, it will supply an IP address, an IP network mask (also known as a Subnet mask) and a Gateway address. Remote users must be informed of the IP address to remotely connect.

IP Address, Net Mask, and Gateway

Enter the IP, Net Mask, and Gateway addresses that have been assigned to the UltraLink 2 unit. If Use DHCP was selected, these fields will be greyed out.

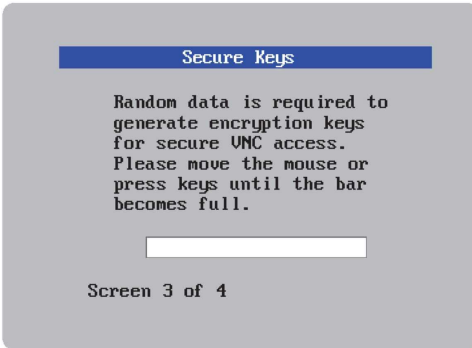
VNC and HTTP ports

These should remain set to 5900 and 80, respectively, unless they clash with an existing setup within the network.

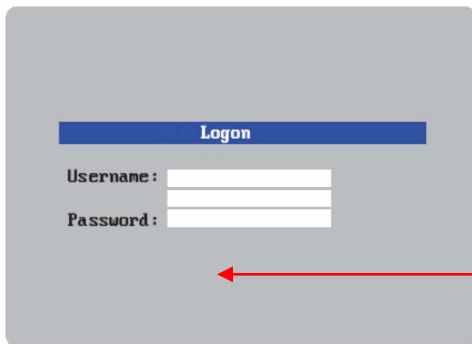
When all of the network information has been entered, click on Save to save the network information and next a secure keys menu will display to develop the encryption keys that are used to establish secure remote links.

Secure Keys Menu

This screen uses your mouse movements or 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 screen (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 UltraLink-2 will be created – this process takes roughly 30 to 40 seconds. Once the secure keys have been calculated the UltraLink-2 will restart and present a standard logon screen.

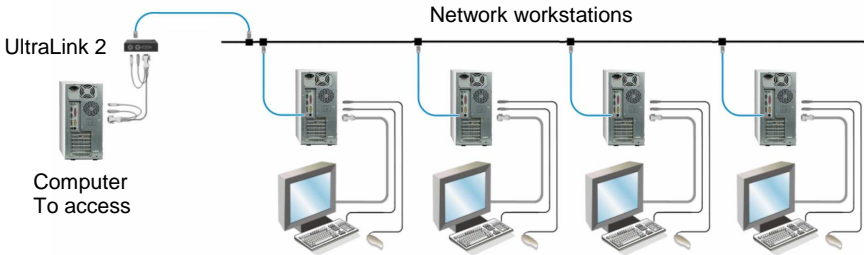


When the Logon screen displays, all remotely connected user will display In this area (separated by a comma)

Enter the Username “admin” and the password entered on the configure unit menu. Upon acceptance, the connected computer’s video will display on the local monitor. The unit is now configured with the correct network and unit information for local and remote access.

Connecting Remotely

With the UltraLink 2 network information configured to match your network, connect the unit to a computer and to the network.



Using a computer connected to the same subnet of the network as UltraLink 2, start a web browser and enter the UltraLink 2's assigned network IP address in the URL field of the browser. When the browser locates the UltraLink 2, it will respond back to the browser with the below request.



- There are three options available to select from;
1. Connect using built-in Java VNC Viewer
 2. Download Windows VNC Viewer from unit
 3. Download latest VNC Viewer from realvnc.com

Initially select option 1 or option 2 to connect to the computer. Option 1 will install a small temporary Java applet on the connecting computer and display the VNC viewer window shown below.

<p>The dialog box is titled 'VNC Viewer : Connection Details'. It has a 'Server:' field with the value '192.168.0.50:0'. The 'Encryption:' dropdown menu is set to 'Let Server Choose (Default)'. There are four buttons at the bottom: 'About...', 'Options...', 'OK', and 'Cancel'.</p>	<p>Refer to Appendix E for VNC Options</p> <p>Color / Encoding / Scaling /Inputs / load-save / Identities / Misc.</p>
---	---

Verify that the Server IP address is correct and click on "OK". The VNC authentication window will display requesting a Username and Password. Enter the username of **admin** and the admin password created during the initial configuration and press Enter.

<p>The dialog box is titled 'VNC Authentication [No Encryption]'. It has a 'Username:' field with the value 'admin' and an empty 'Password:' field.</p>	<p>Upon verification, the connected computer's video will display in the browser's VNC window</p>
---	---

VNC Viewer Toolbar

Figure 6 shows the VNC viewer toolbar and an explanation of each toolbar tab.

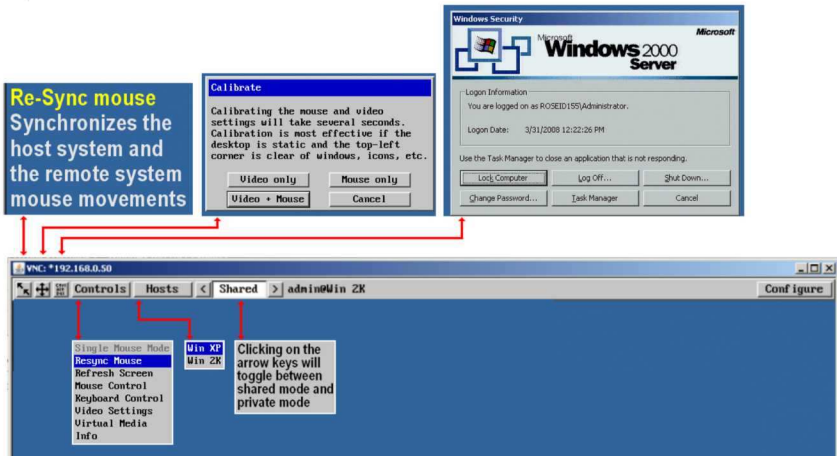








Figure 6. VNC Toolbar

	<p>Clicking on the re-sync icon will synchronize the host and remote system mouse movements.</p>
	<p>This icon brings up a selection box to calibrate the video and/or mouse. Clicking on video or video + mouse will calibrate the video threshold, phase, etc. and then the mouse.</p>
	<p>This icon sends a Ctrl Alt Del command to the host computer and brings up the host computer's task menu.</p>
	<p>The Controls tab displays a selection box that allows you to re-sync the mouse, refresh the screen, mouse and keyboard controls, adjust the video settings, set-up UltraLink 2 for Virtual Media function, and information.</p>
	<p>The Hosts tab provides the quickest and most efficient way to switch between different KVM hosts computers that are connected to a KVM switch.</p>
	<p>Clicking on the left or right arrows switches UltraLink 2 from the shared mode to the private mode. Private mode inhibits other connections.</p>

Remote Configuration Menu

VNC Remote Configuration menu

In the upper right corner of the VNC viewer is the “Configure” tab. Click on this tab to display the configuration menu.

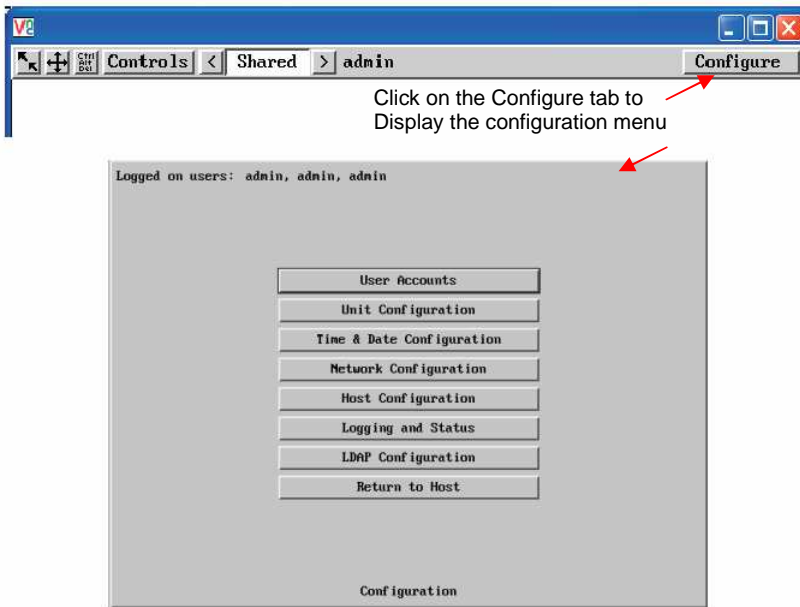


Figure 7. Remote Configuration Menu

The configuration menu allows you to set-up various properties of the UltraLink 2.

User Accounts tab

Allows you to create and manage up to sixteen separate user accounts, each with separate access permissions. Account #1 is the admin account.

Unit Configuration tab (Similar to the initial unit set-up configuration)

Allows you to alter the UltraLink-2 settings. You can define the keyboard, set-up the admin account, assign a name to the unit, screensaver time and encryption options.

Time and Date Configuration tab

Set the time and date, this time stamps the log files

Network Configuration tab (Similar to the initial network set-up configuration)

Allows you to alter the network settings.

Host Configuration tab

Allows configuration of various details for each host system connected to UltraLink 2. 128 entries max, Add host names, Users, and Hotkey.

Logging and Status tab

Provides various details about the user activity on the UltraLink 2.

LDAP Configuration

Allows set-up for LDAP authentication

Return to Host tab

Exit the configuration menu system and return to the host computer.

User Account

Click on the “User Accounts” tab to display the user account menu and to set-up authorized users.

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"/>

Save User Configuration Cancel

Figure 8. Remote User Account Menu

The User Accounts menu allows you to manage up to sixteen separate accounts. Account #1 is the administrator account. Only this account has access to the configuration menus. The admin accounts user name and access rights are fixed. Only the password can be modified.

There are fifteen user account positions.

To create a new account

1. Select a user name field and enter a User Name to activate that position (the Password and access tick box positions will become editable).
 - a. All user names must consist of lower case characters or numbers only. No symbols or upper case characters are permissible. The user name can be between 1 and 16 characters in length
2. Optionally enter a password for the user account.
 - a. Passwords are case sensitive and can include certain keyboard symbols. The password can be between 1 and 16 characters in length. The password background remains shaded in amber while the UltraLink 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.
3. Tick/untick the Local and Remote options that are appropriate to the user.
 - a. Local - User can access the UltraLink 2 directly from the local KVM station
 - b. Remote – User can access the UltraLink 2 via an IP network link or via the internet (depending how the unit is connected and network permissions)
4. Tick/untick the Auto logon option for a selected user. Local access unit only and the user must have local access permission. When power is applied to the unit, the user is automatically logged on. When not in use, the user should logoff.
5. Select another account field and enter the next user information
6. Click on the Save tab to register your changes.

Unit Configuration

Click on the “Unit Configuration” tab to display the Unit Configuration menu. This menu is similar to the initial unit configuration performed.

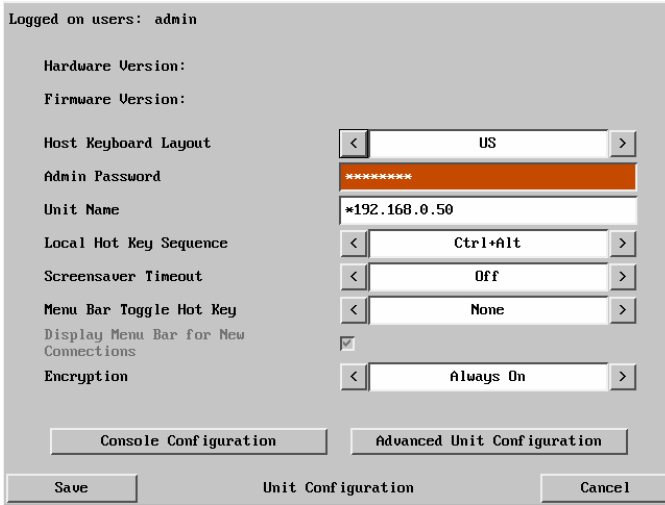


Figure 9. Remote Unit Configuration

Hardware Version -

Indicates the version of the electronic circuitry within the UltraLink 2 unit.

Firmware Version –

Indicates the version of the hardwired software within the UltraLink 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 UltraLink 2. There can only be one admin user and only that user is given access to the configuration menus.

Unit Name -

The name 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.

Note: **DO NOT** assign a Local Hot Key Sequence that is the same as other Hot Key assignments that might be in the system UltraLink 2 is connected to. If you have the UltraLink 2 connected to a KVM switch and assign a hot key of, for instance, F5 and that is the same hot key used by the KVM switch, the UltraLink 2 will intercept that hot key as an instruction and not pass the key sequence to the KVM switch.

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.

Menu Bar Toggle Hot Key

Use the arrow keys to select the hot key to use to toggle the menu bar on and off. Choices are: None, F5-F7, F9-F12

Note: **DO NOT** assign a Menu Bar Toggle Hot Key Sequence that is the same as other Hot Key assignments that might be in the system UltraLink 2 is connected to. If you have the UltraLink 2 connected to a KVM switch and assign a hot key of, for instance, F5 and that is the same hot key used by the KVM switch, the UltraLink 2 will intercept that hot key as an instruction and not pass the key sequence to the KVM switch.

Encryption

Three 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.

Advanced Unit Configuration

Logged on users: admin

Force VNC Protocol 3.3

Idle Timeout (minutes)

Protocol Timeout (seconds)

Background Refresh Rate

Mouse Latency Allowance (milliseconds)

Mouse Rate (milliseconds)

Single Mouse Mode Mouse Switch

Use Quick Mouse Calibration

Behaviour for admin connections when limit reached

Use VESA GTF

Enable Virtual Media

Figure 10. Remote Advanced Unit Configuration

Force VNC protocol 3.3

IMPORTANT: Protocol 3.3 is a legacy version that does not offer any encryption and is not recommended.

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. The Screensaver option serves a similar purpose for local connections.

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 from alternative manufacturers.

During calibration, the UltraLink-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 when using fast KVM switches. 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 from alternative manufacturers. 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

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, or Middle + Left Button.

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 C for a list of all supported video modes.

Reset Unit

Selecting the Reset Unit tab will reset the unit to factory defaults.

Console Configure



Clicking on the Configure Console tab allows you to select the Local Hot Key Sequence, turn on or off the screensaver timeout feature, and turn on or off the notification to the local use that a remote user has logged on

Upgrade Firmware

UltraLink-2 is fully reconfigurable via flash upgrade. This will always keep your UltraLink 2 current and up to date with new enhancements and equipment. Contact Rose Electronics for full details

To perform a flash upgrade

1. Connect to the UltraLink 2 from a remote workstation and log on as the admin user. The firmware upgrade file (xxxxxxx.bin) must be saved on the connecting remote workstation's PC. Upgrades may be performed in one or two stages depending on the update. Make sure that switch 1 is in the off position.
2. Access the Unit configuration page to determine the current firmware version. Ensure that the replacement firmware file has a later version than the installed firmware.
3. Within the Unit configuration page, click the Advanced Unit Configuration button.
4. Click the Upgrade Firmware button and in the subsequent dialog, note the displayed IP address and click OK. The unit is now ready to accept the upgrade files.
5. Open your browser and log into the unit using the IP address that was confirmed in step 4. Once connected, use the Browse button to locate the replacement (.bin) firmware file on your system (Stage 1 or 2). Click the Upload file button. The browser window will confirm the current and replacement firmware versions.
6. Click the Perform upgrade button to proceed. The upgrade progress will be shown on screen and you will be notified when it is complete. When complete cycle power on the unit to complete the upgrade.

Time and Date

Clicking on the "Time & Date Configuration" tab brings up the below Time & Date Configuration menu.

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 11. Remote Time / Date Configuration

Use the arrow keys to set the time (24 hour base) and date. If you wish to use NTP (Network Time Protocol) to set the time, check the box next to Use NTP, enter the NTP Server IP address, and then click on Set Time from NTP Server.

Network Configuration

Click on the "Network Configuration" tab brings up the below configuration menu.

The screenshot shows a "Network Configuration" window. At the top, it says "Logged on users: admin". Below that, the "MAC address" is displayed as "00:0F:5B:01:1F:6E". There is a section for "Use DHCP" with an unchecked checkbox. Below this are three input fields for "IP Address", "IP Network Mask", and "IP Gateway". Further down, the "UNC Port" is set to "5900" and the "HTTP Port (0=disabled)" is set to "80". The "IP Access Control" section includes buttons for "Add", "Remove", "Up", "Down", and "Edit", and a list box containing the IP address range "+0.0.0.0/0.0.0.0". At the bottom of the window are "Save" and "Cancel" buttons, and the text "Network Configuration" is centered.

Figure 12. Remote Network Configuration

The UltraLink 2 is designed to use either a static IP address or an IP address that is assigned by your DHCP server. If you choose to use the DHCP feature, check the box adjacent to "Use DHCP".

NOTE: If you choose the option "Use DHCP" the IP address will change to whatever IP address your DHCP server assigns it. Once the IP address is changed the connection to UltraLink 2 will be lost. Also, if it is changed by the DHCP server the user must determine the new IP address in order to connect to the computer to access.

If you choose to use a static IP address, change the IP address, IP network mask, and IP Gateway as needed to be compatible with your network. The UNC port (5900) and HTTP Port (80) should only be changed if they conflict with existing network settings or equipment. .

The IP Access Control feature allows you to specify a range of IP address that will or will not be granted access to the UltraLink 2 unit. This additional feature adds to the security of the UltraLink 2. The default IP access control is +0.0.0.0/0.0.0.0 which grants all IP addresses access to the UltraLink 2. Click on the "Add" tab to add an IP range to grant or deny access.

NOTE: The IP Access Control list should have all granted access IP addresses added first and all denied access IP address added last. This is because of the position of the entries in the list. Once a range of addresses is denied access, it is not possible to grant access to a particular address within the denied range down the list. Below is an example of the correct and incorrect way to control access.

Calculating the mask for IP access control

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 IP address(es).

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, 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 that 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.

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 and 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)

When complete, click on the “Save” tab to save the new IP information.

Host Configuration

Click on the “Host Configuration” tab to display the Host menu shown in Figure 13.

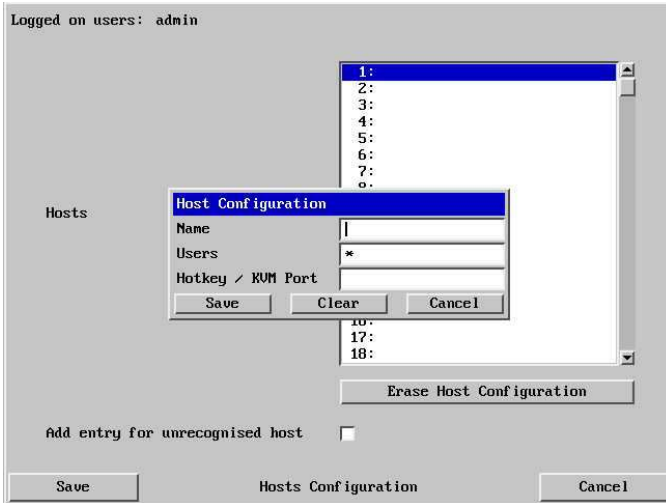


Figure 13. Remote Hosts Configure Menu

Connecting the UltraLink 2 to a KVM switch provides remote access to all the equipment connected to the KVM switch. The Host feature is designed to easily switch to any of the KVM switches ports. Clicking on a Host position (1 – 128) will display the Host Configuration data box. Each Host can be assigned a Host Name, grant specific users access, and the Hotkey / KVM port keystroke sequence to access the specific port. Enter a Host Name in the Name field. This name will display when you select the Host tab on the VNC viewer toolbar. Enter a user name (e.g. admin, david, mark,...) or * for all users.

Next enter the Hotkey / KVM port keyboard sequence to switch to this Host position.

Hotkey sequences

Almost any combination of key presses can be emulated using the following notations:

- +** means press down the key that follows;
- means release the key that follows
- + -** means press and then release the key that follows
- *** means add a delay. The standard delay period is 250ms; however, if a number immediately follows the asterisk, this will define an alternate delay period (in milliseconds)

Notes

- *The entries are not case sensitive.*
- *It is not necessary to specify all keys to be released at the end because they are all released automatically after the last code.*
- *A number of KVM switches from alternative manufacturers use hot key sequences that begin with a press/release of either the Scroll Lock or Ctrl keys. These often require a delay between the initial key press and the channel number to allow the switch to respond. A 500ms delay is usually sufficient.*

Examples:

To end the command Press/release Ctrl + 5 + enter, enter the following: +-Ctrl+-5+enter

To send the command *Ctrl + Alt 4*, enter following: +Ctrl+Alt+4.

To send the command *Ctrl + Alt 12*, enter the following: +Ctrl+ALT+-1+2

To send the command Ctrl + 1 + enter, enter the following: +Ctrl+-1+enter

To send the command Ctrl + 15 + enter, enter the following: +Ctrl+-1+-5+enter (the '+-1' entry causes the 1 key to be pressed and released before the-2 key is pressed).

To send the command *Scroll lock 1 + Enter* (with a 500ms delay), enter the following: +-Scr*500+1+Ent

Permissible key presses

Main control keys

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

Add (Plus) | Subtract (Minus) | Multiply

Central control keys

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

Keypad keys

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.

When all entries have been made, click on the Save tab to save the information entered.

Logging and Status

The Logging and Status screen provides various details about the user activity on the UltraLink 2.

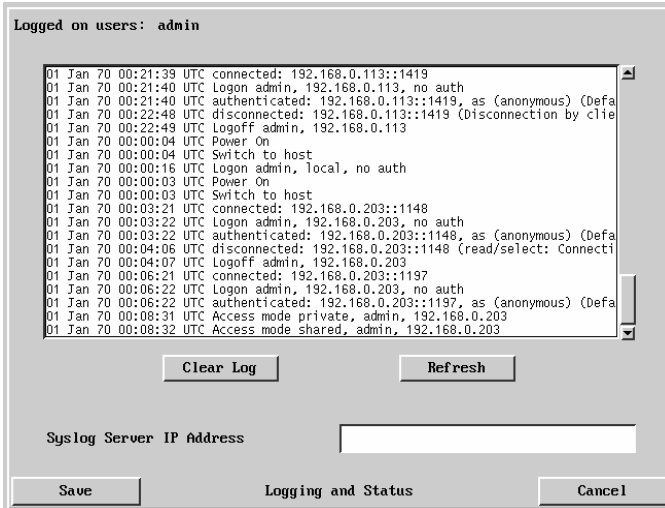


Figure 14. Logging and Status Screen

The log shows the date, time, connection type, and activity that has taken place on the UltraLink 2 unit.

If you wish to route the log information to a Syslog Server, enter the server's IP address in the field provided.

To clear the log, click on the "Clear Log" tab. Click on the "Refresh" tab to refresh the log status information.

The Save tab saves the log status information.

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

LDAP Configuration

The LDAP configuration should be performed by the administrator and / or the network administrator. Inputs will vary depending on the network configuration, LDAP server IP address and port number, and other parameters.

LDAP configuration can be done by clicking on the “Configure LDAP” tab from the main menu. This brings up the below menu. To implement the use of LDAP authentication, check the box. This enables the input fields.

Logged on users: admin

Use LDAP

Host Address

Host Port

Base DN

User field

Anonymous Bind

Save LDAP Configuration Cancel

Figure 15. LDAP Configuration

Host address	The IP address of the LDAP server to contact for authentication
Host Port	The port number that the LDAP server uses for authentication
Base DN	The name to bind against the LDAP server (Example – “dc=rose, dc=com”)
User Field	The LDAP database entry field to match usernames against. This field will vary depending on the specific LDAP database being used. Typical values are ‘uid’ or ‘cn’.
Anonymous bind	If checked, bind requests are anonymous (suitable for Linux implementations). If unchecked, the bind requests are sent with the user name and password (suitable for active directory)

INSTALLATION

Single Unit Installation

The installation of the UltraLink 2 single access unit is a very easy process. Connect the provided CPU adapter cable to the corresponding PS/2 keyboard, monitor, and PS/2 mouse ports on the UltraLink 2 and on the computer to access. Next connect the network cable from the unit to the network and your done.

- - - UltraLink 2 must be configured properly before installing and accessing - - - .

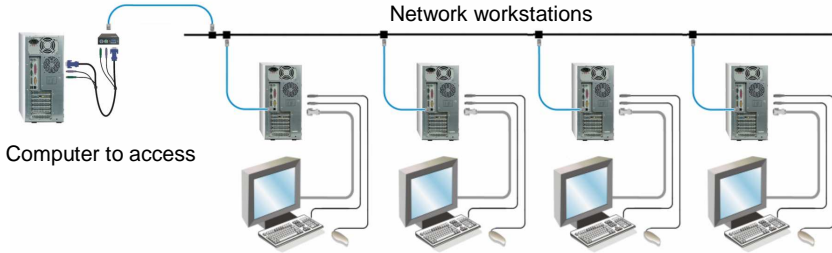


Figure 16. Single unit installation

Dual Unit Installation

The installation of the UltraLink 2 Dual access model is the same as the single model with the addition of a local KVM station. Connect a local keyboard, monitor, and mouse to the corresponding top connectors on the UltraLink 2. Connect the keyboard, monitor, and mouse cable from the computer to access to the corresponding bottom connectors on the UltraLink 2.

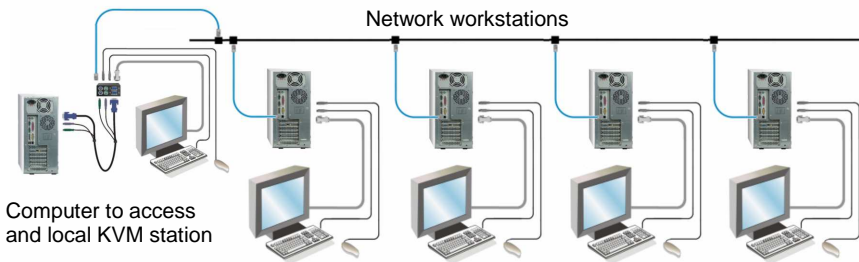


Figure 17. Dual unit installation

Dual Unit Installation to a KVM Switch

The installation of the UltraLink 2 Dual model to a KVM switch is the same as the dual model installation except a KVM switch is substituted for the stand-alone computer as show in Figure 18. Connect a local keyboard, monitor, and mouse to the corresponding PS/2 top connectors. Connect the supplied keyboard, monitor, and mouse cable from the UltraLink 2, bottom connectors, to the corresponding keyboard, monitor, and mouse ports on the KVM switch. If the KVM switch does not provide +5VDC on both the keyboard and mouse connections, then an optional power adapter must be used.

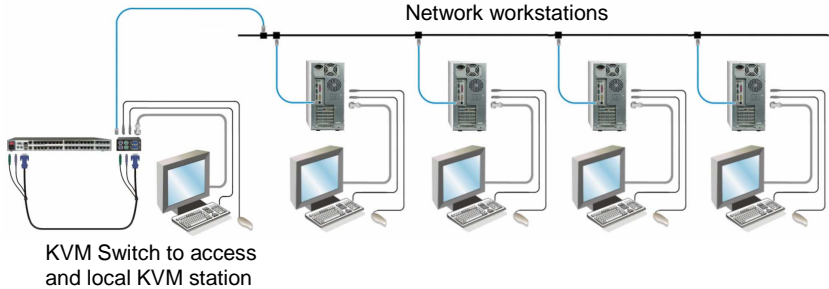


Figure 18. Installation to a KVM switch

In this configuration, all network and IP workstations have access to the KVM switch. The Hosts tab on the VNC viewer toolbar can be set-up to access all equipment connected to the KVM switch. See "Hosts Configuration" and Figure 13 for host configuration procedures.

Hotkey port switching can also be done from remote workstations provided the Hotkey assignments for the UltraLink 2 do not conflict with any of the KVM switches Hotkey assignments. If a Hotkey assignment has been set-up on the UltraLink 2 that is the same as a Hotkey on the KVM switch, the KVM switch will never receive the Hotkey because UltraLink 2 will intercept it and treat it as an instruction for UltraLink 2.

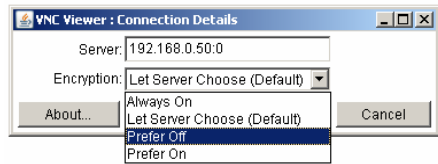
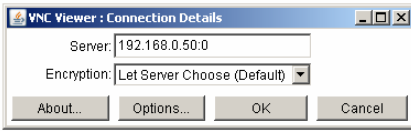
Operating procedure

From any network workstation, start a web browser and enter in the URL field, the IP address assigned to the UltraLink 2 unit. When the unit is located on the network, it will respond back to the web browser with the following three options:

1. Connect using built-in VNC Viewer
2. Download Windows VNC Viewer from unit
3. Download latest VNC Viewer from realvnc.com

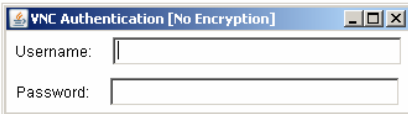


Selecting option 1 will invoke UltraLink 2 to download a small temporary Java applet to the connecting computer and then display the VNC Viewer Connection Details window. Verify that the Server IP address is correct. Click on the down arrow to list the Encryption options. Normally the default setting is used.



Click "OK" to connect to the UltraLink 2 unit.



The VNC authentication box will display requesting a Username and Password.



Enter the correct Username and Password that was set-up for the user on the configure user menu and press enter. Upon authentication, the connected computer's video will display in the VNC viewer window.

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)

Figure 19 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 (Host Computer) or the remote PC's desktop. When working within the VNC Viewer window, 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 UltraLink 2 or switch CPU ports if connected to a KVM switch, 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 VNC viewer window.

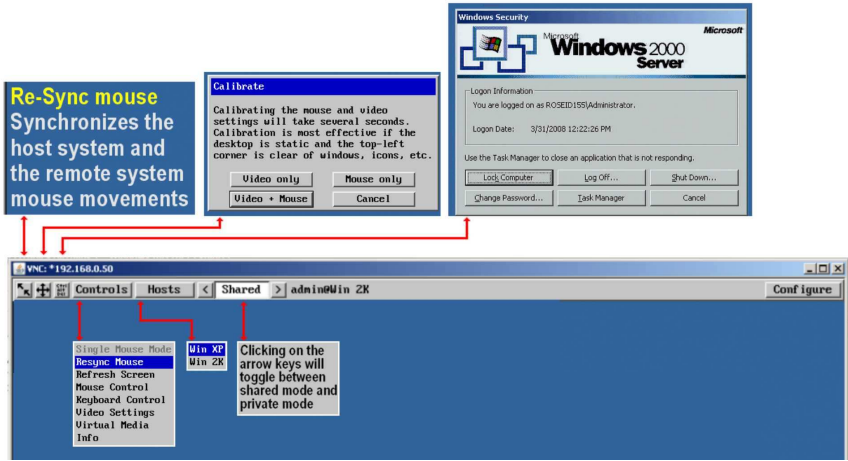


Figure 19. VNC Viewer Toolbar

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.

Video Settings

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

Video Settings

Video mode: ves a 1024 x 768 @ 60Hz

Threshold	◀ ▶	512	Auto
Phase	◀ ▶	30	Auto
Horizontal Position	◀ ▶	4	Auto
Vertical Position	◀ ▶	1	Auto

Brightness		Contrast			
Red	◀ ▶	128	◀ ▶	76	
Green	◀ ▶	128	◀ ▶	74	Auto
Blue	◀ ▶	128	◀ ▶	79	

Display Activity 0.55%

Custom Modes

Save Calibrate All Advanced Cancel

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. UltraLink-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 UltraLink-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 UltraLink-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.

Phase, Position (Horizontal / Vertical), Brightness, Contrast

Use the left or right arrow keys to adjust the phase, position, brightness and contrast to produce the desired display results.

Virtual Media

A unique feature of the UltraLink 2 is the Remote Virtual Media function. This feature allows you to remotely send or receive files or folders from the connected computer. Single files or collections of files and folders up to 2GB in size can be quickly transferred via the VNC link. This can prove to be an invaluable tool when upgrading host computers from remote positions. In order to use the Remote Virtual Media feature, a VM link must be made between the unit and a **USB** port on the host computer. See Appendix D for detailed instructions on using the Virtual Media feature.

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



If UltraLink 2 is connected to a KVM switch and the Configure Host feature has been set-up, the “Host” tab on the toolbar will display. It allows you to easily switch to any CPU port on the KVM switch. Each of the 128 Host locations can be set-up with the appropriate keyboard command sequence 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.

Shared Tab

The shared feature allows you to either share the connection with up to 4 simultaneous users or select the private mode, which inhibits other users from accessing the UltraLink 2. In the shared mode, all connected users see and control the same computer simultaneously. Keyboard and mouse activity is on a first come, first serve basis. This feature allows remote users to collaborate on a common project, review information, and other functions that involve multiple users at different remote locations.

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' network address has not been excluded in the IP access control section.
- If the UltraLink-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.

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 UltraLink 2 for two to three seconds. This will reset the unit and unlock the IP address. If the UltraLink2 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.

Virtual media feature not functioning

- Keyboard and mouse connection to the remote computer must use the PS/2 to USB adapters and connect to the remote computer's USB ports.

Safety

The UltraLink-2, like all electronic equipment, should be used with care. To protect yourself from possible injury and to minimize the risk of damage to the Unit, read and follow these safety 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.

Provide proper ventilation and air circulation.

Keep connection cables clear of obstructions that might cause damage to them.

Use only power cords, power adapter and connection cables designed for this Unit.

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.

Do not use liquid or aerosol cleaners to clean this Unit. Always unplug this Unit from the power source before cleaning.

Remove power from the Unit and refer servicing to a qualified service center if any of the following conditions occur:

- The connection cables are 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.

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 UltraLink 2, 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.

Appendix A- Specifications

Video	Resolution – 1600 x 1200 (See Appendix C for supported video modes)
Power ports.	Obtained from the host computer's keyboard and mouse or USB Optionally connect a power adapter if needed 5VDC -1A – Standard
Connectors	Power: Barrel jack Local KVM: Video – HD15F Keyboard – MD6F (PS/2) Mouse – MD6F (PS/2) Host computer: Video – HD15F Keyboard – MD6F (PS/2) Mouse – MD6F (PS/2) Network port: RJ45F
Chassis	Steel (Black)
Switches	Power select Switch
Indicators	LEDs: Power, Link, Local, Remote, VNC, Speed
Ethernet Link	10/100 Mbs Ethernet speed
Environmental	0°- 45°C / 32°- 113°F, 5 - 80% non-condensing RH
Approvals	FCC, CE

Dimensions	Width	Depth	Height	Weight
UL2-SA (in)	2.95	4.72	1.06	0.76 lbs
(mm)	75	120	27	0.34 kg
UL2-DA (in)	2.95	4.72	1.65	1.02 lbs
(mm)	75	120	42	0.46 kg

Appendix B- Part Numbers

Part Number	Description
UL2-SA	UltraLink 2 Single mode
UL2-DA	UltraLink 2 Dual mode
TRF-05D250FSUB-2.5	Power adapter (Optional - /SW P/N suffix)
	CPU Adapter cable (Supplied with order)

Appendix C- Video Modes

The following video modes are supported and can be automatically configured by the UltraLink-2. If a recognized video mode cannot be found, the UltraLink-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 640 x 480 @ 60Hz
vesa 640 x 480 @ 72Hz
vesa 640 x 480 @ 75Hz
vesa 640 x 480 @ 85Hz
vesa 800 x 600 @ 56Hz
vesa 800 x 600 @ 60Hz
vesa 800 x 600 @ 72Hz
vesa 800 x 600 @ 75Hz
vesa 800 x 600 @ 85Hz
vesa 1024 x 768 @ 60Hz
vesa 1024 x 768 @ 70Hz
vesa 1024 x 768 @ 75Hz
vesa 1024 x 768 @ 85Hz
vesa 1152 x 864 @ 75Hz
vesa 1280 x 960 @ 60Hz
vesa 1280 x 1024 @ 60Hz
vesa 1280 x 1024 @ 75Hz
vesa 1600 x 1200 @ 60Hz
vesa 720 x 400 @ 70Hz*
sun 1152 x 900 @ 66Hz
sun 1152 x 900 @ 76Hz
sun 1280 x 1024 @ 67Hz
apple 640 x 480 @ 67Hz
apple 832 x 624 @ 75Hz
apple 1152 x 870 @ 75Hz

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

Appendix D- Virtual Media Feature

The UltraLink-2 provides an ingenious feature that allows authorized remote users to transfer files and folders to a host computer. The “Host” computer must be connected to the UltraLink 2 using the PS/2 to USB adapters.

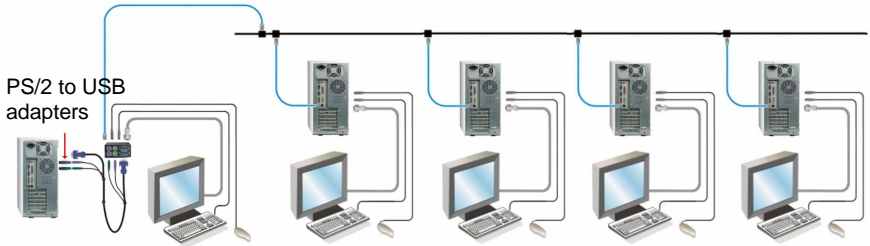
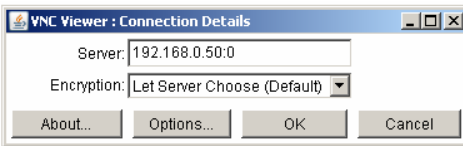
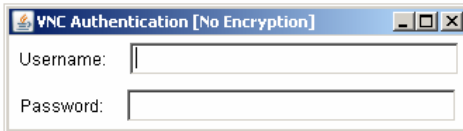


Figure 20. Virtual Media set-up

Start the VNC viewer, not the Java applet, and enter the assigned IP address in the Server field. Select the encryption needed or use the Default value and click on OK.

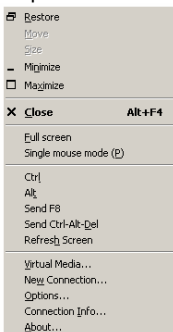


Upon connection, the VNC Authentication screen will display. Enter the Username and Password and press Enter.



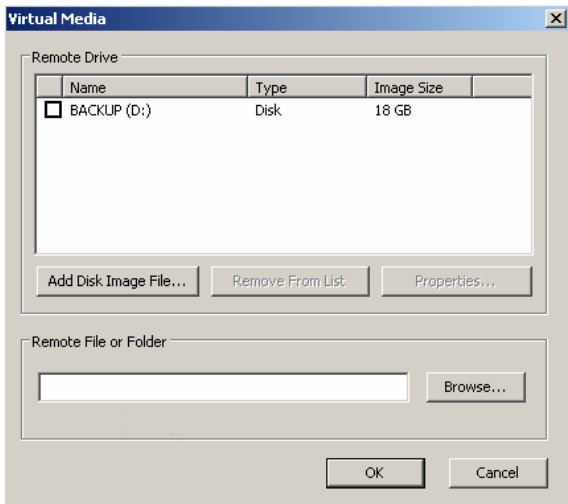
When the username and password are authenticated, the Host computer's video will display. Once connected the Virtual Media feature can be executed.

To start the Virtual Media feature, press the F8 key, then select “Virtual Media” from the drop-down list.



Select Virtual Media

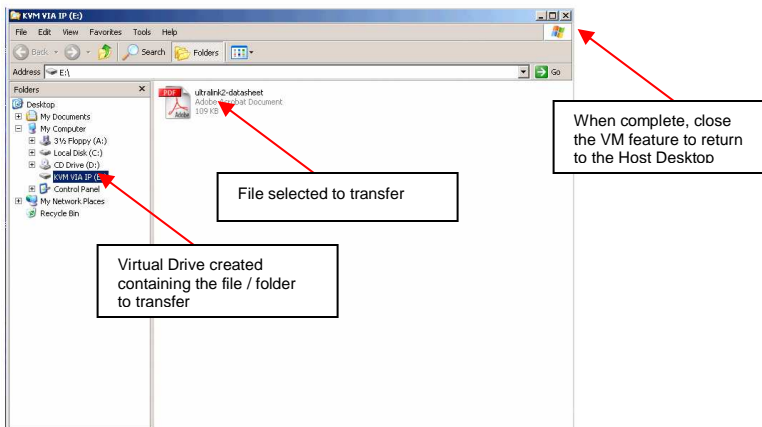
When you select Virtual Media, a file selection window will open requesting the file or folder name to transfer to the Host computer.



Enter the file or folder name to transfer from the remote connection to the Host computer or click on the Browse tab to locate the file / folder to transfer. When the file / folder name has been entered, click on OK to start the process.

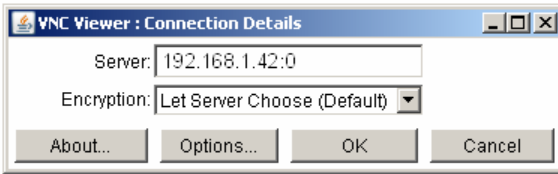
UltraLink 2 will establish a USB connection from the remote to the Host computer and start windows explorer showing the virtual drive and the selected file to transfer to the Host computer.

Select the file to transfer and drag and drop it to the needed location on the Host computer. The file / folder will not be transferred until you drag and drop it to the Host computer.

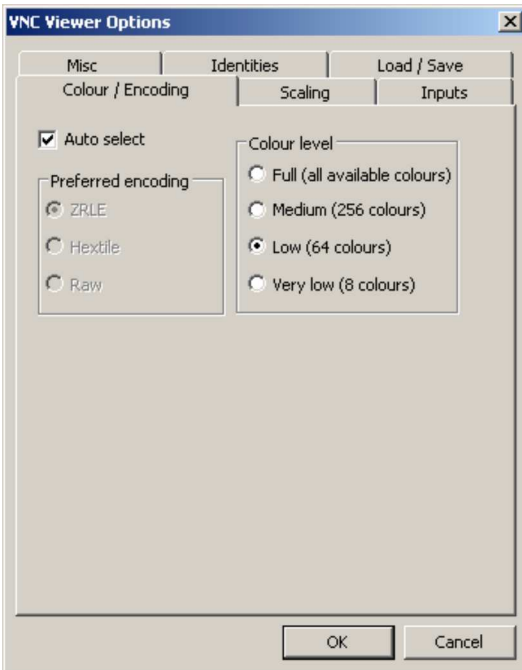


Appendix E- VNC Viewer Options

When you are connected to the UltraLink 2 using the VNC viewer (not the java applet), there are several options that are available to modify the way the connection is made.



Click on the “Options” tab and the below VNC Viewer Option screen will display.



When Auto select is checked, this option will examine the speed of your connection to the UltraLink 2 and apply the most suitable encoding method. This option is suggested for the majority of installations. When unchecked, there are three encoding options that can be selected.

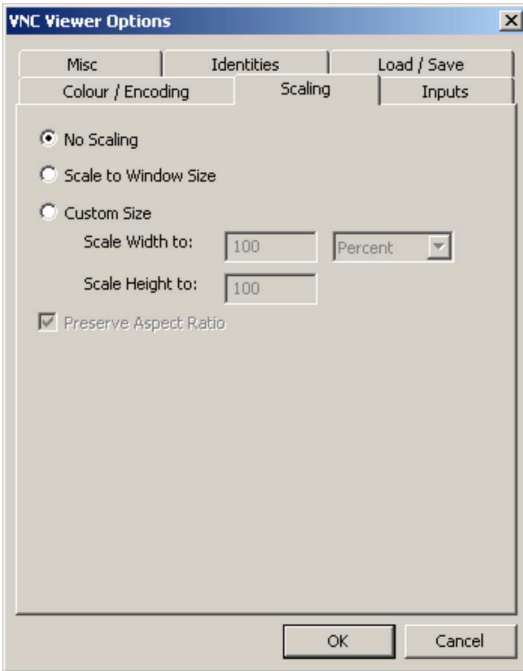
- **ZRLE** – This is a highly compressed method that is best suited to slow modem connections.
- **Hextile** – This method offers better performance than the ZRLE when used over a high speed network because there is no need for the unit to spend time highly compressing the data.
- **Raw** – This is a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

Color level

This section allows you to select the most appropriate color level for the speed of the connection to the UltraLink 2. 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 (colors)** – This mode reduces the host system output to a 256 color mode and is more suitable for ISDN and fast modem connections.
- **Low (colors)** – This mode is suitable for slower modem connections and reduces the host system output to 64 colors.
- **Very low (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 tab



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.

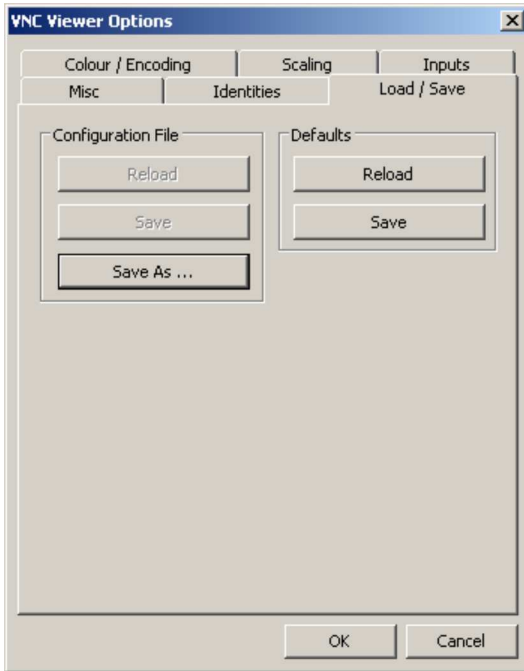
Custom Size

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.

Load / Save tab



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.

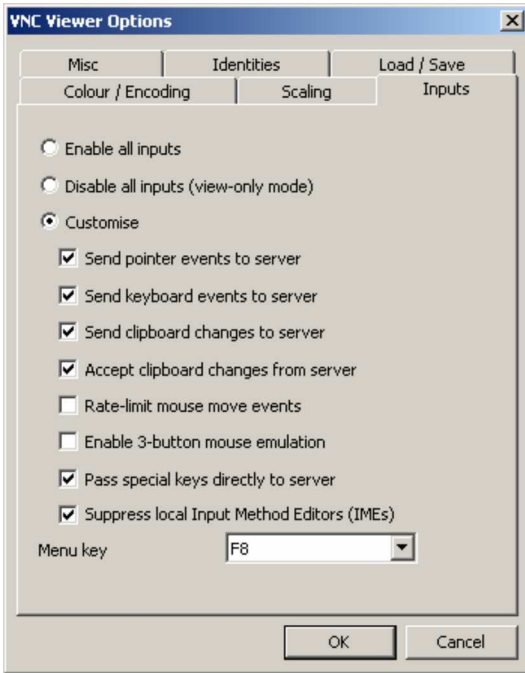
Defaults - Reload

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.

Inputs tab



Enable all inputs

When selected, allows keyboard, mouse and clipboard data to be transferred between server and viewer systems.

Disable all inputs (view-only mode)

When selected, prevents control data being passed between server and viewer. Viewer can display the server output, but cannot control it.

Customize

Allows you to select which data can be transferred between server and viewer.

Send pointer events to server

When un-ticked, the VNC viewer will not send mouse movement or click data to the unit or host system.

Send keyboard events to server

When un-ticked, the VNC viewer will not send keyboard information to the unit or host system.

Send clipboard changes to server

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

Accept clipboard changes from server

This feature is restricted to software server versions of VNC and has no effect on unit installations, except for retrieving the activity log as described in the logging and status section.

Rate-limit mouse move events

When ticked, this feature reduces the mouse movement information that is sent to the unit and host system. This is useful for slow connections and you will notice that the remote cursor will catch up with the local cursor roughly once every second.

Enable 3-button mouse emulation

This feature allows you to use a 2-button mouse to emulate the middle button of a 3-button mouse. When enabled, press the left and right mouse buttons simultaneously to create a middle button action. You are advised to generally use a 3-button mouse.

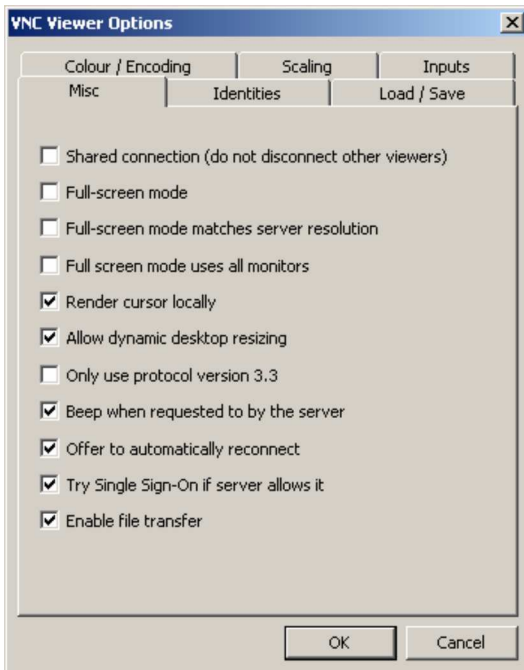
Pass special keys directly to server

When ticked, 'special' keys (the Windows key, the Print Screen key, Alt+Tab, Alt+Escape and Ctrl+Escape) are passed directly to the unit rather than being interpreted locally.

Menu key

This feature allows you to select which function key is used to display the VNC viewer options menu. The menu key is only way to exit from the full screen viewer mode.

Misc tab



Shared connection (do not disconnect other viewers)

This option does not apply to UltraLink 2 connections.

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.

Render cursor locally

This option does not currently apply to unit connections.

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

This option does not apply to the UltraLink 2 connections.

Beep when requested to by the server

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

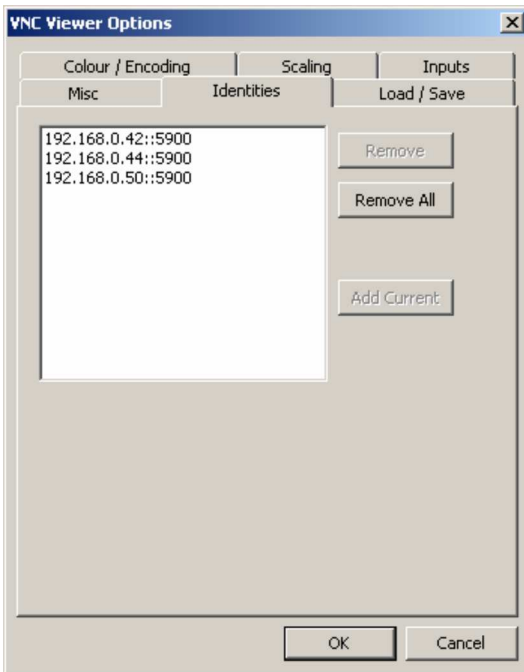
Offer to automatically reconnect

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

Try Single Sign-On if server allows it

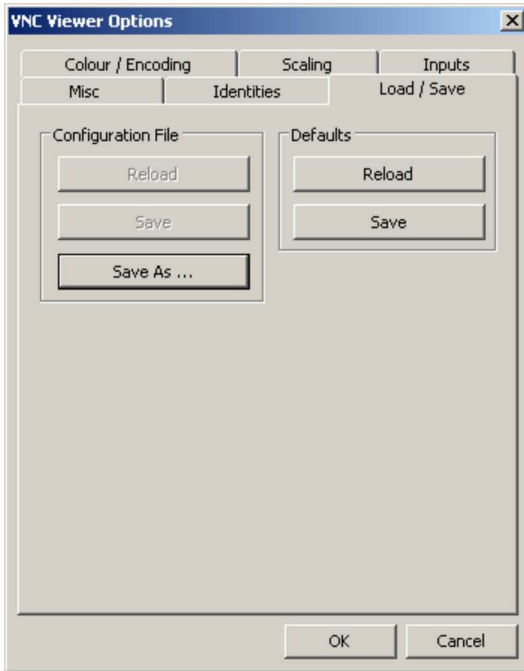
This option does not apply to UltraLink 2 connections.

Identities tab



This feature helps your VNC viewer to confirm that a revisited UltraLink 2 is genuine and not another device masquerading as an UltraLink 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 unit, the security information for that UltraLink 2 unit is cached within this Identities tab (i.e. the "identity" is known). The next time that you connect to the 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 UltraLink 2 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 tab



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.

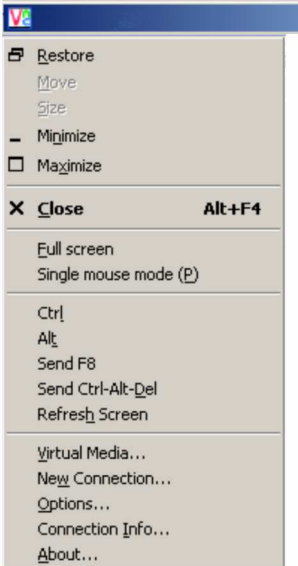
Defaults - Reload

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.

VNC viewer window options



Standard window control items

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.

Single mouse mode (P)

Used for fast network connections where a second, "predictor" cursor is not required.

Ctrl, Alt, Send F , Send Ctrl-Alt-Del

Sends the selected keypress(es) to the UltraLink 2 and host system. This is necessary because certain keys and key combinations are trapped by the VNC viewer.

Refresh Screen

Requests data from the server for a complete redraw of the screen image, not just the items that change.

New connection...

Displays the connection dialog so that you can log on to a different UltraLink 2 or VNC server location.

Options...

Displays the full range of connection options

Connection info...

Displays various connection and display details.

About...

Displays information about your VNC viewer.



Server Management



Solutions

10707 Stancliff Road
Houston, Texas 77099

Phone (281) 933-7673
www.rose.com